BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

DNS ABUSE: ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI İLE MÜCADELEDE DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER

Burak EREN

Bilişim Uzmanlık Tezi

Temmuz 2024

Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

DNS ABUSE: ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI İLE MÜCADELEDE DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER

Burak EREN

Bilişim Uzmanlık Tezi

Temmuz 2024

Ankara

Burak EREN tarafından hazırlanan “DNS ABUSE: ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI İLE MÜCADELEDE DÜNYA ÖRNEKLERİNİN İNCELENMESİ VE ÜLKEMİZ İÇİN ÖNERİLER” adlı bu tezin Bilişim Uzmanlık tezi olarak uygun olduğunu onaylarım.

Meltem ERGÜN
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlık tezi olarak kabul edilmiştir.

Başkan : Kurul Başkanı, Ömer Abdullah KARAGÖZOĞLU

Üye : Kurum Başkan Yardımcısı, Mustafa KARAMAN

Üye : Daire Başkanı, Mahmut Esat YILDIRIM

Üye : Bilişim Başuzmanı, Onur GENÇER

Üye : Bilişim Uzmanı, Meltem ERGÜN

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	DNS Abuse: Alan Adı Sisteminin Kötüye Kullanımı ile Mücadelede Dünya Örneklerinin İncelenmesi ve Ülkemiz İçin Öneriler
Türü	Bilişim Uzmanlık Tezi
Yazar	Burak EREN
Teslim Tarihi	02.07.2024
Anahtar Kelimeler	DNS, Alan Adı, DNS Abuse, ccTLD, gTLD, ICANN, Alan Adı Sisteminin Kötüye Kullanımı
Tez danışmanı	Meltem ERGÜN
Sayfa Adedi	vi + 186

İnternet kullanımının artması ve dijitalleşmenin hız kazanmasıyla birlikte alan adı sektörü yıllar içinde önemli ölçüde büyümüş ve bu büyüme ile birlikte alan adı sisteminin kötüye kullanımı amaçlı faaliyetler de artmıştır. Bu kötü amaçlı faaliyetlerin önemli bir kısmını DNS Abuse oluşturmaktadır.

Bu tezde; ulusal ve uluslararası çalışmalar ışığında, ".tr" uzantılı alan adları üzerinden gerçekleştirilebilecek DNS Abuse faaliyetlerinin önlenmesi ve gerçekleşmesi sonrasındaki mağduriyetlerin azaltılması için kayıt otoriteleri nezdindeki uygulamalar açıklanmış ve mevzuat düzenlemelerine ilişkin öneriler sunulmuştur.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	DNS Abuse: Examining World Examples in Combating Domain Name System Abuse and Recommendations for Our Country
Type	ICT Expert Thesis
Author	Burak EREN
Submission Date	02.07.2024
Key Words	DNS, Alan Adı, DNS Abuse, ccTLD, gTLD, ICANN, Adı Sisteminin Kötüye Kullanımı
Advisor	Meltem ERGÜN
Total Page	vi + 186

With the increase in the use of the Internet and the acceleration of digitalization, the domain name industry has grown significantly over the years, and with this growth, activities aimed at misuse of the domain name system have also increased. DNS Abuse constitutes a significant part of these malicious activities.

In this thesis; in the light of national and international studies, recommendations on the implementation and legislative regulation at the registration authority are presented in order to prevent DNS Abuse activities that may be carried out through domain names with ".tr" extension and to reduce the victimization after the occurrence.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Meltem ERGÜN'e, yine kıymetli tecrübelerinden faydalandığım çalışma arkadaşım Naci Soner PAYASLI'ya ve tüm çalışma arkadaşlarıma, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli aileme ve sevgili eşim Kübra ÖNCÜ EREN'e sonsuz minnet ve şükranlarımla.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

auDA	.au Domain Management Limited
BTK	Bilgi Teknolojileri ve İletişim Kurumu
ccTLD	Ülke Kodu Üst Düzey Alan Adı (Country Code Top-Level Domain)
CIRA	Canadian Internet Registration Authority
DAAR	Alan Adı Kötüye Kullanım Faaliyeti Raporlama (Domain Abuse Activity Reporting)
DNS	Alan Adı Sistemi (Domain Name System)
DNSSEC	Alan Adı Sistem Güvenliği Uzantısı (Domain Name System Security Extensions)
DNSTICR	Alan Adı Güvenliği Tehdidi Bilgi Toplama ve Raporlama (The Domain Name Security Threat Information Collection and Reporting)
GNSO	Jenerik Alan Adları Destek Kuruluşu (Generic Names Supporting Organization)
gTLD	Genel Üst Düzey Alan Adı (General Top-Level Domain)
ICANN	İnternet Tahsisli Sayılar ve İsimler Kurumu (Internet Corporation for Assigned Names and Numbers)
IP	İnternet Protokolü (Internet Protocol)
RA	Kayıt Otoritesi Yetki Sözleşmesi (Registry Agreements)
RAA	Kayıt Kuruluşu Akreditasyon Sözleşmesi (Registrar Accreditation Agreement)
RBL	Reputation Block List
TAKAL	Tahsisi Kapalı Alan Adları Listesi
TAKIL	Tahsisi Kısıtlı Alan Adları Listesi
TLD	Üst Düzey Alan Adı (Top Level Domain)
TRABİS	.tr Ağ Bilgi Sistemi
USOM	Ulusal Siber Olaylara Müdahale Merkezi

GİRİŞ

İnternet, bilgisayar ve diğer akıllı cihazlar aracılığıyla veri ve bilgilerin iletilmesini veya alınmasını sağlayan bir iletişim ağıdır. İnternet üzerinden iletişim "İletişim Kontrol Protokolü (*Transmission Control Protocol - TCP*)" ve "İnternet Protokolü (*Internet Protocol - IP*)" ile sağlanmakta ve ağdaki her bir cihaza benzersiz bir tanımlayıcı olan IP adresi atanmaktadır. İnternet site içeriklerinin bulunduğu sunucular da bu cihazlar arasında yer almaktadır.

IP adreslerinin uzun ve karmaşık olmasından dolayı kendilerine karşılık gelen ve akılda tutulması kolay olan alan adları oluşturulmuştur. Alan adı IP eşleşmesini sağlamak için de Alan Adı Sistemi (*Domain Name System - DNS)* geliştirilmiştir. Bu sayede, tarayıcı arama sekmesine yazılan alan adları ile internet sitelerine erişilebilmektedir.

DNS, hiyerarşik bir yapı olarak tasarlanmıştır ve alan adı yapısı da bu tasarımı yansıtmaktadır. Alan adı yapısındaki bu hiyerarşi sağdan sola doğru gerçekleşmektedir. Alan adının en sağında görülen ".tr, .com, .gov, .be" gibi uzantılar üst düzey alan adı *(top level domain - TLD)* olarak isimlendirilmektedir. TLD'ler kendi içerisinde üçe ayrılmaktadır:

1. Ülke Kodu Üst Düzey Alan Adı *(Country Code Top-Level Domain - ccTLD)*: ".tr", ".uk", ".de," ".be" vb.
2. Genel Üst Düzey Alan Adı *(General Top-Level Domain - gTLD)*: ".com", ".net", ".gov", ".edu" vb.
3. Teknik amaçlı kullanılan ".arpa"

ccTLD uzantılı alan adı yönetimi ve düzenlemeleri ilgili "Kayıt Otoritesi (*Registry*)" tarafından gerçekleştirilirken, gTLD uzantılı alan adı yönetimi ve düzenlemeleri büyük oranda İnternet Tahsisli Sayılar ve İsimler Kurumu (*Internet Corporation for Assigned Names and Numbers - ICANN*) tarafından gerçekleştirilmektedir. ".arpa"

uzantısının yönetimi ise İnternet Mimari Kurulu *(Internet Architecture Board - IAB)*[1] ile IANA tarafından iş birliği içerisinde yürütülmektedir.

2000'li yıllarla birlikte kullanımı ciddi oranda artan internet, 2010'lu yıllarla birlikte hayatımızın vazgeçilmez bir unsuru olmuştur. Bu değişimde, internet altyapısının gelişmesi, fiyat tarifelerindeki düşüş, dijitalleşme, kişisel bilgisayar sayısındaki artış, akıllı telefonlar ve elektronik ticaret (e-ticaret) gibi unsurlar etkili olmuştur. İnternet kullanımının artmasıyla beraber de alan adı sayısı artmıştır. Bilgiye erişimde kolaylık sağlayan bu gelişmeler, beraberinde riskleri ve tehditleri meydana getirmiştir. Bunlar tehditlerden birisi "Alan Adı Sistemi Kötüye Kullanımı (*DNS Abuse*)"dır. İnternetin küresel düzeyde bir iletişim aracı olmasından dolayı da DNS Abuse, tüm dünyayı etkileyen bir tehdit olarak algılanmaktadır.

DNS Abuse'un evrensel bir tanımı bulunmamakta ve çeşitli kurum ve kuruluşlar tarafından farklı şekillerde yorumlanmaktadır. Bu konuda çeşitli görüşler olmakla birlikte, alan adı üzerinden kişisel ve finansal bilgilerin ele geçirilmesi, cihazlara zararlı yazılım bulaştırılması gibi güvenlik tehdidi olan unsurlar genel olarak DNS Abuse olarak kabul edilmektedir. Kavram hakkında evrensel bir uzlaşı olmamasının sebebi, yasa dışı içeriklerin DNS Abuse kapsamına dahil edilip edilmeyeceği konusundaki görüş farklılıklarıdır.

DNS Abuse ile mücadele politikaları alan adı sektöründe farklılık gösterebilmektedir. gTLD uzantılı alan adları kapsamında ICANN tarafından genel bir çerçeve oluşturulmuş iken, ccTLD'lerde durum daha farklıdır. ccTLD'lerde DNS Abuse ile mücadele politikası doğrudan kayıt otoritesi tarafından belirlenmektedir.

Bu çalışma; ".tr" uzantılı alan adlarındaki DNS Abuse ile mücadeleye, ".tr" kayıt otoritesi olan Bilgi Teknolojileri ve İletişim Kurumu (BTK) perspektifinden yaklaşmaktadır. Çalışmada sunulacak öneriler ile DNS Abuse'un oluşmasını

[1] Daha fazla bilgi için bkz. (https://www.iab.org/), (31.08.2023)

engellemek ve gerçekleştikten sonra oluşabilecek mağduriyetleri azaltmak için yapılacak çalışmalara katkı sağlanması amaçlanmaktadır.

Tez dört bölümden oluşmaktadır. Tezin ilk bölümünde, DNS Abuse ve ilgili kavramlar olan internet, internet protokolü, alan adı ve alan adı sistemi hakkında bilgi verilmiştir.

Tezin ikinci bölümünde, kayıt otoritesi açısından DNS Abuse tespit etme yöntemleri, DNS Abuse'a karşı uygulanan eylemler ve DNS Abuse ile mücadele yöntemleri açıklanmıştır.

Tezin üçüncü bölümünde, uluslararası kuruluşların DNS Abuse ile mücadelesi incelenmiş, ICANN'in gTLD uzantılı alan adları kapsamında yaptığı çalışmalar, Avrupa Birliği düzeyinde yürürlüğe giren NIS 2 Direktifi ve Avrupa Komisyonu tarafından yayınlanan "DNS Abuse Raporu" hakkında bilgi verilmiştir.

Tezin dördüncü bölümünde, DNS Abuse ile mücadele kapsamında çeşitli ülkeler incelenmiştir. Bu ülkeler; Almanya, Avustralya, Belçika, Danimarka, Hollanda, İngiltere, Kanada ve Türkiye'dir. İncelemeler ccTLD kayıt otoriteleri nezdinde gerçekleştirilmiştir.

Tezin sonuç bölümünde, çalışma boyunca incelenen konular değerlendirilmiş; öneriler bölümünde, ulusal ve uluslararası çalışmalar ışığında ".tr" uzantılı alan adlarında DNS Abuse faaliyetlerinin etkisini azaltmaya yönelik öneriler sunulmuştur.

1. KAVRAMLAR VE TARİHÇE

Bu bölümde ilk olarak internet kavramı ve internetin tarihçesi açıklanacak, sonrasında internet protokolü (*IP*) hakkında bilgi verilecektir. Ardından alan adları; alan adlarının tarihi, alan adlarının yapısı ve alan adları yönetimi alt başlıklarıyla ayrıntılı bir şekilde incelenecektir. Alan adı sistemi (*DNS*) kısmında ise DNS'in bileşenleri tanımlanacak ve işleyişi hakkında bilgi verilecektir. Son olarak, alan adı sisteminin kötüye kullanımı (*DNS Abuse*), yapılan literatür araştırması çerçevesinde incelenecektir.

1.1. İnternet Kavramı ve Tarihçesi

1.1.1. İnternet Kavramı

İnternet kavramı 1930'lu yılların başından itibaren oluşmaya başlamıştır. 1930'lu yıllarda yazar ve fütürist Herbert George Wells, tüm insanlık için eksiksiz bir evrensel hafıza olan "Dünya Beyni *(World Brain)*" fikrini tasarlamıştır. Wells gelecekle ilgili olarak: "Dünyanın herhangi bir yerinde herhangi bir öğrencinin, kendi çalışma odasında projektörüyle birlikte oturup herhangi bir kitabı veya dokümanı bire bir kopyası olarak inceleyebileceği zaman yakındır." demiştir. Wells'in vizyonu İkinci Dünya Savaşı sırasında unutulmasına rağmen savaş sonrası Amerika Birleşik Devletleri (ABD)'nde Vannevar Bush tarafından benzer bir kavram olarak, bilgi depolama ve geri alma makinesi "Memex" tanımlanmıştır (Campbell-Kelly ve Garcia-Swartz, 2013, s.19-20). 1962 yılında ise Joseph Carl Robnett Licklider tarafından, kavram olarak bugünün internetine çok benzeyen; herkesin herhangi bir sitedeki verilere ve programlara hızlı bir şekilde erişebileceğini öne süren "Galaktik Ağ *(Galactic Network)*" kavramı tanımlanmıştır (LEINER Barry M. vd., 1997, s.3).

24 Ekim 1995 tarihine gelindiğinde ise Federal Ağ Konseyi (*Federal Networking Council - FNC)* tarafından internet kavramını tanımlayan bir karar oy birliğiyle kabul edilmiştir. Bu tanım, internet ve fikri mülkiyet hakları topluluklarının üyelerine danışılarak geliştirilmiştir:

> *"İnternet -- (i) İnternet Protokolü (IP) veya sonraki uzantıları/takipçileri temelinde küresel olarak benzersiz bir adres alanı ile mantıksal olarak birbirine bağlanan; (ii) İletim Kontrol Protokolü/İnternet Protokolü(TCP/IP) paketi veya sonraki uzantıları/takipçileri ve/veya diğer IP uyumlu protokolleri kullanarak iletişimi destekleyebilen; ve (iii) iletişim ve ilgili altyapı üzerine katmanlanmış üst düzey hizmetleri kamuya açık veya özel olarak sağlayan, kullanan veya erişilebilir kılan küresel bilgi sistemini ifade eder."* (LEINER Barry M. vd., 1997, s.17).

İnternetin, yaygın olarak kullanılmaya başlandığı 21. yüzyılın başında; İnan (2000) interneti "Birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağı" olarak ifade etmiş, Timisi (2003) ise, "Fiziksel ya da elle tutulur bir araç olmaktan ziyade birbirine bağlı sayısız küçük bilgisayar ağlarından oluşan büyük bir bilgisayar ağı" olarak tanımlamıştır (Doğan, 2014).

Mobil iletişim araçları teknolojisinin gelişmesi ve son yıllarda daha çok gündeme gelen nesnelerin interneti *(Internet of Things – IoT)* kavramının günlük hayatımızdaki yerinin giderek artmasıyla birlikte internet kavramının kapsamı da genişlemiştir. Günümüzde internet; bilgisayar ve diğer akıllı cihazlar aracılığıyla veri ve bilgi iletmeyi/almayı sağlayan bir iletişim ağı olarak da tanımlanabilmektedir.

1.1.2. Tarihçe

İnternet üzerine yapılan çalışmaların başlangıcı İkinci Dünya Savaşı sonuna kadar uzanmaktadır. İkinci Dünya Savaşı'nın sona ermesiyle birlikte ABD ile Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) arasında başlayan "soğuk savaş" dönemi ve SSCB'nin 1949 yılında atom bombası testi yapması sonucu, ABD'de hava savunma sistemleri kapsamında ağ teknolojisine yapılan harcamalar artmıştır. 1957 yılında SSCB tarafından uzaya Sputnik uydusu gönderilmesine karşılık, ABD Savunma Bakanlığı tarafından savunmayla ilgili alanlarda önemli ilerlemeler vaat eden

araştırma projelerini sürdürerek ABD'yi askeri rakiplerinin önünde tutma misyonuyla Gelişmiş Araştırma Projeleri Ajansı *(Advanced Research Projects Agency - ARPA)* kurulmuştur (Campbell-Kelly ve Garcia-Swartz, 2013, s.21).

İnternet üzerine yapılan çalışmalar askeri alanda sınırlı kalmayıp sivil alanda da gerçekleştirilmiştir. 1960'ların başlarında teknolojik açıdan gelişmiş birçok şirkette zaman paylaşımlı sistemler[1] kullanılmaya başlanmıştır. Bu sistemler, kullanıcı kuyruğunda olan kişilere çok hızlı cevap verdiğinden, sisteme aynı anda erişen pek çok kişinin varlığına rağmen her kullanıcının görevine ayrılmış gibi görülmüştür. 1969 yılında ise bir adım ileri gidilerek, bilgisayar kaynaklarının bir ağ üzerinden paylaşılması fikri ARPA tarafından oluşturulan ARPANET ile hayata geçirilmiştir. İlk olarak ABD'deki üniversitelerde zaman paylaşımlı bilgisayarları birbirine bağlayan ARPANET, kısa sürede ABD'deki bilgisayar bilimleri araştırma topluluğu için kritik bir altyapı parçası haline gelmiş ve İleri Savunma Araştırma Projeleri Ajansı (*Defense Advanced Research Projects Agency -DARPA*)[2] tarafından ABD'yi Birleşik Krallık, Norveç, Almanya ve İtalya' daki ağlara bağlamak için kullanılmıştır (Britannica Online Encyclopedia, 2024).

Artan bilgisayar ağı sayısıyla birlikte çeşitli ağlar arası iletişim sorunu da ortaya çıkmıştır. Bu sorun, farklı ağlardaki farklı bilgisayar türlerinin birbirleriyle iletişimine olanak sağlayan Transfer Kontrol Protokolü/İnternet Protokolü (*Transmission Control Protocol - TCP/Internet Protocol - IP*) adı verilen yeni bir iletişim protokolü oluşturulmasıyla çözülmüştür. ARPANET ve Savunma Veri Ağı'nın *(Defense Data Network - DDN)* 1 Ocak 1983'te resmi olarak TCP/IP standardına geçmesiyle de tüm ağların evrensel bir dille birbirine bağlanabilir hale gelmesi adına önemli adım atılmıştır (Online Library Learning Center, 2023).

---

[1] Bir bilgisayar kaynağının, birden fazla kullanıcıyla art arda ve hızlı bir şekilde paylaşılmasına izin veren sistemdir.

[2] 1972 yılında ARPA' nın ismi DARPA olarak değiştirilmiştir.

1990'lı yıllarda internet kullanımı ciddi oranda artmıştır. Hiç kuşkusuz bu artışta, World Wide Web (www)[3] adı verilen yeni bir internet uygulaması ile bu uygulamayı içeren ve çoğu bilgisayar türünde çalışan, "işaretle ve tıkla" arayüzü sayesinde internet üzerinden dosyalara erişimi, dosyaların alınmasını ve görüntülenmesini basitleştiren tarayıcılar etkili olmuştur (Britannica Online Encyclopedia, 2024).

Milenyum adı verilen 2000'li yıllarla birlikte internet kullanımı dünya genelinde yaygınlaşmış, hayatın birçok alanında kullanılan önemli bir olgu haline gelmiştir. Bu artışta kişisel bilgisayar kullanımın yaygınlaşması, internet altyapısının genişlemesi ve internet kullanım fiyatlarındaki düşüş anahtar rol oynamıştır. İlk başlarda akademik çalışmalar ile kamu kurum ve kuruluşları arası iletişim için kullanılan, zamanla ticari faaliyetlerin öznesi hale gelen internetin 2000'li yıllarda eğlence sektörü özelinde ticari yönü ağır basmaya başlamıştır. Kuşkusuz bu değişimde, sosyal medya platformları ile dünya çapında oyuncusu bulunan çevrimiçi bilgisayar oyunlarının payı büyüktür.

2010'lu yıllarda internet hayatın vazgeçilmez bir parçası haline gelmiştir. Mobil internetin yükselişiyle birlikte, akıllı telefonlar ve tabletler aracılığıyla internet erişiminin yaygınlaşması; bulut bilişim, büyük veri ve yapay zekâ gibi teknolojilerin gelişimi; online haber platformları ve elektronik ticaret (e-ticaret) alanında meydana gelen ciddi gelişmeler internetin iş dünyası ve günlük hayat üzerinde önemli etkilere neden olmuştur.

Bugün, internet hemen hemen her sektörde yaygın olarak kullanılmakta ve küresel iletişim, bilgi paylaşımı ve e-ticaret gibi birçok alanda önemli bir rol oynamaktadır. Nesnelerin interneti kavramının günlük hayattaki yerinin giderek artmasıyla da internetin hayatımızdaki öneminin daha da artacağı değerlendirilmektedir.

---

[3] Tim Berners-Lee tarafından Avrupa Nükleer Araştırma Örgütü'nde (CERN) geliştirilen bir dizi erişim protokolü ve görüntüleme standardıdır. Daha fazla bilgi için bkz. (https://www.britannica.com/topic/Web-20), 05.05.2024)

1.2. İnternet Protokolü (Internet Protocol - IP)

İnternet protokolü, ağlar arasında seyahat edebilmeleri ve doğru hedefe ulaşabilmeleri için veri paketlerini yönlendirmek ve adreslemek için kullanılan bir protokol veya kurallar dizisidir. İnternette aktarılan veriler paket adı verilen daha küçük parçalara bölünmektedir. Her pakete IP bilgileri eklenmekte ve bu bilgiler yönlendiricilerin paketleri doğru yere göndermesine yardımcı olmaktadır (Cloudflare, 2024).

Bir IP ağındaki her cihazın tanımlanması IP adresi ile gerçekleşmektedir. IP adresi, internete bağlanan bir cihaza veya alan adına atanan benzersiz bir tanımlayıcıdır. Her IP adresi "192.168.1.1" gibi bir dizi karakterden oluşmaktadır (Kerner, 2021). İnternete bağlı cihazların IP adresleri olduğu gibi internet sitelerinin barındığı sunucuların da IP adresleri bulunmaktadır (ALTINOK, 2019). IP adreslerinin karmaşık karakter dizinlerinden oluşmasından ve akılda tutulmasının zor olmasından dolayı internet siteleri için hatırlaması kolay olan alan adları oluşturulmuş, alan adlarını IP adreslerine çevrilmesi için de DNS geliştirilmiştir. Örneğin "turkiye.gov.tr" nin IP adresi "94.55.118.33"'tür ve tarayıcıdan "turkiye.gov.tr"' ye erişmek istediğimizde asıl erişilen "94.55.118.33" sayılı IP adresidir.

IP, verilerin internette hareket ettiği protokolü tanımlarken, asıl taşımayı yapan ise IP paketidir. Bir IP paketi, adres bilgilerini ve içindeki bilgileri gösteren zarflı bir mektuba benzetilebilmektedir. Bir IP paketinin zarfına başlık adı verilir. Paket başlığı, paketi hedefine yönlendirmek için gereken bilgileri sağlamaktadır. Bir IP paket başlığı en fazla 24 bayt uzunluğundadır ve kaynak IP adresini, hedef IP adresini ve tüm paketin boyutu hakkında bilgi içermektedir. Bir IP paketinin diğer önemli kısmı ise, iletilen içeriği barındıran ve boyutu değişebilen veri bileşenidir (Kerner, 2021).

1.3. Alan Adı

1.3.1 Alan Adlarının Tarihi

Alan adı kavramı ilk olarak Postel ve Zew Sing Su tarafından 1982 yılında yayımlanan "İnternet İçin Alan Adı İsimlendirme Kuralları *(The Domain Naming Convention for Internet)*" adlı eserde açıklanmıştır. 1983 yılında Mockapetris tarafından yayımlanan "Alan Adına İlişkin Kavram ve İmkanlar *(Domain Name-Concepts and Facilities)*" adlı eserde ilk kez alan adının yapısı ve nasıl çalışacağına dair ilkeler ortaya konmuştur (Gürel, 2022, s.8). Yapılan teorik çalışmalardan kısa bir süre sonra, daha sonra dünya genelinde benimsenecek olan ve genel üst düzey alan adı *(general top-level domain - gTLD)* olarak tanımlanan ".com, .org, .net, .int, .gov, .edu ve mil" uzantıları oluşturulmuştur (Soysal, s.203).

1990'lı yılların ortalarında internetin ticarileşmesi ve küreselleşmesi ile birlikte özellikle ".com" uzantılı alan adları tahsisleri ciddi oranda artmıştır. Artan tahsis işlemleriyle birlikte işlemlerin ücretsiz yapılmasına dair politika da değişmiş ve 1995 Eylül ayında Network Solutions Inc. *(NSI)*[4] tarafından ".com, .org, .net, .edu ve .gov" uzantılı alan adları kayıt ve yenileme işlemlerinden ücret alınmaya başlanmıştır. Uygulamaya konan yeni politika sonucu, bu kararın tek başına verilemeyeceği ve konu ile ilgili tüm kesimlerin (son kullanıcılar, servis sağlayıcılar, NSF ve diğer gruplar) dahil olacağı bir zeminde politika oluşturulması gerektiğine dair eleştiri ve değerlendirmeler yapılmıştır (Işıklı, 2001, s.16). Ücret politikası yanında diğer işletim sorunlarına dair eleştiri ve tepkilerin artması üzerine, alan adı sektöründe oluşan tekel piyasaya son vermek ve rekabet ortamının sağlanması adına 1997 yılında ABD Ticaret Bakanlığı tarafından, "E-Ticaret İçin Küresel Çerçeve *(A Global Framework for Electronik Commerce)"* projesi kapsamında çalışmalar başlatılmıştır. Yapılan çalışmalar neticesinde ilerleyen bölümlerde ayrıntılı olarak açıklanacak olan İnternet

[4] Ulusal Bilim Vakfı *(National Science Foundation - NSI*) tarafından alan adı kayıt işlemleri için yetkilendirilen ve 1993-1998 yılları arasında faaliyet gösteren kuruluş.

Tahsisli Sayılar ve İsimler Kurumu (*Internet Corporation for Assigned Names and Numbers - ICANN*) kurulmuştur. ICANN 1998 yılında ABD Ticaret Bakanlığı ile "Mutabakat Zaptı" imzalayarak ABD Hükümeti tarafından resmen tanınmış ve alan adları yönetimi konusunda faaliyete başlamıştır (Gül, 2015, s.15; Gürel, 2022, s.9)

ICANN, 2000 yılında mevcut gTLD'lere ek olarak ".aero, .biz, .coop, .info, .museum, .name ve .pro" uzantılarını oluşturmuş, 2003 yılında ise ".asia, .cat, .jobs, .mobi, .tel, .travel, .post ve .xxx" uzantılarının ilerleyen yıllarda kullanıma sunulması ile sonuçlanacak bir süreç başlatmıştır (ICANN, 2023a; ICANN, 2005, s.5; Soysal, s.200). 2005 yılında yeni gTLD'lerin oluşturulması çalışmaları başlamış, yapılan çalışmalar neticesinde ICANN uhdesinde faaliyet gösteren Jenerik Alan Adları Destek Kuruluşu *(Generic Names Supporting Organization - GNSO)* tarafından 2007 yılında yeni genel üst düzey alan adlarına *(new general top-level domain - ngTLD)* ilişkin politikalar oluşturulmuştur. 2008 yılında ICANN Yönetim Kurulu tarafından politikaların onaylanması ile de new gTLD'lerin oluşturulmasına ilişkin süreç başlamıştır (ICANN, 2023b; Soysal, s.236).

Bu gelişmelerin yanında, ISO 3166[5] ile ülke kısaltmalarından oluşan ve ülke kodu üst düzey alan adları *(Country code top-level domain - ccTLD)* olarak tanımlanan ülke kodları (örn ".us, .uk, .il, .au, .tr vb.") belirlenmiş ve yapılan anlaşmalar neticesinde ilgili ülkelere verilmeye başlanmıştır (Gürel, 2022, s.9).

İlk olarak 1980'li yıllarda kullanılan alan adları yıllar içerisinde önemini, etkisini, kullanım alanlarını ve sayısını arttırmıştır. Bu artışta; internet kullanımının yaygınlaşması, "www" devrimi, tarayıcıların hizmete açılması, kişisel ve firma internet sitesi kullanımı artışı ile forumların yaygınlaşması, dijitalleşmenin hız kazanması ve e-ticaret olgusu etkili olmuştur.

---

[5] Uluslararası Standart Örgütü (*International Standard Organization - ISO*) tarafından ülkeler ve bölgelerine atıfta bulunmak için oluşturulan, uluslararası kabul görmüş harf ve/veya rakam kodlarının listesidir.

Verisign[6] tarafından desteklenen The Domain Name Industry Brief (DNIB)'in, hazırladığı 2023 yılı alan adı sektörü raporuna göre; 2023 yılı sonu itibariyle toplam aktif alan adı sayısı 359,8 milyondur (The Domain Name Industry Brief, 2024). Alan adı sektörünün geldiği bu seviyenin 1980'li yıllarda tahmin edilmesinin zor olduğu değerlendirilmektedir. Gelecekte ise sektörün büyüme devam mı edeceği yoksa çevrimiçi alışveriş ve sosyal medya platformları sebebiyle küçülmeye mi gideceği ilerleyen zamanda gözlemlenebilecektir.

1.3.2 Alan Adlarının Yapısı

DNS hiyerarşik olarak tasarlanmıştır ve alan adı yapısı da bu tasarımı yansıtmaktadır (Yeşil, 2013). Alan adı yapısındaki bu hiyerarşi sağdan sola doğru gerçekleşmektedir. Örneğin trabis.gov.tr. alan adında; hiyerarşide en üst düzey olan ancak kullanımda görülmeyen ve "." olarak temsil edilen kök *(root)* yer almaktadır. Kök'den sonraki "tr" bölümü üst düzey alan adı *(Top Level Domain - TLD)*[7], "gov" bölümü ikinci derece alan adı *(second-level domain - SLD)* "trabis" bölümü ise üçüncü derece alan adı *(third-level domain)* olarak ifade edilmektedir (Chandramouli, Rose, 2013, s.2-2; Gül, 2015, s.7; OECD, 2006, s.20). Bir alan adında yüz yirmi sekize kadar derece oluşabilmektedir (ICANN, 2023c). Tüm bu bölümlerin birleşimi olan trabis.gov.tr. ise Tam Nitelikli Alan Adı *(Fully Qualified Domain Name – FQDN)* olarak ifade edilmektedir[8] (Chandramouli, Rose, 2013, s.2-2).

TLD'ler; ccTLD, gTLD ve teknik altyapı amacıyla kullanılan özel bir TLD olan .arpa olmak üzere üç kategoriye ayrılmaktadır (ICANN, 2023a). Bu üç kategori aşağıda sırasıyla açıklanacaktır.

---

[6] ".com" ve ".net" gibi TLD'lerin kayıt otoritesi olması yanında, on üç kök sunucudan ikisini yöneten kuruluştur. Daha fazla bilgi için bkz. (https://www.verisign.com/en_US/company-information/index.xhtml), (06.05.2024)

[7] Birinci seviye alan adı (first-level domain) olarak da ifade edilebilir.

[8] Bu çalışmada ifade edilen alan adı terimi FQDN'nin karşılığı olarak kullanılmıştır.

1.3.2.1 ccTLD

ccTLD'ler ülkeler ve bölgelerle ilişkili olan ve genellikle iki harften oluşan uzantılardır. Örnek olarak ".tr, .eu, .uk, .us, .香港,.الجزائر., .бел"[9] uzantıları verilebilir. 2024 Nisan ayı itibariyle mevcut sayısı 316 olan bu uzantılar, kayıt otoriteleri tarafından teşkilat yapılarına, ülke mevzuatına, prosedürlere ve kurallara göre yönetilmektedir. Genel olarak ilgili ülke veya bölgede ikamet eden kişiler tarafından alınmakla birlikte, bazı ccTLD uzantılı alan adları ikamet şartı aranmaksızın tahsis edilebilmektedir (IANA, 2024; Yasaman, 2019, s.112). Ayrıca, birçok ccTLD'de "x.eu, x.ca" gibi doğrudan TLD altında alan adı kaydetmek mümkünken bazı ccTLD'lerde "x.com.tr, x.net.uk" gibi ikinci derece alan adı[10] altında alan adı kaydetme imkânı sağlanmaktadır. Bu kapsamdaki ikinci derece alan adları genellikle şirketler için ".com/co", kuruluşlar için ".org", devlet kurumları için ".gov/.gouv/.gob", üniversiteler için ".edu" ve bireyler için ".id/.name/.nom/.me" olarak oluşturulmuştur (OECD, 2006, s.20; Yeşil, 2015, s.48). "com, .co, gov, edu vb." ikinci derece alan adları gTLD olarak da oluşturulmuş iken, ".gouv, .nom, .tsk, .pol, .kep" gibi gTLD olmayan ikinci derece alan adları da mevcuttur.

1.3.2.2 gTLD

gTLD'ler en az üç karakter içeren, coğrafi konumla sınırlı olmayıp herkes tarafından kayıt edilebilen ve kendi içerisinde sponsorlu ve sponsorsuz olarak sınıflandırılan uzantılardır (Karakoç, 2022). Sponsorlu gTLD'lerin yönetimi ICANN ile yapılan sözleşmeye bağlı olarak sponsor kuruluşlar tarafından daha serbest bir şekilde gerçekleştirilmektedir. Bu gTLD'lere örnek olarak ".edu, .gov, .int, .aero, .museum" verilebilir. Sponsorsuz gTLD'lerin yönetimi üzerinde ise ICANN'in daha fazla etkisi bulunmaktadır. Bu uzantıların yönetimi ICANN ile yapılan sözleşmeye bağlı olarak

---

[9] 2009 yılından itibaren farklı alfabelerdeki karakterler, Uluslararasılaştırılmış Alan Adı (*Internationalized Domain Names - IDN*) kapsamında kullanılmaya başlamıştır. Daha fazla bilgi için bkz. (https://www.icann.org/resources/pages/idn-2012-02-25-en), (31.08.2023)

[10] ".tr" uzantılı alan adlarına ilişkin mevzuatta "alt alan adı" olarak tanımlanmıştır.

yetkilendirilen kayıt otoriteleri tarafından gerçekleştirilmektedir. Bu gTLD'lere örnek olarak ".com, .net, .biz, .org, .wiki, .机构, .بازار., .москва" verilebilir (Soysal, s.201).

Alan adı sektöründe rekabet ortamını oluşturmak, yenilikleri desteklemek ve seçenekleri artırmak amacıyla 2005 yılında başlayan yeni gTLD oluşturma çalışmaları, 2008 yılında ICANN Yönetim Kurulu tarafından GNSO'nun new gTLD'lere ilişkin geliştirdiği politika önerilerini kabul etmesiyle önemli bir noktaya gelmiştir. GNSO tarafından 2011 yılında yayımlanan ve ICANN Yönetim Kurulu tarafından onaylanan "gTLD Uygulama Rehberi *(gTLD Applicant Guidebook)*[11]" ile birlikte de "new gTLD Programı" resmen başlamıştır (ICANN, 2023b; Soysal, s.236).

New gTLD başvuru süreci 12 Ocak 2012 - 30 Mayıs 2012 tarihleri arasında gerçekleştirilmiştir. Bu süre içerisinde 1.409 adet ad için toplam 1.930 adet başvuru yapılmıştır. ICANN, ilk değerlendirme sonuçlarını 22 Mart 2013'te yayınlamış, Ekim 2013'te de ilk new gTLD'ler, başvurusu onaylanan taraflara tahsis edilmiştir[12](ICANN, 2023b; Soysal, s.237). New gTLD'lere örnek olarak ".wiki, .istanbul, .bank, .online, .shop" verilebilir.

2000'li yıllarda 22 olan gTLD sayısı new gTLD programı ve Uluslararasılaştırılmış Alan Adı (*Internationalized Domain Names - IDN*) ile birlikte yıllar içerisinde artmış ve 2024 Nisan ayı itibariyle 1.263 olmuştur (IANA, 2024).

1.3.2.3. arpa

ccTLD ve gTLD'lerin yanı sıra özel bir TLD olarak ".arpa" oluşturulmuştur. ".arpa" yalnızca teknik altyapı amacıyla kullanılmakta ve yönetimi İnternet Mimari Kurulu

[11] gTLD Uygulama Rehberi'nin(gTLD Applicant Guidebook) 2012 Haziran itibariyle nihai hali için bkz. https://newgtlds.icann.org/sites/default/files/guidebook-full-04jun12-en.pdf, (31.08.2023)
[12] ngTLD'ler için sponsorluk sistemi uygulanmamıştır.

(Internet Architecture Board - IAB)[13] ile IANA tarafından iş birliği içerisinde gerçekleştirilmektedir (IANA, 2023; ICANN, 2023a).

1.3.3. Alan Adları Yönetimi

Bu bölümde ilk olarak ICANN hakkında bilgi verilecek, ardından gTLD ve ccTLD'lerin yönetimi; ICANN, kayıt otoriteleri ve kayıt kuruluşları kapsamında açıklanacaktır.

1.3.3.1. ICANN

ICANN 1998 yılında Kaliforniya yasalarına göre kurulmuş, kar amacı gütmeyen ve kamu yararına çalışan bir özel sektör kuruluşudur. Uluslararası kamu hukuku kapsamında kurulmuş uluslararası bir örgüt olmamasına rağmen, yaptığı düzenlemelere göre birçok ülkedeki kuruluş ve kişilerin yanı sıra hükümetlerle de iş birliği yapmasının zorunlu olması bakımından, uluslararasıdır bir örgüt olarak kabul edilmektedir (Weitzenboeck, 2014, s.50).

ICANN'in misyonu, internetin benzersiz tanımlayıcı sistemlerinin *(unique identifier systems)* istikrarlı ve güvenli bir şekilde çalışmasını sağlamaktır. ICANN misyonu özellikle:

- Kök'te yeni uzantıların oluşturulması ve ilgili tarafların yetkilendirilmesi ile gTLD kapsamında ikinci derece alan adlarının tahsisine ilişkin politikaların geliştirilmesini ve uygulanmasını koordine etmek,
- DNS'teki kök sunucu sisteminin işleyişinin ve gelişiminin koordinasyonuna olanak sağlamak,
- IP adreslerinin ve otonom sistem numaralarının en üst düzeydeki tahsisini ve atamasını koordine etmek,

[13] Daha fazla bilgi için bkz. (https://www.iab.org/), (31.08.2023)

- IP standartları geliştirme kuruluşları tarafından belirtildiği şekilde internetin işleyişi için gerekli olan kayıtları sağlamak üzere diğer kurumlarla iş birliği yapmaktır (Gül, 2015, s.15; ICANN, 2022a).

ICANN; Topluluk *(Community)*, Yönetim Kurulu *(Board of Directors)* ve Personel Kadrosu *(Staff)* olmak üzere üç temel yapı üzerine organize edilmiştir. Çeşitli grupları temsil eden Topluluk, ICANN'in politikalarını geliştirmektedir. Yönetim Kurulu, Topluluk tarafından geliştirilen politikaları incelemekte ve politikaların uygulanmasına dair nihai kararı vermektedir. Personel Kadrosu ise politika geliştirmede Topluluğa idari ve maddi destek sağlamakta ve ICANN Yönetim Kurulu tarafından onaylanan politikaları uygulamaktadır (ICANN, 2019a).

ICANN Topluluğu temel olarak konuya özel politikalar geliştiren üç Destek Kuruluşundan ve bu politikalar ve daha kapsamlı ICANN faaliyetleri hakkında tavsiyelerde bulunan dört Danışma Komitesinden oluşmaktadır (ICANN, 2019a).

ICANN Destek Kuruluşları şunlardır:

- **Genel Adları Destekleme Kuruluşu (*Generic Names Supporting Organization - GNSO*):** Kayıt otoritelerini, kayıt kuruluşlarını, işletmeleri, fikri mülkiyet ile ilgili kuruluşları, internet servis sağlayıcılarını, ticari faaliyette bulunmayan kuruluşları ve kullanıcıları bir araya getirerek gTLD'lere ilişkin politikalar geliştiren kuruluştur. Kişiler ve kuruluşlar GNSO'ya direk katılamamakta, bunun yerine GNSO'yu oluşturan paydaş gruplarından veya seçim bölgelerinden birine katılabilmektedirler. GNSO politikalarının birçoğunun, ICANN ile sözleşmeye dayalı ilişkisi olan kayıt otoriteleri ve ICANN tarafından akredite edilen kayıt kuruluşları üzerinde doğrudan etkisi bulunmaktadır.
- **Ülke Kodu Adlarını Destekleme Kuruluşu (*Country Code Names Supporting Organization - ccNSO*):** ccTLD yöneticilerine, ccTLD'leri ilgilendiren güncel sorunları küresel bir perspektiften bakmak ve tartışmak için

bir ortam sağlayan kuruluştur. Ayrıca, IDN ve ccTLD'lerin tanıtılması gibi ccTLD'lerle ilgili konular kapsamında, ICANN Yönetim Kurulu'na küresel politikalar geliştirmek ve önermekten de sorumludur.

- **Adres Destekleme Kuruluşu (*Address Supporting Organization - ASO*):** IP adres politikasına ilişkin tavsiyeleri gözden geçiren ve geliştiren, Bölgesel İnternet Tescil Kurumu *(Regional Internet Registry - RIR)*[14] topluluklarıyla birlikte ICANN Yönetim Kurulu'na numara kaynak tahsisi politikası konusunda tavsiyelerde bulunan kuruluştur (ICANN, 2019a; ICANN, 2023e).

Danışma Komiteleri şunlardır:

- **At-Large Danışma Komitesi (*At-Large Advisory Committee - ALAC*):** Bireysel internet kullanıcılarının menfaatleriyle ilgili olarak ICANN'in faaliyetleri ve politikaları hakkında tavsiyelerde bulunan komitedir.
- **Hükümet Danışma Komitesi (*Governmental Advisory Committee - GAC*):** ICANN'in faaliyet ve politikalarının ulusal yasalar, uluslararası anlaşmalar ve kamu politikası meseleleriyle ilgili olduğu durumlarda, hükümetlerin endişeleriyle ilgili olan ICANN faaliyetleri ve politikaları hakkında tavsiyelerde bulunan komitedir. GAC üyeleri; ulusal hükümetlerin ve hükümetler arası kuruluşların resmi olarak tanınan temsilcilerinden oluşmaktadır.
- **Güvenlik ve İstikrar Danışma Komitesi (*Security & Stability Advisory Committee - SSAC*):** İnternet adlandırma ve adres tahsis sistemlerinin güvenliği ve bütünlüğü ile ilgili konularda ICANN Topluluğu'na ve Yönetim Kurulu'na tavsiyelerde bulunan, istikrar ve güvenliğe yönelik temel tehditlerin kaynaklarını değerlendirmek için internet adlandırma ve adres tahsisi hizmetlerinin sürekli tehdit değerlendirmesi ve risk analiziyle ilgilenen ve ICANN Topluluğu'na buna göre tavsiyelerde bulunan komitedir.

---

[14] İnternet numara kaynaklarını (IP adresleri ve Otonom Sistem numaraları) yöneten, dağıtan ve kaydeden kurumlardır.

- **Kök Sunucu Sistemi Danışma Komitesi (*Root Server System Advisory Committee - RSSAC*):** Kök sunucu sisteminin işleyişi, yönetimi, güvenliği ve bütünlüğü ile ilgili konularda ICANN Topluluğu'na ve Yönetim Kurulu'na tavsiyelerde bulunmaktan sorumlu olan komitedir (ICANN, 2019a; ICANN, 2023e).

Destek Kuruluşları ve Danışma Komitelerine ek olarak Teknik İrtibat Grubu *(Technical Liaison Group - TLG)* Topluluğun bir parçasıdır. TLG, Avrupa Telekomünikasyon Standartları Enstitüsü *(European Telecommunications Standards Institute - ETSI)*, Uluslararası Telekomünikasyon Birliği Telekomünikasyon Standardizasyon Sektörü *(International Telecommunications Union's Telecommunication Standardization Sector - ITU -T)*, World Wide Web Konsorsiyumu *(World Wide Web Consortium - W3C)* ve IAB olmak üzere dört kuruluştan oluşmaktadır. TLG kuruluşlarının rolü, teknik bilgi ve rehberliği ICANN Yönetim Kuruluna ve diğer ICANN kuruluşlarına aktarmaktır (ICANN, 2019a; ICANN, 2022a).

Topluluğun bir diğer parçası olan Aday Belirleme Komitesi *(Nominating Committee - NomCom)*, Yönetim Kurulu'nun yanı sıra ALAC, ccNSO Konseyi ve GNSO Konseyi de dahil olmak üzere önemli ICANN üyelerini seçmekle görevli bağımsız bir komitedir. NomCom, ICANN Yönetim Kurulu'ndan, Destekleyici Kuruluşlardan ve Danışma Komitelerinden bağımsız olarak çalışacak şekilde tasarlanmıştır (ICANN, 2023e).

ICANN Yönetim Kurulu, 16'sı oy kullanma hakkına sahip Direktörlerden, 4'ü oy kullanma hakkı olmayan İrtibat Görevlilerinden olmak üzere 20 üyeden oluşmaktadır. ICANN Yönetim Kurulu'ndaki Direktörler:

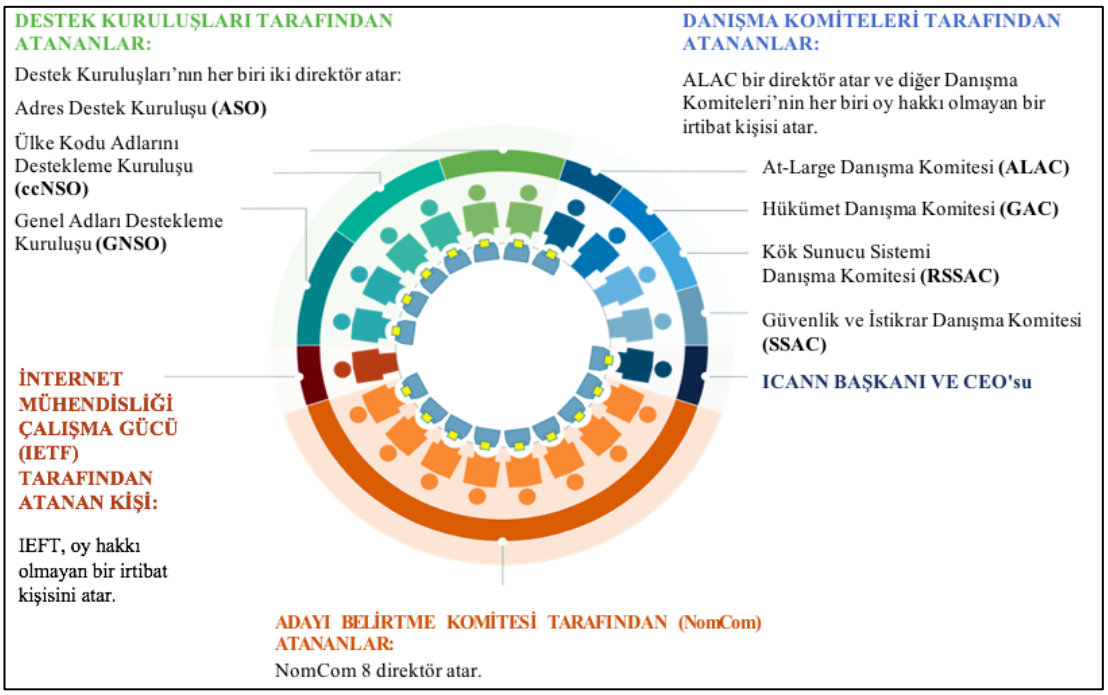
- GNSO tarafından aday gösterilen 2 kişi,
- ccNSO tarafından aday gösterilen 2 kişi,
- ASO tarafından aday gösterilen 2 kişi,
- ALAC tarafından aday gösterilen 1 kişi,

- NomCom tarafından seçilen 8 kişi,
- ICANN Başkanı ve CEO'sundan oluşmaktadır.

Oy hakkı olmayan 4 İrtibat Görevlisi aşağıdaki gruplar tarafından belirlenmektedir:

- GAC tarafından atanan 1 kişi,
- SSAC tarafından atanan 1 kişi,
- RSSAC tarafından atanan 1 kişi,
- IETF[15] tarafından atanan 1 kişi (ICANN, 2022a).

Şekil 1.1. ICANN Yönetim Kurulu Şeması



Kaynak: ICANN, 2022

[15] İnternet Mühendisliği Görev Gücü *(The Internet Engineering Task Force - IETF)*, internet için standart geliştiren bir organizasyonudur. IETF, genellikle internet kullanıcıları, ağ operatörleri ve ekipman satıcıları tarafından benimsenen gönüllü standartları oluşturmaktadır. Daha fazla bilgi için bkz. (https://www.ietf.org/about/introduction/), (29.01.2024)

ICANN Yönetim Kurulu üyeleri çeşitli Topluluk gruplarından seçildiğinden Topluluğun bir parçası olarak kabul edilebilirler. Ancak, ICANN Yönetim Kurulu üyeleri kendilerini atayan kuruluşları temsil etmemektedirler (ICANN, 2019a).

1.3.3.2. ccTLD Yönetimi

Küresel ccTLD politikasının tarihi DNS'in geliştirilmesiyle başlamıştır (Yu, 2004). İlk zamanlarda ccTLD yönetimi için başvuru işlemleri, Postel[16] tarafından Kaliforniya Üniversitesi Bilgi Bilimleri Enstitüsü'nde yürütülmüştür. Başvurunun kabul görmesi durumunda ccTLD delegasyonu için, alan adlarının yönetiminde yetki ve teknik uzmanlığa sahip olarak tanımlanan "Sorumlu kişi" kullanılmıştır (Yeşil, s.10-11). 1990'ların ortalarına gelindiğinde, neredeyse tüm mevcut ülkelerin ccTLD'leri Postel tarafından devredilmiştir. Postel çoğu ccTLD'yi yazılı anlaşmalar olmaksızın ilk başvuran kişiye devretmiştir (Yeşil, 2013, s.30; Yu, 2004, s.390-391).

Alan adları yönetiminin ICANN'e geçmesinden sonra, ICANN Yönetim Kurulu tarafından bireylerin artık ccTLD'ler için delege olmasına izin verilmemesine karar verilmiştir (ICANN, 2011, s.14).

Eylül 2000'de ICANN Yönetim Kurulu tarafından, ccTLD kayıt otoriteleri ile sponsorluk anlaşmalarının yapılması zorunlu kılınmıştır (ICANN, 2011, s.14). ICANN'in ccTLD kayıt otoriteleri ile bir sözleşme üzerinde anlaşmaya varma girişimleri birkaç kayıt otoritesi ile yapılan anlaşmalar dışında başarısız olmuştur. Kayıt otoritelerinin reddetme nedenleri arasında; sözleşmedeki ödeme yükümlülükleri ile bazı hükümetlerin, ICANN'in kendi ülke kodlarının kayıt otoriteleri üzerindeki yetkisinden duyduğu hoşnutsuzluk yer almaktadır (Frankel, 2004, s.482-483). Ayrıca, ccTLD kayıt otoritelerinin ICANN ile sözleşme ilişkisine girmekten kazanacakları çok

[16] İnternetin yaratılmasında önemli bir rol oynayan ABD'li bilgisayar bilimci. Daha fazla bilgi için bkz. (https://icannwiki.org/Jon_Postel), (10.10.2023)

az şey vardır çünkü ülke kodları zaten kökte yer almaktadır ve ICANN'in bunları geri çekme konusunda net bir yetkisi bulunmamaktadır (Yeşil, 2013, s.16).

ICANN, ccTLD'lerle olan ilişkisini resmileştirmek için başka stratejiler de izlemiştir. Şu anda iki farklı yöntem bulunmaktadır: "Hesap Verebilirlik Çerçevesi"ni imzalamak ve resmi mektup alışverişinde bulunmak (Yeşil, 2013, s.16). 2006 yılından bu yana 47 ccTLD kayıt otoritesi mektup alışverişini tercih ederken, 30 ccTLD kayıt otoritesi hesap verebilirlik çerçevesini imzalamayı tercih etmiştir (ICANN, 2022b). ICANN ve ccTLD'ler bu yöntemler ile birbirlerine karşı yasal olarak sorumlu olmayacak şekilde ilişkilerini resmileştirmek istemiştir (Yeşil, 2013, s.16).

Birçok ccTLD kayıt otoritesi yukarıda bahsedilen iki yöntemden birini tercih etmiştir. Yine de çoğu ccTLD kayıt otoritesi yerellik[17] ilkesini benimsemiştir (Weitzenboeck, 2014, s.60). Yerellik ilkesi çerçevesinde, ccTLD yönetimine ilişkin olarak ilgili kayıt otoritelerinin ICANN'e karşı bir sorumluluğu bulunmamaktadır.

ccTLD kayıt otoriteleri, tahsis modellerinde ve kimlerin alan adlarını tahsis edebileceğine ilişkin politikalarında farklılaşmışlardır. Tahsis modelleri; belgeli, belgesiz, belgeli ve belgesizin birlikte uygulandığı karma model olarak sınıflandırılabilirken, alan adı sahiplerine ilişkin olarak; ülkede yerleşik olan veya olmayan şeklinde sınıflandırma yapılabilmektedir.

Bir ccTLD'nin yönetimi ilgili ccTLD kayıt otoritesi tarafından yürütülse de son kullanıcıların alan adına ilişkin işlemleri genel olarak kayıt otoriteleri tarafından yetkilendirilen kayıt kuruluşları vasıtasıyla yapılmaktadır. Yetkilendirilen kayıt kuruluşları faaliyetlerini ilgili ccTLD kayıt otoritesinin düzenlemelerine göre

[17] ccTLD politikasının, küresel etkiye sebep olmadığı sürece yerelde/ülke içerisinde belirlenmesidir. Daha fazla bilgi için bkz. (https://archive.icann.org/en/committees/gac/gac-cctld-principles.htm), (23.09.2023)

yürütmekte ve alan adı işlemleri bu çerçevede gerçekleştirilmektedir (Weitzenboeck, 2014, s.61).

1.3.3.3. gTLD Yönetimi

gTLD yönetimi sözleşmelerden oluşan bir ağa dayanmaktadır. Bu ağda taraflar sırasıyla; ICANN, kayıt otoriteleri ve kayıt kuruluşlarıdır (Weitzenboeck, 2014, s.54).

ICANN, gTLD'nin yönetiminde bir sözleşme portföyü kullanmaktadır. ICANN'in gTLD sözleşmeleri incelendiğinde, uzantının sponsorlu olup olmamasına bağlı olarak değişen, standart bir sözleşme kullandığı görülmektedir. Bu standart format kullanımı new gTLD Kayıt Otoritesi Yetki Sözleşmesi (*Registry Agreement - RA*) için de geçerlidir. ICANN ayrıca, gTLD kayıt kuruluşlarıyla "Kayıt Kuruluşu Akreditasyon Sözleşmesi *(Registrar Accreditation Agreement - RAA)*" yoluyla sözleşmeye dayalı bir ilişki kurmaktadır. Bu sözleşmeler, akredite kayıt kuruluşları için yükümlülükler içermekte ve kayıt kuruluşları sözleşmede belirlenen çerçevede faaliyetleri gerçekleştirmektedir (Weitzenboeck, 2014, s.55) ICANN'e akredite olmayan kayıt kuruluşları ise gTLD uzantılı alan adlarına ilişkin hizmet verememektedir (ICANN, 2023d).

Sözleşmeler ağına dayanan gTLD yönetiminin merkezinde ICANN yer almaktadır. gTLD kapsamında hizmet sunan kayıt otoritesi ve kayıt kuruluşları ile gTLD uzantılı alan adı kaydettirmek isteyen son kullanıcıların genel olarak ICANN tarafından belirlenen şartları kabul etmekten başka seçeneği bulunmamaktadır (Weitzenboeck, 2014, s.59). ccTLD kayıt otoritelerinin aksine gTLD kayıt otoriteleri ve kayıt kuruluşları, ICANN ile yaptıkları sözleşme sebebiyle ICANN'e karşı sorumlu olmakta ve faaliyetlerini bu çerçevede gerçekleştirmektedir.

1.4. Alan Adı Sistemi (Domain Name System - DNS)

Bu bölümde daha önce ifade edilen ancak açıklaması yapılmayan DNS hakkında bilgi verilecektir.

Bölüm 1.2.'de anlatıldığı üzere internet üzerindeki cihazlar birbirleriyle IP adresleri aracılığıyla iletişim kurmaktadır. Bilgisayar, cep telefonu, tablet vb. cihazların IP adresleri olduğu gibi internet sitelerinin bulunduğu sunucuların da IP adresleri bulunmaktadır. IP adreslerinin karmaşık karakter dizinlerinden oluşmasından ve akılda tutulmasının zor olmasından dolayı da ayırt edilmesi ve akılda tutulması kolay olan alan adları oluşturulmuştur. Alan adları ile IP adreslerinin eşleşmesi için de hiyerarşik yapıya sahip olan DNS geliştirilmiştir.

DNS'in temel olarak dört bileşeni bulunmaktadır; "yinelemeli çözümleyici *(recursive resolver*[18]*)*, kök sunucu *(root server),* TLD sunucu *(TLD server)* ve yetkili ad sunucu *(Authoritative name server)*". Bu dört bileşen aşağıda kısaca açıklanmıştır:

- **Yinelemeli çözümleyici:** Alan adı isteklerini alan ve DNS'i kullanarak alan adı IP adres bilgisini elde etmek için gerekli ağ sorgularını gerçekleştiren sunucudur. Dünyada binlerce yinelemeli çözümleyici sunucusu vardır ancak çoğu kişi internet servis sağlayıcıları tarafından yönetilen özyinelemeli çözümleyici sunucularını kullanmaktadır.
- **Kök sunucu:** DNS hiyerarşisinin en üstünde yer alan ve TLD bilgilerine sahip olan sunucudur. Dünya çapında ICANN, Verisign, ABD Savunma Bakanlığı *(US Department of Defense - NIC)* ve RIPE gibi on iki farklı kurumun yönettiği toplam on üç tane[19] kök sunucu bulunmakla birlikte, yoğunluk ve yakınlığa göre dağıtmak için kullanılan Anycast mimari sayesinde dünya üzerinde altı yüzden fazla kök sunucu bulunmaktadır. Kök sunucular, yinelemeli

[18] DNS resolver, DNS recursor, recursive DNS ve recursive server olarak da ifade edilmektedir.
[19] Tüm liste için bkz. https://www.iana.org/domains/root/servers (03.09.2023)

çözümleyiciden bir sorgu aldığında alan adının TLD'sini kontrol edip, eğer mevcut ise ilgili TLD sunucu bilgisini yinelemeli çözümleyiciye iletmektedir.

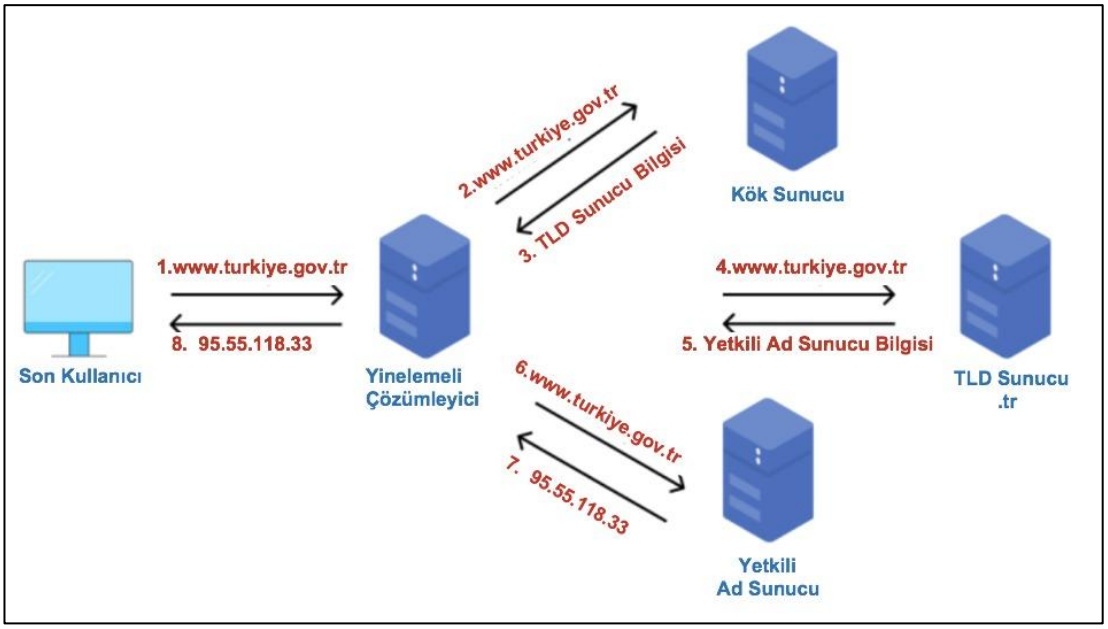
- **TLD Sunucu:** Yönetilen TLD uzantılarına ait alan adı bilgilerine sahip olan ve TLD kayıt otoriteleri tarafından yönetilen sunuculardır. TLD sunucu, yinelemeli çözümleyiciden bir sorgu aldığında alan adını kontrol edip, eğer alan adı ve alan adı yetkili ad sunucu bilgisi mevcut ise ilgili yetkili ad sunucu bilgisini yinelemeli çözümleyiciye iletmektedir.
- **Yetkili ad sunucu:** Yönetilen alan adı IP adres bilgisine sahip olan sunucudur. Yetkili ad sunucu, yinelemeli çözümleyiciden bir sorgu aldığında alan adının IP adres bilgisini kontrol edip bu bilgiyi yinelemeli çözümleyiciye iletmektedir (Bellon, 2023; Cloudflare, 2023; ICANN, 2023ç; Hasna, 2023)

DNS bileşenlerine ilişkin verilen bilgiler ışığında DNS'in nasıl çalıştığı, örnek üzerinden adımlar halinde açıklanacaktır.

1. İlk olarak son kullanıcı tarafından ilgili internet sitesine erişmek için tarayıcı arama motoruna alan adı bilgisi girilir.
2. Ardından gelen sorguya karşılık yinelemeli çözümleyici tarafından önbelleği *(cache)* kontrol edilir. Önbellekte daha önce yapılan sorgulara binaen alan adı IP adres bilgisi mevcut ise tarayıcıya IP adres bilgisi iletilir ve internet sitesine erişim sağlanır, mevcut değilse alan adı sorgusu kök sunucuya iletilir.
3. Kök sunucu tarafından cevap olarak; TLD kayıt otoritesinin yönettiği ilgili alan adının uzantısına ait (".tr, .com, .org, .uk vb.") TLD sunucu bilgisi yinelemeli çözümleyiciye iletilir.
4. Sonrasında yinelemeli çözümleyici tarafından alan adı sorgusu, kök sunucudan iletilen bilgiye karşılık TLD sunucusuna iletilir.
5. TLD sunucu tarafından cevap olarak; ilgili alan adının IP adres bilgisinin mevcut olduğu yetkili ad sunucu bilgisi yinelemeli çözümleyiciye iletilir.
6. Daha sonra yinelemeli çözümleyici tarafından alan adı sorgusu, TLD sunucudan iletilen bilgiye karşılık yetkili ad sunucusuna iletilir.

7. Yetkili ad sunucusu cevap olarak; ilgili alan adına ait IP adres bilgisini yinelemeli çözümleyiciye iletilir.
8. Son olarak yinelemeli çözümleyici tarafından ilgili alan adı IP adres bilgisi tarayıcıya iletilir ve web sitesine erişim sağlanır (Amazon, 2023).

Şekil 1.2. Alan Adı Çözümleme Süreci



Kaynak: Elshazly, 2023

Yukarıda belirtilen işlemler çok kısa sürede gerçekleşmektedir. İnternet sitesine hızlı bir şekilde erişme imkânı sunan DNS'in aynı ölçüde güvenli olduğunu söylemek zordur. Çünkü, yinelemeli çözümleyici kendisine gelen cevapların doğruluğunu kontrol etmemektedir. 1990'lı yıllarda internet kullanımın artması ile başlayan DNS güvenlik sorunu günümüzde internet kullanımının yaygınlaşması ve dijitalleşmenin hız kazanmasıyla çok daha önemli bir hal almıştır.

1.5. Alan Adı Sisteminin Kötüye Kullanımı (DNS Abuse)

Güvenli ve emniyetli bir DNS; kişiler, kurumlar ve ülkeler için büyük önem arz etmektedir. Genel olarak DNS Abuse olarak adlandırılan DNS üzerindeki kötü amaçlı kullanımlar, çevrimiçi güvenliği etkileyen ciddi bir sorundur.

DNS Abuse'un üç tarafı bulunmaktadır. Bunlar; saldırgan, mağdur edilen ve aracı kurumdur. Saldırgan, kötü amaçla alan adı tahsis eden veya meşru amaçla tahsis edilmiş alan adlarını üzerinden kötü amaçlı faaliyetlerini gerçekleştiren kişidir. Mağdur edilen, DNS Abuse faaliyetinden dolayı zarar gören taraftır. Aracı kurum, DNS'in ve internetin doğası gereği DNS Abuse faaliyetine aracılık eden taraftır. Kayıt otoriteleri, kayıt kuruluşları, yer sağlayıcıları[20] ve internet servis sağlayıcıları gibi internet aktörleri aracı kurumlar arasında yer almaktadır. Bu aktörler DNS Abuse ile mücadelede önemli rol oynamaktadır (European Commission, 2022, s.34-35)

DNS Abuse'un küresel çapta kabul edilmiş bir tanımı ve kapsamı bulunmamaktadır. Literatürde yapılan incelemede, DNS Abuse kavramına farklı anlamlar verildiği veya aynı anlamına gelen benzer kavramların kullanıldığı gözlemlenmiştir.

İnternet ve Yargı Politikası Ağı *(The Internet & Jurisdiction Policy Network)*[21] tarafından hazırlanan bir raporda DNS Abuse ile ilişkili olarak; alan adı kaydı kötüye kullanımı ve alan adının kötüye kullanımı olarak geleneksel bir ayrım olduğu belirtilmiştir. Alan adı kaydı kötüye kullanımı ile ilgili ayrıntı verilmemiş, kayıt otoriteleri ve kayıt kuruluşları tarafından gerçekleştirilen alan adı ile ilgili temel faaliyetlere ilişkin olduğuna dair bilgi verilmekle yetinilmiştir. DNS Abuse yerine kullanılabilecek olan alan adı kötüye kullanımı ise teknik kötüye kullanım ve kötü amaçlı içerik olarak ikiye ayrılmıştır (The Internet & Jurisdiction Policy Network,

---

[20] Yer sağlayıcı; internet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileridir

[21] İnternet ve Yargı Yetkisi Politika Ağı, sınır ötesi internet ile ulusal yargı yetkileri arasındaki çatışmayı ele alan çok paydaşlı bir kuruluştur. Daha fazla bilgi için bkz. (https://www.internetjurisdiction.net/about/mission), (03.04.2024)

2019, s.7). Teknik kötüye kullanım kendi içerisinde sınıflandırılmış ancak belirtilen türlerle sınırlı olmadığı ve farklı şekillerle de teknik kötüye kullanımın yapılabileceği ifade edilmiştir. Kötü amaçlı içerik de aynı şekilde kendi içerisinde sınıflandırılmış ve yapılan sınıflandırmanın çeşitli kaynaklardan yararlanılarak oluşturulduğu ve kesin tanımlar olarak sunulmadığı ifade edilmiştir (The Internet & Jurisdiction Policy Network, 2019, s.20-21). Teknik kötüye kullanım ve kötü amaçlı içerik türleri ve açıklamaları aşağıda yer almaktadır:

Teknik Kötüye Kullanım

- **Kötü Amaçlı Yazılım (*Malware*):** Kullanıcının izni olmadan bir cihaza kurulan, cihazın işlemlerini bozan, hassas bilgileri toplayan ve/veya sistemlerine erişim sağlayan kötü niyetli yazılımdır. Kötü amaçlı yazılım; virüsleri, casus yazılımları, fidye yazılımları ve diğer istenmeyen yazılımları içermektedir.
- **Kimlik Avı/Oltalama (*Phishing*):** Kullanıcının hassas, kişisel, kurumsal veya finansal bilgilerini (örneğin hesap numaraları, şifreleri vb.) elde etmek amacıyla kullanılan bir yöntemdir. Bu yöntem, sahte elektronik postalar göndererek veya son kullanıcıları taklit internet sitelerine çekerek gerçekleştirilebilir. Bazı kimlik avı/oltalama saldırıları, son kullanıcının kötü amaçlı yazılımı yüklemesini sağlamak amacıyla da yapılmaktadır.
- **Site Trafiği Yönlendirme (*Pharming*):** Saldırganın, yetkili ad sunucuyu ele geçirerek ilgili IP adresini değiştirmesi veya kullanıcının cihazına yüklediği kötü amaçlı yazılımla internet trafiğini manipüle etmesi sonucu kullanıcının sahte sitelere veya hizmetlere yönlendirilmesidir.
- **Köle Bilgisayar Ağları (*Botnets*):** Kötü amaçlı yazılım bulaştırılmış ve uzaktaki bir yöneticinin kontrolü altında faaliyetler gerçekleştirmesi emredilmiş internet bağlantılı bilgisayar topluluğudur.
- **İstenmeyen Elektronik Posta (*Spam*):** Elektronik posta alıcısının istemediği ve büyük ölçüde aynı içeriğe sahip olan elektronik postalardır. İstenmeyen

elektronik posta ile kimlik avı/oltalama veya site trafiği yönlendirme saldırıları gerçekleştirilebilir. Ayrıca, içeriğinde kötü amaçlı yazılım bulunabilir.

- **Hızlı Akış Barındırma (*Fast-Flux Hosting*):** Alan adı IP adreslerinin ve DNS kayıtlarının sürekli olarak değiştirilerek internet sitelerinin veya diğer internet hizmetlerinin konumunu gizlemek ve tespit edilmesini zorlaştırmak için kullanılmaktadır. Bu yöntemle kötü amaçlı alan adlarının yayın süresi daha uzun olabilmektedir (The Internet & Jurisdiction Policy Network, 2019, s.20).

Kötü Amaçlı İçerik

- **Çocuk İstismarı Materyali:** Suçlu tarafından çekilen ve bir çocuğun cinsel istismarını gösteren fotoğraf veya videolardır.
- **Satışa veya Ticarete Yönelik Kontrole Tabi Maddeler ve Denetime Tabi Mallar:** Yasa dışı uyuşturucuları, yasal uyuşturucuların yasa dışı satışını, yasa dışı hizmetleri, çalıntı malları ve yasa dışı ateşli silahları veya diğer silahları içermektedir. Belirli bir maddenin veya malın yasallığı yargı bölgelerine göre değişebilmektedir.
- **Aşırılık Barındıran Şiddet İçeriği:** Şiddet eylemlerini gösteren, şiddet eylemlerini teşvik eden, bir terör örgütünü veya eylemlerini destekleyen veya insanları bu tür gruplara katılmaya teşvik eden içeriktir.
- **Nefret Söylemi:** Ulusal, ırksal veya dini nefreti teşvik eden ve ayrımcılığa, düşmanlığa veya şiddete tahrik eden ifadeleri içermektedir.
- **Fikri Mülkiyet Hakları İhlali:** Sahte ürün satışı, patent veya ticaret sırrı ihlali, telif hakkı ihlali gibi iddialara sebep olan içeriklerdir (The Internet & Jurisdiction Policy Network, 2019, s.21).

İnternet ve Yargı Politikası Ağı tarafından yapılan çalışmaya benzer bir çalışma Avrupa Komisyonu tarafından daha kapsamlı olarak yayınlanmıştır. Bu çalışmada DNS Abuse; *"Zararlı veya yasa dışı faaliyetler gerçekleştirmek için alan adlarını veya DNS protokolünü kullanan her türlü faaliyettir."* şeklinde tanımlanmış ve alan adı tahsis sürecinin, alan adı çözümleme sürecinin veya alan adıyla ilişkili diğer

hizmetlerin kötüye kullanılması sonucunda oluştuğu belirtilmiştir (European Commission, 2022, s.10). DNS Abuse'un kötü niyetli tahsis edilen alan adları üzerinden yapılabileceği gibi alan adının kötü niyetli kişiler tarafından ele geçirilmesi sonucu da yapılabileceği ifade edilmiştir. Çalışmaya göre DNS Abuse'un ayrıldığı üç ana tür ise aşağıda yer almaktadır:

> *"1. Kötü niyetle kaydedilmiş alan adları ile ilgili kötüye kullanım*
> *2. DNS ve diğer altyapıların işleyişi ile ilgili kötüye kullanım*
> *3. Kötü amaçlı içerik dağıtan alan adları ile ilgili kötüye kullanım (*European Commission, 2022, s.11*)."*

Avrupa Komisyonu tarafından yayımlanan çalışmadaki DNS Abuse tanımına, Association of the Internet Industry *(ECO)*[22] tarafından eleştiri getirilmiştir. ECO'ya göre tüm çevrimiçi yasa dışı faaliyetlerin geniş bir tanımla DNS Abuse olarak kabul edilmesi, ICANN'i, kayıt otoritelerini ve kayıt kuruluşlarını sorunun çözümü için doğrudan ilişkili kurumlar haline getirebilecektir. Bu durum DNS'in teknik koordinatörü olarak ICANN'in içerik düzenlemeyi içermeyen kapsam ve görev alanına uymamaktadır (ECO, 2022, s.1-2).

Küresel çapta kabul edilmiş bir DNS Abuse tanımı olmadığı gibi ICANN tarafından da kabul edilmiş bir DNS Abuse tanımı bulunmamaktadır. ICANN internet sitesinde yer alan *"Kısaltmalar ve Terimler"* bölümünde DNS Abuse, internet site içeriği dahil edilmeden ve DNS seviyesinde tanımlanmıştır:

> *"DNS altyapısını bozmayı veya DNS'in istenmeyen bir şekilde çalışmasına neden olmayı amaçlayan her türlü kötü niyetli kullanımdır. Kötüye kullanım faaliyetleri arasında DNS bölge verilerini bozma, bir yetkili ad sunucusunun*

[22] Eco, bin üyesiyle Avrupa'nın en büyük internet birliğidir. Dijital ekonomideki teknolojileri, altyapıları ve piyasaları teşvik etmektedir. Dijital altyapının güvenilirliği ve güçlendirilmesi, BT güvenliği ve etik odaklı dijitalleşme, birlik çalışmalarının odak noktasını oluşturmaktadır.

> *yönetim kontrolünü ele geçirme ve alan adı çözümleme hizmetlerini bozmak için DNS'yi binlerce iletiyle doldurma yer alır* (ICANN, 2023ç)."

ICANN Güvenlik, İstikrar ve Dayanıklılık (Second Security, Stability, and Resiliency - SSR2) İnceleme Ekibi Nihai Raporu *"Tanımlar"* bölümünde ise DNS Abuse, aşağıda yer alan tanımda görüldüğü gibi yasa dışı internet site içeriği dahil edilerek daha geniş bir tanımla ifade edilmiştir:

> *"DNS tarafından sağlanan evrensel tanımlayıcıların siber suç altyapısı için kasıtlı olarak kötüye kullanılması ve kullanıcıların çocuk istismarı, fikri mülkiyet ihlali ve dolandırıcılık gibi diğer suç türlerini mümkün kılan internet sitelerine yönlendirilmesi* (ICANN, 2021b, s.60)*"*

ICANN Güvenlik ve İstikrar Danışma Komitesi'nin "DNS'de Kötüye Kullanımın Ele Alınmasına Yönelik Birlikte Çalışabilir Yaklaşıma İlişkin Rapor *(Report on an Interoperable Approach to Addressing Abuse Handling in the DNS)*"da DNS Abuse, İnternet ve Yargı Politikası Ağı tarafından hazırlanan rapordaki teknik kötüye kullanımlar ve aşağıda açıklanacak olan "DNS Abuse Çerçevesi *(DNS Abuse Framework)*" ile benzer şekilde; "kötü amaçlı yazılım, köle bilgisayar ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türleri yaymak için kullanıldığında istenmeyen elektronik posta olmak" üzere sınıflandırılmıştır. Ancak, bu yaklaşımın tüm DNS Abuse türlerini temsil etmediği ve zamanla yeni DNS Abuse türleri oluşacağı için DNS Abuse tanımının hiçbir zaman kapsamlı olmayacağı da ifade edilmiştir (ICANN, 2021c, s.12-13).

ICANN internet sitesindeki *"DNS Güvenliği Tehditlerini Azaltma Programı"* başlıklı sayfada ise, ICANN Topluluğu'nun ortak bir DNS Abuse kavramı oluşturamadığı ifade edilmiş ve bu kavrama benzer olarak *"DNS Güvenlik Tehditleri"* kavramı kullanılmıştır. DNS güvenlik tehditleri, ICANN Güvenlik ve İstikrar Danışma Komitesi raporundaki DNS Abuse tanımı gibi beş türde sınıflandırılmıştır (ICANN, 2023f).

Son olarak, ICANN'in kayıt otoriteleri ve kayıt kuruluşları ile yaptığı sözleşmelerde yapılan son değişiklikte[23], DNS Abuse; kötü amaçlı yazılım, köle bilgisayar ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türler için dağıtım mekanizması olarak kullanıldığında istenmeyen elektronik posta olarak tanımlanmış; çocuk istismarı, fikri mülkiyet ihlali gibi yasa dışı internet site içerikleri dahil edilmemiştir (ICANN, 2024a; ICANN, 2024b)

2019 yılında yayınlanan ve mevcut kırk sekiz kayıt otoritesi ve kayıt kuruluşunun kabul ettiği "DNS Absuse Çerçevesi *(DNS Abuse Framework)*" metnine göre ise DNS Abuse; DNS ile ilişkili olduğu ölçüde beş geniş zararlı faaliyet türünden oluşmaktadır. Bu türler; İnternet ve Yargı Politikası Ağı tarafından yapılan çalışmada *"Teknik Kötüye Kullanım"*da belirtilenler, ICANN'in kayıt otoriteleri ve kayıt kuruluşları ile yaptığı sözleşmelerdeki DNS Abuse tanımında yer alanlar ve ICANN'in*"DNS Güvenlik Tehditleri"* kavramı altında sınıflandırılan türlere benzer olarak; kötü amaçlı yazılım, bot ağları, kimlik avı/oltalama, site trafiği yönlendirme ve DNS Abuse'un diğer türleri için bir dağıtım mekanizması olarak hizmet ettiği ölçüde istenmeyen elektronik postadır (DNS Abuse Framework, 2020, s.1). Metinde ayrıca, kayıt otoriteleri ve kayıt kuruluşlarına DNS Abuse dışında internet site içeriklerine dair kötüye kullanım şikayetleri geldiği ancak ICANN ile yapılan sözleşmeler uyarınca bu şikayetlere karşın eylemde bulunma yükümlülükleri bulunmadığı belirtilmiştir (DNS Abuse Framework, 2020, s.3).

Yapılan incelemeler neticesinde DNS Abuse'un tanımı ve kapsamı üzerine bir fikir birliği olmadığı görülmüştür. Fikir ayrılığının temel sebebi ise çocuk istismarı, fikri mülkiyet hakları ihlali, nefret söylemi gibi yasa dışı internet site içeriklerinin DNS Abuse kapsamına alınıp alınmayacağı ile ilgilidir.

[23] ICANN Yönetim Kurulu tarafından 21 Ocak 2024'te onaylanan ve 5 Nisan 2024 tarihinden itibaren geçerli olan değişiklikler.

Avrupa Komisyonu'nun yayımladığı çalışma ile ICANN'in Güvenlik, İstikrar ve Dayanıklılık (SSR2) İnceleme Ekibi Nihai Raporu'nda yasa dışı internet site içerikleri DNS Abuse kapsamına dahil edilmiş, İnternet ve Yargı Politikası Ağı tarafından yapılan çalışmada ise *"alan adı kötüye kullanımı"* altında *"kötü amaçlı içerik"* olarak yer almıştır. Kırk sekiz kayıt otoritesi ve kayıt kuruluşunun kabul ettiği *"DNS Absuse Çerçevesi"* metninde, ICANN Güvenlik ve İstikrar Danışma Komitesi raporunda ve ICANN'in gTLD kayıt otoriteleri ve kayıt kuruluşları ile yaptığı sözleşmelerde ise yasa dışı internet site içeriği DNS Abuse kapsamına dahil edilmemiştir.

Avrupa Komisyonu'nun yayımladığı çalışmada DNS Abuse'un geniş tanımlanması ECO tarafından eleştirilmiştir. ICANN'in Güvenlik, İstikrar ve Dayanıklılık (SSR2) İnceleme Ekibi Nihai Raporu'nda yasa dışı internet site içerikleri DNS Abuse kapsamına alınmıştır. Ancak, ICANN'in *"Kısaltmalar ve Terimler"* bölümündeki DNS Abuse tanımı, ICANN Güvenlik ve İstikrar Danışma Komitesi raporu ve gTLD kayıt otorite ve kayıt kuruluşu sözleşmelerindeki DNS Abuse tanımında yasa dışı internet site içerikleri tanıma dahil edilmemiştir. Ayrıca, ICANN internet sitesindeki *"DNS Güvenliği Tehditlerini Azaltma Programı"* başlıklı sayfada ICANN Topluluğu'nun ortak bir DNS Abuse kavramı oluşturamadığı ifadesi ve DNS güvenlik tehditlerinin teknik açıdan sınıflandırılması, ICANN Topluluğu'ndaki genel görüşün, yasa dışı internet site içeriklerinin DNS Abuse kapsamına dahil edilmemesi yönünde olduğunu düşündürmektedir. İnternet ve Yargı Politikası Ağı tarafından yapılan çalışmada ise kötü amaçlı içeriğin sınıflandırılmasında kullanılan tanımların, çeşitli kaynaklardan yararlanılarak oluşturulduğunun ve kesin tanımlar içermediğinin belirtilmesi bu içerikler üzerinde uzlaşı olmadığını göstermektedir.

Ülkeler arası yasal düzenleme ve kültürel farklılıklar sebebiyle bir ülkede yasa dışı olarak kabul gören internet site içeriği farklı bir ülkede yasal olarak kabul edilebilmektedir. ccTLD kayıt otoritelerinin, ülke kodu uzantısını yönettikleri ülkenin yasal düzenlemelerine tabi olması ve genel olarak ülkede yerleşik olan kişilere hizmet vermesinden dolayı sorun oluşmayabilir. Ancak, dünya genelinde hizmet veren gTLD kayıt otoriteleri için ülkeler arası yasa dışı internet site içeriği farklılıkları onları

ikilemde bırakabilecek ve siyasi bir karar vermeye itebilecektir. gTLD kayıt otoriteleri arasında görüş farklılıklarının olduğu durum da karmaşık bir yapı ortaya çıkaracaktır. Diğer taraftan, DNS'in temel amacı teknik bir işlevi yerine getirmektir. Bu sebeple DNS Abuse kapsamının da yasa dışı internet site içeriği dahil edilmeden teknik ve güvenlik odaklı olarak belirlenmesinin daha uygun olacağı değerlendirilmektedir.

2. ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI (DNS ABUSE) İLE MÜCADELEDE ALINAN ÖNLEMLER VE YAPILAN ÇALIŞMALAR

Bu bölümde ilk olarak DNS Abuse tespit etme yöntemleri açıklanacak, ardından DNS Abuse ile mücadelede uygulanan eylemler hakkında bilgi verilecektir. Sonrasında, DNS Abuse ile mücadele yöntemleri yedi alt başlık altında incelenecektir.

2.1.1. DNS Abuse Tespit Etme Yöntemleri

İnternetin günümüzde neredeyse tüm alanlarda kullanılması güvenlik unsurunu çok daha önemli bir hale getirmiştir. DNS Abuse ile mücadele de bu güvenliğin sağlanması için ayrı bir öneme sahiptir.

DNS Abuse ile mücadele edebilmek için öncelikle onu tespit etmek gerekmektedir. Kamu kurumları, kayıt otoriteleri, ticari şirketler ve kar amacı gütmeyen kuruluşlar gibi farklı aktörler tarafından DNS Abuse tespitleri yapılabilmektedir. Bu tespitler kapsamında, kayıt otoritelerinin DNS Abuse'a karşı doğrudan aksiyon alabilme yeteneği sebebiyle önemli bir rolü bulunmaktadır. Bu bölümde, alan adı sisteminde kritik bir öneme sahip olan kayıt otoriteleri özelinde DNS Abuse tespit etme yöntemleri incelenecektir.

Kayıt otoriteleri, yönettikleri uzantılar üzerinde DNS Abuse tespitini farklı yöntemlerle yapabilmektedir. Bunlar; resen yapılan tespitler, bildirimlere bağlı yapılan tespitler, hizmet alınan kuruluşlar aracılığıyla yapılan tespitler ve "Reputation Block List - RBL"[1] aracılığıyla yapılan tespitler olarak sınıflandırılabilir.

Kayıt otoriteleri tarafından resen yapılan tespitlerde yapay zekâ teknolojileri aktif bir şekilde kullanılmaya başlanmıştır. DNS Abuse kapsamında yapay zekâ teknolojisi ilk

[1] DNS Abuse yapılan alan adlarını, URL'leri ve IP adreslerini içeren listelerdir. RBL'de yer alan unsurlar, kayıt sırasında veya kullanım esnasında tespit edilmektedir, RBL'ler ticari kuruluşlar, araştırmacılar ve kamu yararına çalışan topluluklar tarafından oluşturulmaktadır.

olarak, “.eu” uzantılı alan adları kayıt otoritesi EURid tarafından kullanılmıştır. 2018 yılında faaliyete geçen “Kötüye Kullanımı Önleme ve Erken Uyarı Sistemi *(Abuse Prevention and Early Warning System - APEWS)*” ile “.eu” kapsamında DNS Abuse yapılması muhtemel olan alan adları tespit edilmeye başlanmış ve tespit edilen alan adları durdurulmuştur. DNS Abuse gerçekleşmeden tedbir amaçlı uygulanan bu sistemin saldırganlara karşı caydırıcı bir etkisi olduğu EURid CEO’su tarafından ifade edilmiştir (EURid, 2020).

APEWS ile birlikte DNS Abuse kapsamında kullanılan yapay zekâ teknolojileri zamanla diğer kayıt otoriteleri tarafından da uygulanmaya başlanmıştır. “.uk, .nl, .be ve .ch” uzantılı alan adlarını yöneten kayıt otoriteleri bunlar arasında yer almaktadır (CENTR, 2022, s.23; DNS Belgium, 2024a; SWITCH, 2021).

Kayıt otoriteleri tarafından, resen yapılan inceleme ve tespitlerin yanında DNS Abuse kapsamında gelen bildirimlere ilişkin olarak prosedürler oluşturulmuştur. Bu prosedürler, sınırları çizilmiş olaylar için uygulanmakta ve yapılacak değerlendirmeye ilgili uzmanlığa sahip taraflar dahil edilmektedir (CENTR, 2022, s.22-23)

DNS Abuse ile ilgili bildirimler; son kullanıcılar, yetkili kurum ve kuruluşlar, ticari işletmeler ve kamu yararına çalışan kuruluşlar gibi farklı aktörler tarafından yapılmaktadır (CENTR, 2022, s.22-23; The Internet & Jurisdiction Policy Network, 2012, s.33). Yapılan bildirimler genellikle, inceleme ve eylem için yeterli bilgi içermeyen farklı formatlarda olmaktadır. Bu sorunun çözümü adına İnternet ve Yargı Politikası Ağı tarafından, bir bildirimde olması gereken asgari unsurları içeren bir tablo hazırlanmıştır. (The Internet & Jurisdiction Policy Network, 2012, s.33).

Tablo 2.1. Alan Adı Kötüye Kullanım Bildirimi

KİMLİK TESPİTİ		**Olmadığı duruma bildirim yapılamayan unsurlar (A)**
Zaman	Bildirimin yapıldığı tarih ve saat	A
Bildirim yapan taraf	Bildirim yapan taraf (mahkeme, kolluk kuvvetleri, şikayet eden kişi, şikayetçinin yasal temsilcisi, isimsiz)	
Düzenleyen kişi	Talep sahibinin adı	A
Bildirim yapanın kimlik numarası	Bildirim yapan tarafından sağlanan referans	
Kayıt kuruluşu (Eğer bildirim kayıt otoritesine yapıldıysa)	Bildirime konu alan adını yöneten kayıt kuruluşunun adı ve kötüye kullanım ile ilgili temas noktası.	
Kayıt otoritesi (Eğer bildirim kayıt kuruluşuna yapıldıysa)	İlgili TLD uzantısını yöneten kayıt otoritesi. Kayıt otoritesi bilinmiyorsa TLD'yi belirtin.	
DAVA - Mahkeme kararı gönderilmesi durumunda		
Kötüye kullanım türü	İddia edilen istismar türünün belirtilmesi	A
Yasal dayanak	Mahkeme kararının bir kopyası	A

Tablo 2.1. Alan Adı Kötüye Kullanım Bildirimi (Devamı)

VAKA - Mahkeme kararının olmaması durumunda		
Değerlendirme	Bildirim yapan kişi tarafından bildirim yapılmadan önce, kayıt otoritesi ve kayıt kuruluşu politikalarına uygun olarak kötüye kullanımın varlığını ve kapsamını tespit etmek için atılan adımlar.	
Destekleyici kanıt	İddia edilen istismar ve değerlendirmeye ilişkin gerçeklere dayalı belgelendirilme. Belgelendirme RBL'e atıf şeklinde olabileceği gibi doğrudan kanıt olarak ekran görüntüsü de olabilir.	
Bildirim yapanın kimlik numarası	Bildirim yapan tarafından sağlanan referans	
Kayıt kuruluşu (Eğer bildirim kayıt otoritesine yapıldıysa)	Bildirime konu alan adını yöneten kayıt kuruluşunun adı ve kötüye kullanım ile ilgili temas noktası.	
Kayıt otoritesi (Eğer bildirim kayıt kuruluşuna yapıldıysa)	İlgili TLD uzantısını yöneten kayıt otoritesi. Kayıt otoritesi bilinmiyorsa TLD'yi belirtin.	
DAVA - Mahkeme kararı gönderilmesi durumunda		
Kötüye kullanım türü	İddia edilen istismar türünün belirtilmesi	A
Yasal dayanak	Mahkeme kararının bir kopyası	A
VAKA - Mahkeme kararının olmaması durumunda		
Değerlendirme	Bildirim yapan kişi tarafından bildirim yapılmadan önce, kayıt otoritesi ve kayıt kuruluşu politikalarına uygun olarak kötüye kullanımın varlığını ve kapsamını tespit etmek için atılan adımlar.	

Tablo 2.1. Alan Adı Kötüye Kullanım Bildirimi (Devamı)

Destekleyici kanıt	İddia edilen istismar ve değerlendirmeye ilişkin gerçeklere dayalı belgelendirilme. Belgelendirme RBL'e atıf şeklinde olabileceği gibi doğrudan kanıt olarak ekran görüntüsü de olabilir.	
Yabancı kamu otoritesi	Eğer var ise, yabancı mahkeme kararının iç hukuka aktarma çalışması da dahil olmak üzere resmi bildirimler.	A
Orantılılık	İddia edilen istismarın DNS düzeyinde harekete geçmek için yeterli bir eşiği karşıladığına dair gerekçe ve potansiyel ikincil zarar ve DNS düzeyinde harekete geçmenin etkinliğinin hesaba katılması.	
TALEP EDİLEN EYLEM		
Alan adı/adları	URL dahil olmak üzere eylemin talep edildiği belirli alan adı/adları.	A
Eylem talebi	Talep edilen eylemin belirtilmesi	A(Mahkeme kararı olması durumunda)
ZAMANLAMA		
Son tarih	Eylemlerin ne zaman gerçekleştirilmesi gerektiği (özellikle müşterek eylemler veya acil durumlarda önemlidir).	
Zaman aralığı	Talep edilen eylemin süresi (eğer uygulanabilirse ve talep edilen eylem transfer ve iptal değilse)	
Acil durum	Talep edilen eylem aciliyet gerektiriyor mu?	
Acil durum gerekçesi	Talep edilen eylemin acil durumla bağlantısının ve acil durumu nasıl önleyeceğinin açıklanması.	A(Gizlilik talep edilirse)

Tablo 2.1. Alan Adı Kötüye Kullanım Bildirimi (Devamı)

GİZLİLİK		
Gizlilik	Alan adı sahibine eylemden önce veya muhtemel eylemden sonra belirli bir süre bilgi verilmemesi talebinde bulunma (uygulanabilir ise).	
Gizlilik zaman aralığı	Talep edilen gizlilik süresi.	A(Gizlilik talep edilirse)
Gizlilik Gerekçesi	Gizlilik talebi ve zaman çizelgesi için uygun gerekçe (Mahkeme Kararlarına dahil edilebilir)	
YETKİ		
Doğrulama	Bildirimde bulunanın kimliğinin ve bildiriminin gerçekliğinin doğrulanmasına olanak tanıyan bilgiler	
Onay beyanı	Bildirimci tarafından; yeterliliğinin, durum tespiti ve beyanlarının doğruluğunun, durdurma/iptal talebinde bulunmak için kötü niyetli bir amacın bulunmadığının yazılı olarak beyan edilmesi.	
İLETİŞİM BİLGİLERİ		
Bildirim yapan kişi	Eylem veya eylemsizlik bildiriminin gönderileceği, talepte bulunan kişinin iletişim bilgileri.	
İMZA		

Kaynak: The Internet & Jurisdiction Policy Network, 2021

Kayıt otoriteleri tarafından, resen veya bildirime bağlı yapılan DNS Abuse tespitlerinin yanında, DNS Abuse konusunda hizmet veren kuruluşlar aracılığıyla da DNS Abuse tespiti yapılabilmektedir. Bu hizmet ücretsiz olabileceği gibi belirli bir ücret karşılığında da yapılabilmektedir. Örneğin DNS Abuse Institute tarafından geliştirilen NetBeacon hizmeti ücretsiz bir şekilde sunulurken, CleanDNS Inc, iQ Global AS ve Knipp Medien und Kommunikation GmbH tarafından geliştirilen CleanDNS, iQ ve Mambo.plus hizmetleri belirli bir ücret karşılığında sunulmaktadır (DNS Abuse Institute, 2023). Ücrete tabi sunulan hizmetlerde, DNS Abuse tespiti yanında hizmet verilen kayıt otoritesi ve kayıt kuruluşları ile birlikte oluşturulan prosedürler kapsamında DNS Abuse'e karşı proaktif çözümler de sunulmaktadır (CleanDNS Inc, 2024a; iQ Global AS ,2024; mambo +, 2024). Bu çözümlere örnek olarak; DNS Abuse tespiti yapılan alan adlarının otomatik olarak durdurulması verilebilir (CleanDNS Inc, 2024b).

NetBeacon Institute[2] tarafından ücretsiz sunulan "NetBeacon Ölçüm ve Analiz Platformu (*Measurement and Analytics Platform - MAP*)" kimlik avı/oltalama ve kötü amaçlı yazılım faaliyetlerini ölçmeye yönelik bir hizmettir. Bu hizmet NetBeacon Institute ile Grenoble Alpes Üniversitesi'nden Prof. Dr. Maciej Korczynski liderliğindeki KOR Labs[3] ile iş birliği içerisinde yürütülmektedir. NetBeacon MAP kapsamında üç farklı formatta rapor yayınlanmaktadır. Bunlar; kamuya açık olan "İnteraktif Grafikler *(Interactive Charts*)" ve "Aylık Analiz (*Monthly Analysis*)" raporları ile ilgili kişi ve kurumlarla paylaşılan "Özel Gösterge Tabloları (*Individual Dashboards*)"dır (NetBeacon, 2024).

Son olarak RBL'ler aracılığı ile de kayıt otoriteleri tarafından DNS Abuse tespiti yapılabilmektedir (DNS Abuse Institute, 2023). RBL'ler; DNS Abuse yapılan alan adlarını, URL'leri ve IP adreslerini içermektedir (ICANN, 2017a). Kayıt otoriteleri,

[2] DNS Abuse Institute'nün ismi 2024 yılı içerisinde NetBeacon Institute olarak değiştirilmiştir. Daha fazla bilgi için bkz. (https://netbeacon.org/the-institute/), (14.10.2024)
[3] Siber tehditlerle mücadeleye yönelik bir üniversite girişimidir. İnternet topluluğunun kötüye kullanımı önlemesine ve şirketlerin ağ koruması ve karşı önlemlerin etkinliğini artırmasına yardımcı olmayı amaçlamaktadır. Daha fazla bilgi için bkz. (https://korlabs.io/about.html, (15.10.2024)

yönettikleri uzantılara ilişkin olarak bu listeleri kontrol ederek DNS Abuse tespiti yapabilmektedir.

2.1.2. DNS Abuse ile Mücadelede Uygulanan Eylemler

DNS Abuse ile mücadelede tespitin yapılması ne kadar önemliyse, uygulanacak eyleme karar verilmesi de aynı derecede önemlidir. Bazı DNS Abuse türleri için DNS düzeyinde eylem uygun olsa da DNS düzeyinde eylemin yalnızca alan adının kendisi üzerinde değil elektronik posta, veritabanları ve alan adıyla bağlantılı hizmetler gibi diğer faaliyetler üzerinde de önemli bir etkisi bulunmaktadır. Bu nedenle uygulanacak eylem sadece etkili değil muhtemel mağduriyetle de orantılı olmalıdır (The Internet & Jurisdiction Policy Network, 2021, s.39).

Kötü amaçlı yazılım ve kimlik avı/oltalama, internet sitesi veya elektronik posta vasıtasıyla yapılabilen DNS Abuse türleridir. Bu gibi durumlarda kötü amaçlı faaliyeti durdurmak veya kesintiye uğratmak için ilgili alan adı üzerinde eylemde bulunulabilir. Buna karşılık, site trafiği yönlendirme bir DNS Abuse türü olmasına rağmen DNS düzeyinde eylem yoluyla her zaman durdurulamaz. Çünkü, saldırganın yetkili ad sunucuyu ele geçirerek ilgili IP adresini değiştirmesi veya kullanıcının cihazına yüklediği kötü amaçlı yazılımla internet trafiğini manipüle etmesini içeren bu türde, DNS düzeyinde eylem yapılması yetkili ad sunucu kaynaklı sorunu çözebilmekte ancak kullanıcı cihazı kaynaklı soruna bir şey yapamamaktadır (The Internet & Jurisdiction Policy Network, 2021, s.39).

Ortaya çıkabilecek bu gibi durumların önüne geçmek adına İnternet ve Yargı Politikası Ağı tarafından, hangi eylemlerin hangi DNS Abuse türlerine uygun olabileceğine ilişkin bir tablo yayınlanmıştır (The Internet & Jurisdiction Policy Network, 2021, s.39). Bu tabloda yer alan eylemler; "Kilitle *(Lock)*, Durdur *(Hold/Suspension)*, Yönlendir *(Redirect)*, Aktar *(Transfer)*, İptal *(Delete)* ve Oluştur *(Create)*"'dir:

Tablo 2.2. Eylem Türleri

EYLEM TÜRLERİ	**UYGULANABİLECEK DNS ABUSE TÜRLERİ**	**EYLEMİN ETKİSİ**
KİLİTLE	Kötü amaçlı yazılım, Kimlik avı/Oltalama, Köle bilgisayar ağları, Hızlı akış barındırma, İstenmeyen elektronik posta (DNS Abuse türleri için bir dağıtım mekanizması olduğu durumda)	Bir alan adının kilitlenmesi; sahiplik, iletişim ve yetkili ad sunucu bilgilerinin değiştirilmesini engellemektedir. Ayrıca, alan adı başka birisine aktarılmaz ve silinemez. Bu eylem, kötüye kullanım iddiasının araştırılmasına olanak sağlanması ve alan adının üçüncü kişilere aktarılmasını engellemek için kullanılmaktadır. Kilitli bir alan adı DNS üzerinden çözümlenmeye devam etmekte, yani alan adı üzerinden ilgili internet sitesine/internet sitelerine erişim sürmektedir.
DURDUR	Kötü amaçlı yazılım, Kimlik avı/Oltalama, Köle bilgisayar ağları, Hızlı akış barındırma, İstenmeyen elektronik posta (DNS Abuse türleri için bir dağıtım mekanizması olduğu durumda)	Durdur eylemi, alan adının TLD bölge dosyasından kaldırılarak DNS'te çözümlenmesinin engellenmesidir. Bu sayede, alan adı üzerinden yetkili ad sunucuları aracılığıyla bağlanan elektronik postalar veya üçüncü/dördüncü derece alan adları dahil olmak üzere internet sitesine/ sitelerine veya diğer hizmetlere erişim engellenmektedir. Bu, kötü amaçlı yazılımların dağıtılmasını ve elektronik posta yoluyla dağıtımı da dahil olmak üzere kimlik avı/oltalamanın önlemesine yardımcı olmaktadır. Durdur eylemi, bir alan adı için uygulanabilecek en güçlü eylemdir ve çoğu DNS Abuse türüne karşı kullanılabilmektedir. Bununla birlikte, ilgili internet sitesinin yalnızca IP adresi üzerinden de olsa erişilebilir kalmaya devam edeceğini unutmamak gerekmektedir.

Tablo 2.2. Eylem Türleri (Devamı)

YÖNLENDİR	Kötü amaçlı yazılım, Kimlik avı/Oltalama, Köle bilgisayar ağları	Kayıt otoritesi ve kayıt kuruluşları, bir alan adının yetkili ad sunucularını değiştirme imkanına sahiptir. Alan adı yetkili ad sunucu bilgileri değiştirilmesiyle ilgili olarak, zararlı içeriğe erişenlerin bilgisine ulaşılması örnek verilebilir.
AKTAR	Kötü amaçlı yazılım, Kimlik avı/Oltalama, Köle bilgisayar ağları, Hızlı akış barındırma, İstenmeyen elektronik posta (DNS Abuse türleri için bir dağıtım mekanizması olduğu durumda)	Kayıt otoritesi ve kayıt kuruluşları, belirli sınırlı durumlarda kötüye kullanımı önlemek için alan adı sahibinin rızası olmadan alan adını üçüncü bir tarafa aktarabilmektedir. Bu eylem sayesinde alan adı kontrolünün üçüncü bir tarafa geçmesiyle kötüye kullanım önlenebilmektedir.
İPTAL	Köle bilgisayar ağları	Bir alan adının iptal edilmesi çok ciddi bir eylemdir ve dikkatli bir durum tespiti yapılmadan ve ilgili yetkililer tarafından talimat verilmeden yapılması önerilmemektedir. İptal eylemi, köle bilgisayar ağlarını kontrol edenlerin komut ve kontrolünü engellemek için kullanılmaktadır. İptal eyleminin alan adı sahibi ve ilgili hizmetler üzerinde büyük bir etkisi vardır ve bu eylem seçiminin yanlışlıkla uygulandığı durumlarda geri dönüş şansı bulunmamaktadır. Alan adları kötü niyetli kişiler tarafından hızlı bir şekilde yeniden tahsis edilebildiğinden, iptal eylemi genellikle kötüye kullanımı azaltmada durdurma gibi eylemler kadar etkili değildir.

Tablo 2.2. Eylem Türleri (Devamı)

OLUŞTUR	Köle bilgisayar ağları, Alan adı oluşturma algoritmaları	Alan adı oluşturma algoritmaları, komuta ve kontrol sunucularıyla buluşma noktası olarak kullanılmak üzere periyodik olarak çok sayıda alan adı oluşturmak için kullanılan, çeşitli kötü amaçlı yazılım gruplarında görülen algoritmalardır. Kayıt otoritesi ve kayıt kuruluşları bazen bir alan adı oluşturma algoritmasının tahmini bir dizisinin parçası olan alan adlarını oluşturmak ve ardından bu alan adlarını yönlendirmek istemektedir. Alan adları oluşturulduktan sonra, köle bilgisayar ağlarını oluşturan sunuculara işaret eden alan adlarına müdahale etmek için durdur, yönlendir veya iptal eylemleri kullanılabilmektedir.

Kaynak: The Internet & Jurisdiction Policy Network, 2021

Kilitle ve durdur eylemleri DNS Abuse ile mücadelede daha fazla kullanılmaktadır. Durdurma eyleminde alan adı TLD bölge dosyasından kaldırılmakta, böylece alan adının DNS'te çözümlenmesi engellenmektedir. Kilitle eyleminde ise, alan adının satışı ve devredilmesi önlenmektedir. Bu iki eylem, kötü amaçlı yazılım ve kimlik avı/oltalama ile mücadelede çoğunlukla birlikte kullanılmaktadır. Aktar, yönlendir ve oluştur eylemleri sınırlı kullanıma sahiptir. Kayıt otoritesi ve kayıt kuruluşları bu eylemleri genel olarak kolluk kuvvetleri veya mahkemelerden gelen resmi talepler doğrultusunda uygulamaktadır. İptal eylemi, genellikle DNS Abuse'a karşı kullanılan bir eylem değildir çünkü bir alan adı iptal edildiğinde tekrar tahsise açılmaktadır. Bu da alan adının saldırgan tarafından tekrar tahsis edilmesine olanak tanımaktadır. Oluştur eylemi, köle bilgisayar ağları gibi belirli DNS Abuse türleri için kullanılmalıdır ancak bu eylemin kullanımı bazı sorunları beraberinde getirmektedir. Oluştur eylemi ile alan adı yaşam döngüsü dışında başvuru olmadan tahsis

yapılmaktadır. Ayrıca, oluşturulan alan adı tahsis ücretlerinin ödenip ödenmeyeceği de başka bir konudur (The Internet & Jurisdiction Policy Network, 2021, s.39).

2.3. DNS Abuse ile Mücadele Yöntemleri

2.3.1. DNSSEC

DNS, internet kullanımının günümüze göre çok az olduğu ve güvenliğin öncelikli konular arasında yer almadığı 1980'li yıllarda tasarlanmıştır. O zamanlar ikincil planda olan DNS güvenliği konusu yıllar içerisinde internet kullanımın artmasıyla birlikte önemini giderek arttırmıştır.

DNS çalışma mantığına göre, yinelemeli çözümleyici bir sorgu gönderdiğinde, cevabın doğruluğu kontrol edilmemektedir. Yinelemeli çözümleyicinin kontrol ettiği husus; cevabın sorguyu gönderdiği kaynaktan yani IP adresinden gelip gelmemesidir. Ancak, bir yanıtın kaynağı olarak sadece IP adresine güvenmek güçlü bir kimlik doğrulama mekanizması değildir (ICANN, 2019b).

Saldırganlar, DNS sorgusunda yer alan sunuculardan (kök sunucu, TLD sunucu ve yetkili ad sunucu) gelen cevapları taklit ederek, yinelemeli çözümleyicinin kendilerini gerçek bir sunucu gibi görmelerini sağlayabilmektedir. Bu durumda son kullanıcılar, farkında olmadan saldırganların istedikleri internet sitelerine yönlendirilerek mağdur edilebilmektedir (ICANN, 2019b).

Diğer bir güvenlik sorunu ise yinelemeli çözümleyicilerin önbelleği ile ilgilidir. Yinelemeli çözümleyiciler, yetkili ad sunucularından aldıkları cevapları önbelleğe alarak DNS sorgu sürecini hızlandırmaktadır. Önbelleğe güvenilerek gerçekleşen internet sitesine hızlı erişme imkânı riskli bir durumu da beraberinde getirmektedir (ICANN, 2019b).

Yinelemeli çözümleyicinin saldırgan tarafından iletilen sahte bir cevabı gerçek sanması durumunda önbelleği zehirlenmektedir. Bu durum, diğer kişiler için de risk oluşturmaktadır. Şöyle ki; diğer kişiler aynı alan adına ilişkin DNS sorgu sürecini başlattığı zaman, yinelemeli çözümleyici önbelleğinde bulunan sahte IP adresini iletmektedir. Sahte IP adresine erişen diğer kişiler de saldırganlar tarafından mağdur edilebilmektedir (ICANN, 2019b).

Bu tehditlere yanıt olarak İnternet Mühendisliği Görev Gücü (*The Internet Engineering Task Force - IETF*) tarafından, DNS sorgu sürecinin güvenliğini artıran Alan Adı Sistem Güvenliği Uzantısı *(Domain Name System Security Extensions - DNSSEC)* geliştirilmiştir. DNSSEC, yinelemeli çözümleyiciye gelen cevapların kimden geldiğinin kontrol edilmesini sağlamakta ve sunucuların verdiği cevapları manipüle eden saldırganlara karşı son kullanıcıları korumaktadır. (Internet Society, 2024).

DNSSEC ile birlikte DNS protokolüne iki önemli özellik eklenmiştir; veri kaynağı kimlik doğrulaması ve veri bütünlüğü koruması. Veri kaynağı kimlik doğrulaması özelliği ile yinelemeli çözümleyici, aldığı verinin yetkili olan sunuculardan geldiğini doğrulayabilmektedir. Veri bütünlüğü korumasında ise, verilerin yetkili sunucular tarafından özel anahtarlarıyla imzalanmasından sonra değiştirilip değiştirilmediği bilgisi yinelemeli çözümleyici tarafından bilinmektedir (ICANN, 2019b).

DNSSEC'te her DNS bölgesinin (kök, TLD, yetkili ad sunucu) bir genel/özel *(public key/private key)* anahtar çifti bulunmaktadır. Bölge sahibi, bölgedeki DNS verilerini imzalamak ve bu veriler üzerinde dijital imzalar oluşturmak için bölgenin özel anahtarını kullanmaktadır. Özel anahtar bölge sahibi tarafından gizli tutulmakta, genel anahtar ise herkes tarafından kullanılabilmesi için yayınlanmaktadır (ICANN, 2019b).

Yinelemeli çözümleyici, yetkili sunuculardan gelen cevaplardaki verilerin doğruluğunu kontrol etmek için sorgu gönderdiği bölgenin genel anahtarını kullanmaktadır. Alınan DNS verileri üzerindeki dijital imzanın geçerliliği yinelemeli

çözümleyici tarafından doğrulanırsa, cevaptaki veriler son kullanıcıya gönderilmektedir. İmzanın doğrulanamadığı durumda ise son kullanıcıya bir hata döndürülmektedir (ICANN, 2019b).

DNSSEC bir güven zinciri oluşturmaktadır ve DNSEEC teknolojisinin kullanılabilmesi için DNS sorgu sürecinde yer alan bileşenlerin (yinemeli çözümleyici, kök sunucu, TLD sunucu, yetkili ad sunucu) bu teknoloji ile uyumlaştırılması gerekmektedir. Bu güven zincirinde bulunan sunuculardan birinde DNSSEC teknolojisi uygulanmadığı takdirde sistem işlevsiz hale gelmektedir. Benzer şekilde, hizmet alınan yinemeli çözümleyicinin DNSSEC ile uyumlu olmaması halinde, yetkili sunucularda gerekli işlemler yapılsa bile kişi DNSSEC teknolojisinden yararlanamayacaktır (ICANN, 2019b).

2.3.2. Alan Adı Kayıt Bilgilerinin Kontrolü

DNS Abuse ile mücadelede kullanılabilecek diğer yöntem ise, alan adı kayıt bilgilerinin doğrulanmasıdır. Alan adı kayıt bilgilerinin doğrulanması, DNS Abuse ile mücadelede önemli bir rol oynamaktadır çünkü kötü niyetli kişilerin alan adlarını tahsis ederken gerçek ve doğru bilgi verme olasılığı düşüktür. Bu bilgilerin doğrulanması, yanlış bilgilerle alan adı tahsisini zorlaştıracak ve DNS Abuse faaliyetlerinin azalmasına katkı sağlayacaktır (Messaging, Malware and Mobile Anti-Abuse Working Group, 2023, s.6).

Alan adı kayıt bilgilerinin doğruluğunu kontrol etmek için standart bir uygulama bulunmamaktadır. Ülkesel farklılıklar nedeniyle, bir ülkede uygulanan bir politika başka bir ülkede aynı sonuçları doğurmayabilmektedir. Bu durum da farklı yöntemlerin uygulanmasına sebep olmaktadır (CENTR, 2021, s.9).

Alan adı kayıt bilgileri kontrolü; ilgili kamu veri tabanlarına erişilerek yapılan doğrulama, başvuru sahiplerinden veya alan adı sahiplerinden belge talep edilerek

yapılan doğrulama, otomatik sözdizimi kontrolleri[4] ve ulusal elektronik kimlik numarasıyla yapılan doğrulanma gibi yöntemlerle gerçekleştirilebilmektedir (CENTR, 2021, s.10). Kontrol işlemleri tahsis sırasında veya sonrasında yapılabilmekte, sürekli ya da duruma özel olarak gerçekleştirilebilmektedir. Duruma özel yapılanlar genellikle, üçüncü taraf şikayetleri, hizmet alınan kayıt kuruluşunun değişmesi ve eksik bilgiler sebebiyle yapılmaktadır (CENTR, 2021, s.12-13).

Alan adı kayıt bilgileri doğrulama işlemlerinin kimin tarafından yapılacağı da önemli bir konudur. CENTR tarafından üyeleri olan ccTLD kayıt otoritelerine yapılan bir ankette; çoğu katılımcı ilgili düzenlemelerine istinaden kayıt kuruluşlarının doğrulama işlemlerini yapmakla yükümlü olduğunu belirtmiştir. Ancak, anket katılımcılarına göre bu düzenleme hükümleri nadiren yerine getirilmektedir. (CENTR, 2021, s.11). Benzer bir şekilde, gTLD uzantılı alan adları kapsamında alan adı kayıt bilgilerinin doğruluğunu sağlama yükümlülüğü, "Kayıt Kuruluşu Akreditasyon Sözleşmesi" gereğince kayıt kuruluşlarına verilmiştir. Sözleşmeye göre kayıt kuruluşları, gTLD uzantılı alan adlarıyla ilgili kayıt verilerinin doğruluğunu sağlamak için gerekli tedbirleri almalıdır (ICANN, 2021a). Avrupa Birliği düzeyinde, 16 Ocak 2023 tarihinde yürürlüğe giren ve üye devletlerin 17 Ekim 2024 tarihine kadar yasal düzenlemelerini tamamlamaları gerektiği NIS 2 Direktifi'nde ise, alan adı kayıt bilgilerini doğruluğu konusunda kayıt otoriteleri ve kayıt kuruluşları birlikte sorumlu tutulmuştur.

Alan adı kayıt bilgilerinin doğrulanması, alan adı sektörünün küresel ölçekte faaliyet göstermesi nedeniyle zorlu bir süreçtir. Kişiler, dünyanın herhangi bir yerinden alan adı tahsis edebilmektedir. Tahsis edilen alan adının ccTLD uzantılı olması durumunda yapılacak kontrol, kayıt otoritesi ve kayıt kuruluşunun genellikle o ülkede faaliyet göstermesi sebebiyle daha kolay olabilir ancak gTLD uzantılı alan adlarında durum

[4] İletilen bilgilerin doğru formatta olup olmadığını kontrol eden süreçtir. Örnek olarak, geçerli bir ülke koduna sahip ve karakter sınırları dahilinde olan telefon numarasının kontrolü verilebilir.

çok daha karmaşıktır. Benzer durum, ülkede yerleşik olmayan kişilere alan adı tahsisi yapan ccTLD kayıt otoriteleri için de geçerlidir.

Bazı ccTLD kayıt otoriteleri, ülkede yerleşik olmayan kişilere tahsisli veya başvuru halinde olan alan adı bilgilerinin doğruluğunu kontrol etmek için yöntemler geliştirmiştir. Örneğin, Danimarka'nın ccTLD'si olan ".dk" altında alan adı tahsis eden yabancı kişilerin alan adı kayıt bilgileri otomatik olarak risk değerlendirmesine tabi tutulmaktadır. Yapılan değerlendirme sonucunda, yabancı kişilerden kimlik bilgilerini kanıtlaması istenebilmektedir. Romanya'nın ccTLD'si olan ".ro" için ise farklı bir yöntem uygulanmaktadır. ".ro" uzantılı alan adı tahsis etmek isteyen yabancı kişi, kimliğinin taranmış halini alan adı başvurusuna eklemek zorundadır. Çekya'nın ccTLD'si olan ".cz"de ise, yabancı kişi tanımı daha farklı olarak, alan adı sahibinin Avrupa Birliği veya Avrupa Ekonomik Bölgesi ülkelerinde yerleşik olmaması şeklinde yapılmıştır. Talep edilmesi halinde ise yabancı kişi, Avrupa Birliği veya Avrupa Ekonomik Bölgesi ülkelerinde geçerli bir iletişim adresini vermeli veya bu ülkelerde yerleşik ve alan adıyla ilgili elektronik postaları takip edebilecek bir temsilci atamalıdır. Bazı kayıt otoriteleri ise yabancı kişilere ait alan adının kayıt bilgilerini doğrulayabilmek için, pasaport ve diğer resmi kimlik belgelerinin taranmış hallerini istemektedir (CENTR, 2021, s.19).

gTLD uzantılı alan adı hizmeti veren kayıt kuruluşlarının alan adı kayıt bilgileri kontrol süreci RAA'da düzenlenmiştir. Sözleşmeye göre kayıt kuruluşu; yönetimi altında bulunan alan adının tahsis edilmesinden, başka bir kayıt kuruluşundan kendisine transfer edilmesinden ve hizmet verdiği alan adının kayıt bilgilerinde değişiklik olmasından sonraki on beş gün içinde "Kayıt Verileri Rehber Hizmeti *(Registration Data Directory Service - RDDS)*[5]*"* bilgileri ile alan adının yönetildiği, kendisinde kayıtlı hesap bilgileri kapsamında kontrol işlemi yapacaktır. Kayıt

[5] WHOIS hizmeti dahil olmak üzere alan adı kayıt verilerine veya bunların bir alt kümesine erişim sağlamak için gTLD kayıt otoriteleri ve kayıt kuruluşları tarafından sunulan toplu hizmetleri ifade etmektedir Daha fazla bilgi için bkz. (https://www.icann.org/resources/pages/whois-rdds-2023-11-02-en), (20.02.20234)

kuruluşunun yaptığı kontrol, alan adı kayıt bilgilerinin doğrulanması ile alan adı sahibinin ve farklı kişi olması durumunda hesap sahibinin, elektronik posta adresinin veya telefon numarasının aktif bir şekilde kullanılıp kullanılmaması ile ilgili teyidi içerecektir (ICANN, 2024b).

gTLD uzantılı alan adı hizmeti veren kayıt kuruluşlarının, alan adı kayıt bilgileri ile ilgili olarak kontrol edeceği hususlar, RAA'nın "RDDS Doğruluk Programı Şartnamesi (*RDDS Accuracy Program Specification*)" başlıklı bölümün birinci maddesinin ilgili bentlerinde aşağıdaki şekilde belirtilmiştir:

> *"a. Sözleşmenin Alt Bölüm 3.3.1 kapsamında gerekli olan tüm alanlara ilişkin verilerin*[6] *ilgili ülke veya bölge için uygun bir formatta mevcut olduğunu doğrulayın.*
> *b. Tüm elektronik posta adreslerinin RFC 5322'ye veya haleflerine göre uygun formatta olduğunu doğrulayın.*
> *c. Telefon numaralarının uluslararası telefon numaraları için ITU-T E.164 notasyonuna veya eşdeğerlerine veya haleflerine göre uygun formatta olduğunu doğrulayın.*
> *d. Posta adreslerinin UPU Posta adresleme formatı şablonlarında, S42 adres şablonlarında (güncellenebilir) veya diğer standart formatlarda tanımlandığı şekilde ilgili ülke veya bölge için uygun formatta olduğunu doğrulayın.*
> *e. İlgili ülke veya bölge için bu tür bilgilerin teknik ve ticari olarak mümkün olduğu durumlarda, tüm posta adresi alanlarının, alanlar arasında tutarlı olduğunu doğrulayın (örneğin: caddenin şehirde bulunması, şehrin eyalet/il olarak bulunması, şehrin posta koduyla eşleşmesi)"* (ICANN, 2024b).

Yukarıda belirtilen doğrulamalar dışında, alan adı sahibinin ve farklı kişi olması durumunda hesap sahibinin, elektronik posta adresi veya telefon numarasının aktifliği

---

[6] Alan adına ilişkin olarak; sahiplik bilgisi, elektronik posta bilgisi, yetkili ad sunucu bilgileri, tahsis başlangıç ve bitiş tarihi, kayıt kuruluşu bilgisi vb. bilgiler.

kayıt kuruluşları tarafından teyit edilmelidir. Kayıt kuruluşlarının teyit sürecini nasıl işleteceği ise mezkûr maddenin ilgili bendinde belirtilmiştir:

> *"f. Teyit Etmek*
> *i. Alan adı sahibinin ve farklı kişi olması durumunda hesap sahibinin elektronik posta adresi, kayıt kuruluşu tarafından gönderilen benzersiz bir kod ve bu kodun kayıt kuruluşu tarafından belirlenen bir yöntemle, alan adı sahibi ve farklı kişi olması durumunda hesap sahibi tarafından geri gönderilmesini içeren bir araç tabanlı doğrulama yöntemiyle teyit edilmeli, veya*
> *ii. Alan adı sahibi ve farklı kişi olması durumunda hesap sahibi telefon numarası, (A) kayıt kuruluşu tarafından aranarak veya kısa mesaj yoluyla gönderilen benzersiz kodun, kayıt kuruluşu tarafından belirlenen yöntemle geri gönderilmesi veya (B) web, elektronik posta veya posta yoluyla iletilen benzersiz kodun, telefon numarası aranarak karşı taraftan istenmesi yoluyla teyit edilmelidir.*
> *Her iki durumda da kayıt kuruluşu, alan adı sahibinden olumlu bir yanıt alamazsa, geçerli iletişim bilgilerini manuel olarak doğrulayacak veya geçerli iletişim bilgilerini doğrulayana kadar alan adının durduracaktır. Kayıt kuruluşu, hesap sahibinden olumlu bir yanıt almaz ise geçerli iletişim bilgilerini manuel olarak doğrulayacak ancak alan adını durdurması gerekmeyecektir."* (ICANN, 2024b).

RAA'a göre; alan adı kayıt bilgilerinin veya alan adlarının yönetildiği hesaplardaki iletişim bilgilerinin değişmesi durumunda, daha önce alan adıyla ilgili doğrulama ve teyit işlemleri yapıldığına bakılmaksızın kayıt kuruluşları tarafından on beş gün içinde, "RDDS Doğruluk Program Şartnamesi" başlıklı bölümün birinci maddesi çerçevesinde değişiklik yapılan bilgiler doğrulanacak ve aynı maddede belirtilen şekilde teyit edilecektir. Kayıt kuruluşu, alan adı sahibinden ilgili teyidi alamazsa, ilgili iletişim bilgilerini manuel olarak doğrulayacak veya geçerli iletişim bilgilerini teyit edene kadar alan adını durduracaktır. Kayıt kuruluşu, hesap sahibinden ilgili

teyidi alamaz ise, geçerli iletişim bilgilerini manuel olarak teyit edecek ancak herhangi bir alan adını durdurması gerekmeyecektir (ICANN, 2024b).

Kayıt kuruluşunun, aynı iletişim bilgilerine ilişkin doğrulama ve teyit prosedürlerini daha önce başarıyla tamamlamış olması ve bu bilgilerin güncel olmadığına dair yeni bir bilgiye sahip olmaması halinde, yukarıda belirtilen birinci madde kapsamındaki doğrulama ve teyit prosedürlerini gerçekleştirmesi gerekmemektedir. Ancak kayıt kuruluşu, hizmet verdiği bir alan adı için birinci maddenin (a) ile (f) bentleri arasında belirtilen iletişim bilgilerinin yanlış olduğunu gösteren bir bilgiye sahipse, daha önce söz konusu alan adıyla ilgili olarak yaptığı doğrulama ve teyit işlemlerine bakılmaksızın birinci madde (f) bendinde açıklandığı şekliyle elektronik posta adresini teyit etmeli veya bu işlemi tekrarlamalıdır (ICANN, 2024b).

Kayıt kuruluşu, birinci maddenin (a) ile (f) bentleri arasında belirtilen iletişim bilgilerinin yanlış olduğunu gösteren bir bilgiye sahip olduktan sonraki on beş gün içinde, alan adı sahibinden gerekli teyidi sağlayan olumlu bir yanıt alamazsa, geçerli iletişim bilgilerini manuel olarak doğrulayacak veya geçerli iletişim bilgilerini doğrulayana kadar kaydı durduracaktır. Alan adı için ödeme yapan müşterinin olduğu durumda ise kayıt kuruluşu tarafından farklı bir süreç işletilecektir. Eğer, yanlış iletişim bilgilerine dair bilgiye sahip olduktan sonraki on beş gün içinde ödeme yapan müşteriden gerekli teyidi sağlayan olumlu bir yanıt alamazsa, geçerli iletişim bilgilerini manuel olarak doğrulayacak ancak herhangi bir alan adını durdurması gerekmeyecektir (ICANN, 2024b).

Son olarak, RAA'nın 3.7.7.1 alt bölümünde açıklandığı şekliyle[7], alan adı sahibinin kasıtlı olarak yanlış veya şüpheli iletişim bilgileri sunması, kayıt kuruluşuna sunduğu bilgilerde değişiklik olmasına rağmen bunları derhal güncellememesi veya kayıt

[7] ICAN Kayıt Kuruluşu Akreditasyon Sözleşmesinde, yanlış veya şüpheli iletişim bilgileri sunulması ve kayıt kuruluşuna sunduğu bilgilerde değişiklik olmasına rağmen bunların derhal güncellenmemesi ilgili ifadeler alt bölüm 3.7.7.2'de geçmektedir ancak "RDDS Doğruluk Program Şartnamesi" başlıklı bölümün beşinci maddesinde 3.7.7.1 olarak yazılmıştır. Yazım hatası yapıldığı değerlendirilmektedir.

kuruluşunun alan adı kayıt verilerinin doğruluğuna ilişkin sorularına on beş gün içerisinde cevap vermemesi halinde, kayıt kuruluşu tarafından alan adı durdurulmalı veya iptal edilmeli ya da kayıt bilgileri doğrulanana kadar alan adını müşteri bekletme ve müşteri transfer yasağı kapsamına alınmalıdır (ICANN, 2024b).

Alan adı bilgilerinin yanlış olduğunda dair ICANN'e şikayette bulunulabilmektedir. ICANN'e gelen şikayetler; sözleşme kapsamında olup olmadığı ve iletilen kanıtın uygunluğu kapsamında incelenmektedir. İnceleme sonucunda sözleşme kapsamı dışında kalan veya uygun kanıtı bulunmayan şikayetler kapatılmaktadır. İncelemeyi geçen şikayetler için, şikayete konu alan adına hizmet veren kayıt kuruluşu hakkında soruşturma başlatılmaktadır. Soruşturma kapsamı, iddia edilen yanlışlığın araştırılması için makul adımları atma yükümlülüğü de dahil olmak üzere RAA'da belirtilen ilgili yükümlülüklerdir. Şikayetlerin yanı sıra, ICANN tarafından gerçekleştiren proaktif izleme faaliyetleri sonucunda da soruşturma başlatılabilmektedir (ICANN, 2021a).

Kayıt kuruluşu tarafından yapılan işlemlerin uygunluğu, şikayet edilen yanlışlığın türüne bağlıdır. Örneğin, aktif olmayan bir elektronik posta adresi şikayeti, kayıt kuruluşunun yalnızca elektronik postanın çalıştığından emin olmak için yapılan teyidi içerebilir. Bununla birlikte, şikayetin kimlik bilgileri ile ilgili olması durumunda (örneğin, alan adı sahibi bilgisi yanlışsa), kayıt kuruluşundan şikayete ilişkin yaptığı tespitler ve yaptığı inceleme sonuçları hakkında daha fazla bilgi talep edilebilecektir (ICANN, 2021a).

Açılan soruşturma genellikle kayıt kuruluşunun alan adını durdurması veya iptal etmesini de içerecek şekilde, RAA'dan doğan soruşturma, doğrulama veya teyid yükümlülüklerine uyduğunu göstermesi halinde sona erdirilmektedir. Kayıt kuruluşunun yükümlülükleri yerine getirmemesi durumunda kamuya açık bir ihlal bildirimi yayınlanmaktadır. İhlal bildiriminden sonra ilgili yükümlülükler yerine getirilmezse, kayıt kuruluşunun RAA'sı askıya alınabilecek veya feshedilebilecektir (ICANN, 2021a; ICANN, 2024c).

2.3.3. Alan Adı Kilidi

Kötü amaçla tahsis edilen alan adları üzerinden DNS Abuse yapılabildiği gibi iyi niyetle tahsis edilen alan adları üzerinden de DNS Abuse yapılabilmektedir. Alan adı sahibi hesabının saldırganlar tarafından ele geçirilmesi durumunda, alan adı yetkili ad sunucu bilgileri değiştirilmekte ve kişiler alan adı üzerinden erişmek istedikleri internet sitesine yönlendirilmek yerine kimlik avı/oltalama amacıyla tasarlanmış ve gerçek internet sitesine çok benzeyen bir siteye yönlendirilmektedir (Malware and Mobile Anti-Abuse Working Group, 2022, s.8).

Meşru amaçlarla tahsis edilen alan adlarının belirtilen şekilde DNS Abuse faaliyetine konu olmaması için "Alan Adı Kilidi" hizmeti geliştirilmiştir. Bu hizmet belirli bir ücret karşılığında sunulmakta ve uzantılara göre farklı isimlendirilmektedir. Örneğin, Almanya'nın ccTLD'si olan ".de" için ".de Kayıt Otoritesi Kilidi *(.de Registry Lock)*" olarak isimlendirilen bu hizmet İngiltere'nin ccTLD'si ".uk" için "Alan Adı Kilidi *(Domain Lock)* olarak adlandırılmıştır (DENIC, 2023a; Nominet, 2023a).

Alan adı kilidi hizmeti ile yetkisiz bir şekilde alan adı kayıt bilgilerinin değiştirilmesi, alan adından feragat edilmesi ve alan adının farklı bir kayıt kuruluşuna transfer edilmesinin önüne geçilmektedir. Belirtilen işlemler, alan adı kilidi konulan bir alan adı için teyit mekanizmaları ile gerçekleştirilmektedir (CIRA, 2023a; DENIC, 2023a; Nominet, 2023a; SIDN, 2024a). Teyit mekanizmaları uzantılara göre değişebilmekte ve uygulamada farklı yöntemler izlenmektedir. Yöntemler arasındaki farklılıklar, belirtilen işlemlere kimin onay vereceği ve onay işleminin nasıl gerçekleşeceği ile ilgilidir. Onay verecek kişi kapsamında, yapılan işlemlere alan adı sahibinin doğrudan onay vermesi gereken yöntemler olduğu gibi, alan adı sahibinin belirlediği üçüncü bir kişi tarafından da onay verilebildiği yöntemler mevcuttur. Bunların yanı sıra, kayıt kuruluşunun sorumlu kişisi tarafından onay verilerek işlemlerin gerçekleştirildiği farklı bir yöntem de uygulanmaktadır. Onayın veriliş şekli ise alan adı sahibinin aranarak onay alınması, kısa mesaj veya uygulamalarla edinilen kodun ilgili yerlere

girilmesi ve gelen elektronik postaya onay verilmesi şeklinde gerçekleşebilmektedir. (DENIC, 2023a; Nominet, 2023a; SIDN, 2024a).

2.3.4. Hesap Güvenliği

Saldırganlar, çeşitli yöntemlerle alan adı sahiplerinin kayıt kuruluşlarındaki hesaplarına erişebilmektedir. Hesaba erişim sağladıktan sonra, kendilerini gizleyerek başka biri adına alan adı tahsis edebilmekte veya mevcut alan adının yetkili ad sunucu bilgilerini değiştirerek DNS Abuse faaliyeti gerçekleştirebilmektedirler.

Bu tür saldırıların önüne geçmek için, kayıt kuruluşları tarafından iki faktörlü kimlik doğrulama yöntemi kullanılabilmektedir. Bu yöntemde alan adı sahibi, kayıt kuruluşundaki hesabına giriş yapmak için kullanıcı adı ve şifresini girdikten sonra doğrulama adımı gerçekleştirmelidir. Bu doğrulama; elektronik posta adresine gönderilen onaylama bağlantısıyla, cep telefonuna gönderilen kısa mesajdaki ya da bunun için geliştirilen yazılımlardaki kodun girilmesi yoluyla gerçekleşebilir. Bunların yanı sıra, anlık bildirim yoluyla da doğrulama gerçekleştirilebilmektedir. Bu yöntemde kod vb. bilgiler iletilmemekte, hesaba giriş yapıldığında hesap sahibi bilgilendirilmekte ve giriş yapan kendisi değilse bunu bildirebilmesi sağlanmaktadır. (ENİSA, 2023, s.39-40; Messaging, Malware and Mobile Anti-Abuse Working Group, 2023, s.8).

2.3.5. Makine Öğrenimi

"Makine Öğrenimi *(Machine Learning)",* yapay zekanın insanların öğrenme şeklini taklit etmesi için veri ve algoritmaların kullanılmasına odaklanan ve doğruluğunu kademeli olarak artıran bir yapay zekâ ve bilgisayar bilimidir (IBM, 2024). Makine öğrenimi teknolojilerinin gelişmesiyle birlikte birçok alanda olduğu gibi DNS Abuse ile mücadelede de makine öğrenimi kullanılmaya başlanmıştır. İlk olarak ".eu" uzantılı alan adları kayıt otoritesi EURid tarafından kullanılmaya başlanılan bu teknoloji

zamanla diğer kayıt otoriteleri tarafından da kullanılmaya başlanmıştır. (CENTR, 2022, s.23; DNS Belgium, 2024a; EURid, 2020; SWITCH, 2021).

Makine öğrenimi sayesinde, DNS Abuse faaliyeti yapılacak muhtemel alan adları hızlı bir şekilde tespit edilebilmekte ve gerekli aksiyonlar alınabilmektedir. Yürütülen süreç ve alınan aksiyonlar ise kayıt otoriteleri nezdinde farklılık gösterebilmektedir. Tespit sonrası kimlik doğrulama süreci yürütülebildiği gibi, alan adının kullanım amacına ilişkin bilgilerin talep edildiği daha geniş çerçeveli süreçler de yürütülebilmektedir. Bunun yanı sıra, alınacak aksiyon ve alınma zamanı da değişiklik gösterebilmektedir. Örneğin, Nominet tespit ettiği alan adlarını direkt durdurmakta, daha sonra alan adı sahibini bilgilendirmektedir. Alan adı sahibi tarafından alan adının meşru amaçlarla tahsis edildiğine dair sunulan bilgi ve belgelerin uygun bulunmaması halinde ise alan adının durdurulması devam etmektedir. ".dk" kayıt otoritesi olan Punktum dk ise, alan adı sahiplerine belirli bir süre tanımakta ve bu sürenin sonunda kimlik bilgileri kanıtlanamazsa alan adını durdurmaktadır. Durdurulma tarihinden otuz gün sonra da alan adı iptal edilmektedir. ".tr" uzantılı alan adlarında ise tespit edilen alan adları tedbir amaçlı durdurulmakta ve hizmet alınan kayıt kuruluşu aracılığıyla alan adı sahibinden kimlik bilgilerini kanıtlaması istenmektedir. Belirlenen sürede belge iletilmez veya iletilen belge uygun bulunmazsa alan adı iptal edilmektedir (Nominet, 2023b; Punktum dk, 2023a).

Makine öğrenimi kapsamında bilgi paylaşımı kayıt otoriteleri arasında farklılık gösterebilmektedir. Örneğin SIDN, makine öğrenimi teknolojisini kullandığı RegCheck sistemine dair ayrıntılı bilgi paylaşırken, Nominet verilecek bilgilerden saldırganların yararlanmaması için ayrıntı vermeyeceğini belirtmektedir (Nominet, 2023b; SIDN, 2023a).

2.3.6. Kurum ve Kuruluşlar ile İş Birliği

Kayıt otoriteleri DNS Abuse ile mücadelede farklı kurum ve kuruluşlar ile iş birliği yapabilmektedir. DNS Abuse tespiti yapan veya bilgisine ulaşan bu kurum ve

kuruluşlar alan adlarını ilgili kayıt otoriteleri ile paylaşmakta ve gerekli aksiyonlar alınmasını sağlamaktadır. İş birliği içerisinde bulunulan kurum ve kuruluşlar kar amacı güden kuruluşlar olabildiği gibi, kamu siber güvenlik kuruluşları, kolluk kuvvetleri ve Bakanlıklar gibi kamu kurum ve kuruluşları da olabilmektedir (DNS Belgium, 2018; DNS Belgium, 2024b; Nominet, 2021, s.4; SIDN, 2024b).

Bu kurum ve kuruluşların DNS Abuse'e karşı mücadeledeki konumu kayıt otoritelerine göre farklılık gösterebilmekte olup, söz konusu farklılık aksiyon alma yetkisinin kimde olduğu ile ilgilidir. Örneğin, Netcraft[8] ile iş birliği içerisinde olan SIDN, uygulanacak tedbir kararını Netcraft'ın bildirimine dair yaptığı inceleme sonucunda kendisi vermekteyken, kolluk kuvvetleri ile hazırladığı prosedür kapsamda iş birliği yapan Nominet'te bu durum daha farklıdır. Nominet, tespit kapsamında sürece pek dahil olmamakta, kolluk kuvvetlerinden gelen bildirimlere göre prosedür çerçevesinde işlem yapmaktadır (Nominet, 2021, s.4; SIDN, 2024b).

Yukarıda belirtilen bazı ccTLD kayıt otoritelerinin iş birliklerinin yanı sıra, beş yüzden fazla TLD'yi koruduğunu belirten ve kar amacı güden bir kuruluş olan CleanDNS Inc ise "Koruyucu Durdurma *(Protective Hold)*" olarak tanımladığı bir işlemi doğrudan yapabilmektedir. Bu işlemde alan adı direkt durdurulmakta, kayıt kuruluşu veya kayıt otoritesi bilgilendirilmektedir (CleanDNS, Inc., 2024a; CleanDNS, Inc., 2024b).

2.3.7. Farkındalık Çalışmaları

Saldırganlar, DNS Abuse faaliyetleriyle kişileri mağdur etmeyi amaçlamaktadır. Bu faaliyetler, kimlik avı/oltalama ve site trafiği yönlendirme türleri aracılığıyla kişilerin kullanıcı adları, şifreleri veya finansal verileri gibi hassas verilerinin ele geçirilmesi şeklinde yürütülebildiği gibi kötü amaçlı yazılımlar vasıtasıyla da yapılabilmektedir.

---

[8] Siber suç tespiti, engelleme ve ortadan kaldırma hizmetlerini veren dünya çapında bir şirkettir. Netcraft'ın misyonu, siber suçları geniş ölçekte tespit etmek ve engellemek ve herkes için daha güvenli bir çevrimiçi deneyim sunmaktır. Daha fazla bilgi için bkz. (https://www.netcraft.com/company/), (05.05.2024)

Kayıt otoriteleri, kayıt kuruluşları ve diğer ilgili kurum ve kuruluşlar tarafından alınan önlemler ve yürütülen çalışmalara rağmen DNS Abuse faaliyetleri azalsa bile varlığını sürdürecektir. Bu nedenle, kişilerin DNS Abuse'a karşı bilinçlendirilmesi önem arz etmektedir. Bu bağlamda, bazı kayıt otoritelerinin kurumsal internet sitelerinde DNS Abuse'a karşı farkındalığı artırmayı hedefleyen içerikler yer almaktadır.

3. ULUSLARARASI KURULUŞLARIN ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI (DNS ABUSE) İLE MÜCADELE UYGULAMALARI

Bu bölümde; ilk olarak ICANN nezdinde yapılan çalışmalar ve düzenlemeler açıklanacak, sonrasında Avrupa Birliği kapsamında yapılan çalışmalar ele alınacaktır.

3.1. ICANN Tarafından Yapılan Çalışmalar

Bölüm 1.5.1. de anlatıldığı üzere ICANN Topluluğu, DNS Abuse tanımı üzerinde fikir birliğine varamamıştır. Bu sebeple, bu kapsamda yapılacak çalışmalar için DNS Abuse kavramı dahil edilmeyerek "DNS Güvenlik Tehditleri Azaltma Programı *(DNS Security Threat Mitigation Program)*" başlığı altında bir program başlatılmıştır. Bu programa göre DNS güvenlik tehditleri; köle bilgisayar ağları, kötü amaçlı yazılım, site trafiği yönlendirme, kimlik avı/oltalama ve diğer türleri yaymak için kullanıldığında istenmeyen elektronik posta olmak üzere beş geniş türde sınıflandırılmıştır (ICANN, 2023f).

ICANN, DNS güvenlik tehditleriyle mücadelede üç yönlü bir yaklaşımı benimsemiştir. Bunlar; konu hakkındaki tartışmalara veri ve uzmanlıkla katkıda bulunulması, ICANN Topluluğu'na yardımcı kaynaklar sağlanması ve kayıt otoriteleri ile kayıt kuruluşu sözleşmelerine bazı yükümlülükler getirilmesidir (ICANN, 2023f).

ICANN, konu hakkındaki tartışmalara veri ve uzmanlıkla katkıda bulunmak için "Alan Adı Kötüye Kullanım Faaliyeti Raporlama *(Domain Abuse Activity Reporting - DAAR)* projesini başlatmış, "Tanımlayıcı Teknoloji Sağlık Göstergeleri *(Identifier Technology Health Indicators - ITHI)*" veya ITHI Metrikleri ile DNS Abuse eğilimlerini analiz etme imkanı sağlamış ve konu hakkında bilgi düzeyini arttırmak için yüz yüze ve çevrimiçi eğitimler vermiştir. Yardımcı kaynaklar sağlanması amacıyla ise, "Alan Adı Güvenliği Tehdidi Bilgi Toplama ve Raporlama *(The Domain Name Security Threat Information Collection and Reporting -DNSTICR)"* projesini başlatmış ve DNS Abuse kapsamında bilgi paylaşımını teşvik etmek ve farklı tarafları

bir araya getirmek için "DNS Abuse Ölçüm Teknolojisine İlişkin Özel İlgi Forumu *(Special Interest Forum on DNS Abuse Measurement Technology)*"nu kurmuştur. Son olarak, DNS Abuse ile mücadeleye ilişkin olarak RA ve RAA'da kayıt otoritesi ve kayıt kuruluşlarına bazı sorumluluklar yüklenmiştir[1](ICANN, 2022c; ICANN, 2023f).

ICANN nezdinde DNS Abuse ile mücadele için yapılan çalışmalar çerçevesinde, DAAR ve DNSTICR projeleri ile RA ve RAA'da kayıt otoritesi ve kayıt kuruluşlarına getirilen yükümlülüklerin önemli olduğu değerlendirilmektedir. Bu kapsamda ilk olarak DAAR ve DNSTICR hakkında bilgi verilecek, daha sonra RA ve RAA'da kayıt otoritesi ve kayıt kuruluşlarına getirilen yükümlülükler incelenecektir.

3.1.1. Alan Adı Kötüye Kullanım Faaliyeti Raporlama (DAAR)

DAAR, TLD uzantılı alan adlarında, alan adı kaydı ve güvenlik tehditlerini inceleyen ve raporlayan bir sistemdir. DAAR'ın genel amacı, sağlıklı politika kararları alınabilmesi için güvenlik tehdidi faaliyetlerini ICANN topluluğuna bildirmektir (ICANN, 2024ç; ICANN, 2024d). Bu genel amacının yanında DAAR'ın özel amaçları da bulunmaktadır. Bu amaçlar:

- TLD'leri, güvenlik tehdidi açısından RBL veri kümelerine dayanarak izlemek.
- DAAR metodolojisini kamuya sunarak alan adı suistimalini önleme çabalarına yardımcı olmak.
- Bir kayıt otoritesinde güvenlik tehditlerinin varlığının veya yaygınlığının belirlenmesine ve raporlanmasına olanak sağlamak.
- Anormal kayıt faaliyetlerinin nedenlerinin belirlenmesinde kayıt otoritelerine veya kayıt kuruluşlarına yardımcı olmak.

[1] ICANN Topluluğunda DNS Abuse kavramı üzerine fikir birliği olmamasına rağmen kayıt otoritesi adayları ile yapılan sözleşme RA ve kayıt kuruluşu adayları ile yapılan akreditasyon sözleşmesi RAA'da yapılan ve 05.04.2024 tarihinden itibaren geçerli olacak son değişiklikte DNS Abuse, kötü amaçlı yazılım, köle bilgisayar ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türler için dağıtım mekanizması olarak kullanıldığında istenmeyen elektronik posta olarak tanımlanmıştır.

- ICANN topluluğunun tüketici güveni ve güven faaliyetlerini desteklemek (ICANN, 2024d).

DAAR, dört tür güvenlik tehdidini incelemektedir. Bunlar; kimlik avı/oltalama, kötü amaçlı yazılım, köle bilgisayar ağları komuta ve kontrol ve istenmeyen elektronik postadır. DAAR projesi, gTLD uzantılı alan adları ile projeye gönüllü olarak dahil olan ccTLD'ler altında tahsis edilen alan adlarını kapsamaktadır. DAAR, güvenlik tehdidi olan alan adlarını kendisi incelememekte, kamuoyunca itibar gören RBL'lere göre tespit etmektedir (ICANN, 2024ç; ICANN, 2024d).

DAAR tarafından kullanılan veriler her gün güncellenmektedir. Alan adı bilgileri, her gün güncellenen TLD bölge dosyalarından alınmaktadır. RBL'lerde yer alan alan adları ise her bir RBL sağlayıcıdan günde birkaç kez alınmaktadır. Her sağlayıcının alan adlarını listelerinden kaldırmak için bir prosedürü bulunmaktadır. Bunlar DAAR içinde izlenmekte ve gerekli düzeltmeler yapılmaktadır (ICANN, 2024d).

DAAR sisteminden toplanan veriler DAAR aylık raporlarını oluşturmak için kullanılmaktadır. Raporlar, verisi bulunan TLD'lerin aylık analizini içermektedir. Raporlar ayrıca kimlik avı/oltalama, kötü amaçlı yazılım, istenmeyen elektronik posta ve köle bilgisayar ağları komuta ve kontrol gibi DAAR'ın ilgi alanına giren güvenlik tehditleri hakkında toplu istatistikler ve zaman serisi analizleri de sunmaktadır (ICANN, 2024ç).

DAAR sistemi tarafından toplanan istatistikler ve anonimleştirilmiş veriler, her bir kayıt otoritesi tarafından kayıt verilerinin veya kötüye kullanım faaliyetlerinin incelenmesi, günlük veya tarihsel olarak raporlanması için bir platform görevi görebilmektedir. Bu toplu veriler şu anda ICANN'in Hizmet Seviyesi Anlaşması İzleme *(Service Level Agreement Monitoring - SLAM)* sistemi kullanılarak kayıt otoritelerine gönderilmektedir. ICANN'in Monitoring API'si, kayıt otoritesi SLAM sistemi tarafından toplanan bilgilerin alınmasına olanak tanımaktadır. Ayrıca, DAAR

incelemelerine ilişkin genel yorumları içeren anonimleştirilmiş raporlar aylık olarak kamuoyu ile paylaşılmaktadır (ICANN, 2024ç).

DAAR'a katılan ccTLD'lere, özelleştirilmiş aylık raporlar sağlanmaktadır. Bu raporlar, ccTLD kayıt otoriteleri tarafından gönderilen verilere dayanan analizleri içermekte ve veriler yalnızca ilgili ccTLD yöneticisiyle paylaşılmaktadır. Her raporda, diğer ccTLD ve gTLD'lerle ilgili veriler anonimleştirilmiş olarak gösterilmektedir. Bu özelleştirilmiş raporlar, ccTLD'lerin diğer TLD'lerle karşılaştırıldığında, RBL sağlayıcıları tarafından listelenen güvenlik tehdidi verileri açısından hangi seviyede olduklarını anlamalarına yardımcı olmayı amaçlamaktadır. Bu belgeler, mevcut DAAR aylık raporlarına ve günlük güvenlik tehdidi puanlarına ek olarak sunulmaktadır (ICANN, 2021d).

3.1.2. Alan Adı Güvenliği Tehdidi Bilgi Toplama ve Raporlama (DNSTICR)

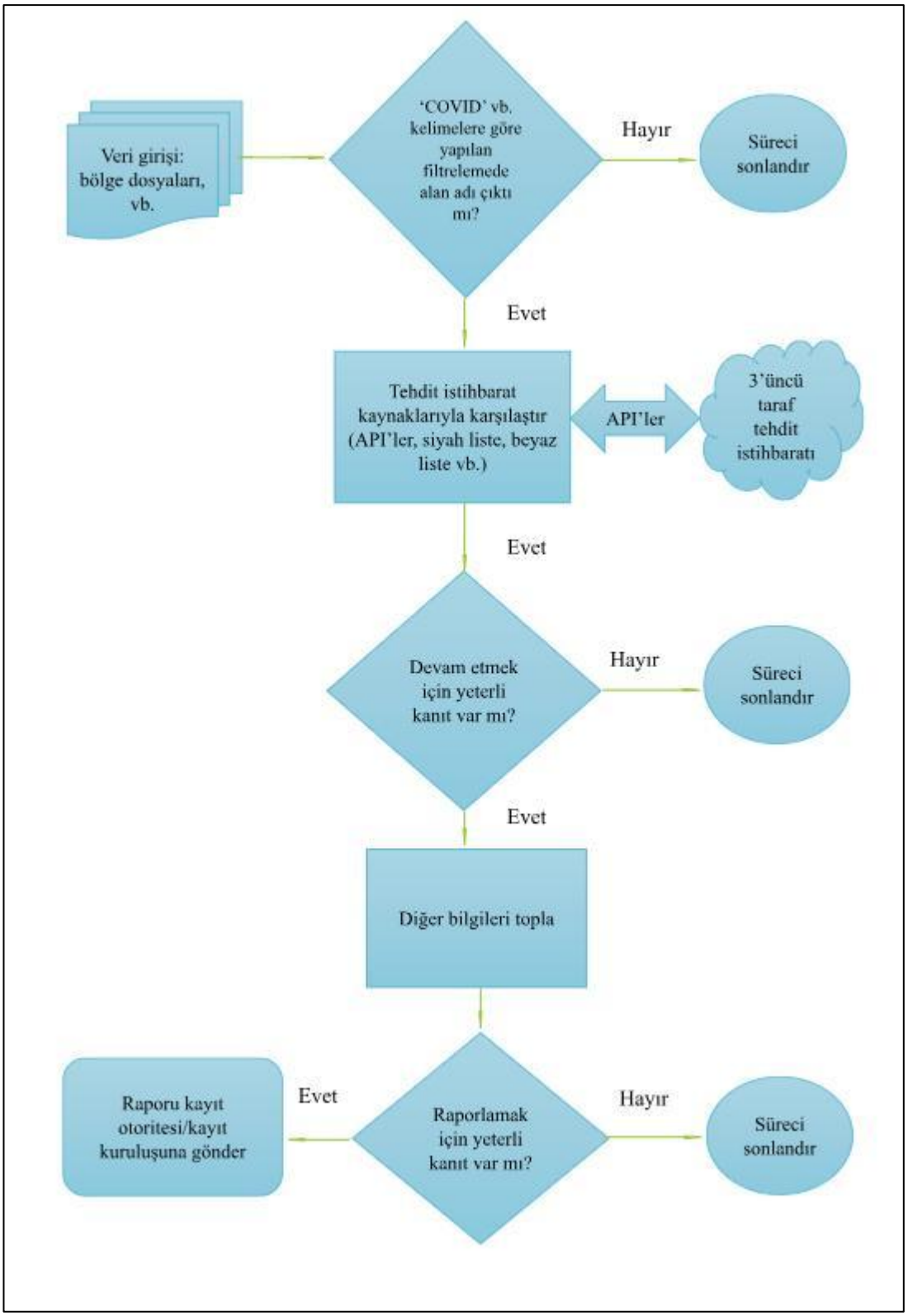
DNSTICR, kimlik avı/oltalama veya kötü amaçlı yazılım faaliyetlerinde kullanılan ve belirli isimleri içeren alan adlarını raporlayan bir projedir. Proje, COVID-19 salgını zamanında, "COVID, korona, pandemi" ve diğer ilgili terimleri içeren ve kimlik avı/oltalama veya kötü amaçlı yazılım faaliyetlerinde kullanılan alan adlarını tespit ederek sorumlu taraflara raporlanması için başlanmıştır. Her rapor, tespite ilişkin kanıtları ve kayıt kuruluşları veya kayıt otoriteleri gibi sorumlu tarafların uygun önlemi almasına yardımcı olabilecek bilgileri içermektedir. Günümüzde DNSTICR kapsamında, "COVID-19" ile ilgili kelimelerin yanında, Ukrayna'daki savaş veya diğer bazı mevcut ve muhtemel krizler kapsamındaki belirli anahtar kelimeler de incelenmektedir (ICANN, 2020; ICANN, 2023f; ICANN, 2024e).

Raporları oluşturmak için, mevcut gTLD bölge dosyalarında belirli anahtar kelimeleri içeren alan adları taranmaktadır. Ortaya çıkan listedeki alan adları hem meşru amaçlı kullanılan hem de kötü amaçlı kullanılan alan adlarını içermektedir. Bu ayrımı yapmak ve kimlik avı/oltalama veya kötü amaçlı yazılım faaliyetlerde kullanılan alan adlarını tespit etmek için; Virus Total, AlienVault OTX, Phishtank ve Google Safe Browsing

gibi tehdit istihbarat kaynaklarına bakılmaktadır. Bu kaynaklar tarafından sağlanan veriler bir alan adının kötü amaçlı olduğunu göstermekte, ancak çoğu durumda çok az kanıta ulaşılmakta veya hiç kanıta ulaşılamamaktadır. Yeterli kanıta ulaşılamama sebebi ise; çoğu alan adının satış yoluyla kar etmek veya reklam yoluyla gelir elde etmek amacıyla tahsis edilmiş olmasıdır. Diğerleri ise, henüz kötü niyetli olarak kullanılmamış yeni tahsis edilen alan adlarıdır. Bu nedenle, zaman içinde bir alan adının durumunun değişmesi mümkün olduğu için, alan adları periyodik olarak yeniden kontrol edilmektedir (ICANN, 2020).

Kötü niyetli faaliyetlere ilişkin güvenilir kanıtlar bulunduğunda, alan adları hakkında "Kayıt Kuruluşu Kötüye Kullanım Raporlama Kılavuzu *(Guide to Registrar Abuse Reporting)*"nda belirtilen raporlama gereklilikleri doğrultusunda daha fazla bilgi toplanmaya devam edilmektedir. Bu raporlama bilgileri; kayıt kuruluşunu ve kötüye kullanım irtibat kişisini, yer sağlayıcı bilgilerini vb. içermektedir. Bu bilgiler, raporların gönderildiği kişilerin alan adına karşı durdurma vb. işlem yapıp yapmama konusunda karar vermelerine yardımcı olmak için toplanmaktadır (ICANN, 2020). Belirtilen bu sürece ilişkin akış diyagramı ICANN tarafından paylaşmıştır:

Şekil 3.1. DNSTICR Raporlama Süreci



Kaynak: ICANN, 2020

DNSTICR raporlama sürecinin sonunda iki farklı formatta dosya oluşmaktadır. İlki; alan adı, IP adresi ve yetkili ad sunucu kayıtları ile her bir tehdit istihbarat kaynağından alınan puanı ve toplamı içeren csv[2] formatındaki özettir. Diğeri ise, her bir alan adı için; mevcut ve uygun olduğunda harici kanıtlara dair bağlantılar da dahil olmak üzere alan adı hakkında daha fazla ayrıntıyı içeren Markdown[3] dosyasıdır (ICANN, 2020)

3.1.3. gTLD Kayıt Otorite ve Kayıt Kuruluşu DNS Abuse Yükümlülükleri

Bölüm 1.3.3. de anlatıldığı üzere ICANN, gTLD kayıt otoritesi olmak isteyen kuruluşlar ve gTLD kapsamında kayıt kuruluşu olarak hizmet vermek isteyenler ile yetkilendirme ve akreditasyon sözleşmeleri yapmaktadır. Kayıt otoritesi adayları ile yapılan sözleşme RA, kayıt kuruluşu adayları ile yapılan akreditasyon sözleşmesi RAA'dır. ICANN ile yapılan her iki sözleşme de taraflara sorumluluklar yüklemektedir. DNS Abuse ile ilgili yükümlülükler de bunlar arasında yer almaktadır. Bu çerçevede, gTLD kayıt otoriteleri ve kayıt kuruluşlarının DNS Abuse kapsamında sözleşmede yer alan yükümlülükleri sırasıyla açıklanacak ve bu yükümlülüklerin yerine getirilmesine ilişkin olarak ICANN tarafından hazırlanan tavsiye metinleri[4] ışığında yapılması beklenen eylemler ifade edilecektir.

---

[2] Verilerin tablo yapısında kaydedilmesine olanak tanıyan özel bir biçimle kaydedilmiş metin dosyalarıdır. Daha fazla bilgi için bkz. (https://www.howtogeek.com/348960/what-is-a-csv-file-and-how-do-i-open-it/), (28.02.2024)

[3] Düz metin belgelerine biçimlendirme öğeleri eklemek için kullanılan bir işaretleme dilidir. Microsoft Word gibi uygulamalarda, kelimeleri ve cümleleri biçimlendirmek için ilgili bölümlere tıklamak yeterliyken Markdown ile biçimlendirilmiş bir dosya oluşturduğunda, hangi sözcük ve ifadelerin farklı görünmesi gerektiğini belirtmek için metne Markdown sözdizimi eklenmesi gerekmektedir. Daha fazla bilgi için bkz. (https://www.knowledgehut.com/blog/web-development/what-is-markdown), (28.02.2024)

[4] ICANN tavsiye metninde, örnek olarak belirtilen işlemleri yapan kayıt otoritesi ve kayıt kuruluşlarının ilgili yükümlülükleri büyük ölçüde yerine getireceği ancak bu işlemlerin bir veya daha fazlasının gerçekleştirilmesinin yükümlülüklerin mutlaka yerine getirildiği anlamına gelmeyeceği belirtilmektedir. Her halükarda, ICANN tarafından bir soruşturma başlatıldığında kayıt otoritesi ve kayıt kuruluşlarının ilgili RAA ve RA gerekliliklerine uyduğunu gösteren kanıtları sunması gerekmektedir.

3.1.1.1. gTLD Kayıt Otoritesi DNS Abuse Yükümlülükleri

RA, *"Kayıt Otoritesi Birlikte Çalışabilirlik ve Süreklilik Şartnameleri (Registry Interoperability And Continuity Specifications)"* başlıklı Şartname 6'nın *"Kötüye Kullanımı Azaltma (Abuse Mitigation)"* başlıklı dördüncü maddesi kapsamında, kayıt otoritesine bazı sorumluluklar yüklenmiştir:

> *"**4.1. Kötüye Kullanım İletişimi**. Kayıt Otoritesi, geçerli bir elektronik posta adresi veya web formu ve posta adresi de dahil olmak üzere doğru iletişim bilgilerini ve DNS Abuse da dahil olmak üzere TLD'deki kötü niyetli davranışlarla ilgili bildirimleri değerlendirecek sorumlu irtibat noktasını ICANN'e bildirecek, internet sitesinde yayınlayacak ve bu iletişim bilgilerindeki herhangi bir değişikliği ICANN'e derhal iletecektir. Bu tür bildirimlerin alınması üzerine Kayıt Otoritesi, bildirimleri aldığını bildirim yapan tarafa iletecektir. Bu Sözleşmenin amaçları doğrultusunda, "DNS Abuse", SAC115 Bölüm 2.1'de (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>) tanımlandığı şekilde kötü amaçlı yazılım, köle bilgisayar ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türler için dağıtım mekanizması olarak kullanıldığında istenmeyen elektronik posta olarak tanımlanmıştır.*
>
> ***4.2. DNS Abuse'un Azaltılması**. Kayıt Otoritesi, TLD'de kayıtlı bir alan adının DNS Abuse için kullanıldığını makul kanıtlara dayanarak tespit ederse, alan adının DNS Abuse için kullanılmasının durdurulması veya başka şekilde engellenmesi için gerekli olan uygun azaltma eylemlerini derhal gerçekleştirmelidir. Bu tür eylemler asgari olarak şunları içerecektir: (i) DNS Abuse için kullanılan alan adlarının ilgili kanıtlarla birlikte hizmet veren kayıt kuruluşuna yönlendirilmesi; veya (ii) Kayıt Otoritesinin uygun gördüğü durumlarda doğrudan işlem yapılması. Eylemler, DNS Abuse'tan kaynaklanan zararın büyüklüğü ve ilgili ikincil zarar olasılığı dikkate alınarak, her bir vakanın koşullarına bağlı olarak değişebilir.*

> ***4.3. Sahipsiz Birleştirici Kayıtlarının[5] Kötü Amaçlı Kullanımı****. Kayıt Otoritesi, bu tür kayıtların kötü amaçlı kullanımına dair kanıta dayalı bildirim aldığında, sahipsiz birleştirici kayıtlarını (https://www.icann.org/en/committees/security/sac048.pdf adresinde tanımlandığı şekilde) kaldırmak için harekete geçecektir."* (ICANN, 2024a).

RA, "Kamu Yararı Taahhütleri (*Public Interest Commitments)*" başlıklı Şartname 11'de, kayıt otoritelerine aşağıda yer alan sorumluluklar yüklenmiş ve bu sorumlulukların yerine getirilmemesi durumunda sözleşmenin feshi dahil bazı yaptırımların uygulanabileceği belirtilmiştir:

> *"3. Kayıt Otoritesi, ICANN tarafından oluşturulan (https://www.icann.org/picdrp adresinde yayınlanan) ve ICANN tarafından zaman zaman esasa etkisi olmayan açılardan revize edilebilecek olan Kamu Yararı Taahhüdü Uyuşmazlık Çözüm Süreci (PICDRP) aracılığıyla uygulanabilir olan aşağıdaki belirli kamu yararı taahhütlerini yerine getirmeyi kabul eder. Kayıt Otoritesi PICDRP'ye uyacaktır. Kayıt Otoritesi, herhangi bir PICDRP panelinin kararını takiben ICANN'in uygulayacağı her türlü yaptırımı (şüpheye mahal vermemek için Sözleşmenin 4.3(e) Bölümü uyarınca Kayıt Otoritesi Yetki Sözleşmesi feshi de dahil olmak üzere her türlü makul yaptırım) uygulamayı ve bunlara uymayı ve bu tür bir karara bağlı kalmayı kabul eder.*
>
> a. *Kayıt Otoritesi, Kayıt Kuruluşu ile alan adı sahibi arasında yapılan sözleşmeye; alan adı sahiplerinin kötü amaçlı yazılım yaymasını, köle bilgisayar ağlarını kötüye kullanmasını, kimlik avı/oltalama, korsanlık, ticari marka veya telif hakkı ihlali, hileli veya aldatıcı uygulamalar, sahtecilik veya yürürlükteki yasalara aykırı başka faaliyetlerde*

[5] Birleştirici kayıtlar, alan adı yetkili ad sunucu bilgisi ile bu sunucunun IP adres bilgisinin birleşik olarak kayıt edilmesidir. Bu sayede, yinelemeli çözümleyici TLD sunucusuna istek gönderdiğinde TLD sunucusu ilgili IP adres bilgisini iletebilmektedir. Sahipsiz birleştirici kaydı ise, alan adı yetkili ad sunucu bilgisinin TLD bölgesinde silinmesine rağmen sunucu IP adres bilgisinin silinmemesi sonucu oluşan durumdur.

bulunmasını yasaklayan ve yürürlükteki yasalar ve ilgili prosedürlerle tutarlı olarak alan adının durdurulması da dahil olmak üzere bu tür faaliyetler için sonuçlar doğuran bir hüküm eklemesini gerektiren bir hükmü, Kayıt Otoritesi-Kayıt Kuruluşu sözleşmesine dahil edecektir.

b. *Kayıt Otoritesi, TLD'deki alan adlarının DNS Abuse için kullanılıp kullanılmadığını değerlendirmek üzere periyodik olarak teknik bir analiz gerçekleştirecektir. Kayıt Otoritesi, tespit edilen DNS Abuse ve periyodik güvenlik kontrolleri sonucunda alınan önlemler hakkında istatistiksel raporlar tutacaktır. Kayıt Otoritesi, kanunlarca daha kısa bir süre gerekmedikçe veya ICANN tarafından aksi belirtilmedikçe, bu raporları sözleşme süresi boyunca saklayacak ve talep üzerine bunları ICANN'e sunacaktır…"* (ICANN, 2024a).

RA'nın Şartname 6'nın, 4 üncü maddesi, genel üst düzey alan adındaki kötü niyetli davranışlarla ilgili taleplerin ele alınması için iletişim bilgilerinin yayınlanmasını ve ICANN'e sunulmasını gerektirmektedir. Ayrıca, kötü niyetli davranışlarla bağlantılı olarak kullanıldığında sahipsiz birleştirici kayıtlarının kaldırılmasıyla ilgili gereklilikleri de içermektedir.

ICANN tarafından yayınlanan tavsiye metnine göre; Şartname 6, madde 4.1. kapsamında kayıt otoritesinin, DNS Abuse da dahil olmak üzere TLD'deki kötü niyetli davranış iddiasında bulunan herhangi bir tarafın bildirim göndermesini kolaylaştırmak için elektronik posta adresi veya web formu, posta adresi ve bu tür bildirimleri ele almak için sorumlu irtibat noktası yayınlaması gerekmektedir. Kayıt otoritesinin, bildirimlerin sorunsuz bir şekilde gönderildiği "Kötüye Kullanım Bildir" veya kötüye kullanım iletişim bilgilerini içeren "İletişim" sayfası bağlantılarını, internet sitesi ana sayfasında görünür bir alana yerleştirmesi ICANN tarafından uygun kabul edilmektedir. Ayrıca, bildirimin alınmasından sonra kayıt otoritesi tarafından bildirimde bulunan tarafa, bildirimin alındığına dair bilgi verilmesi gerekmektedir. Bu alındı bilgisi, kötüye kullanım bildiriminde bulunan tarafa gönderilebileceği gibi bildirim işleminin tamamlanmasından sonra ekranda görüntülenebilir. Alındı

bilgisinin, bildirimde bulunan kişinin kötüye kullanım bildiriminin gönderildiğini kanıtlayabilmesi için yeterli bilgiyi içermesi gerekmektedir. Alındı bilgisinde asgari olarak; kayıt otoritesi, bildirime konu alan adı veya adları ve gönderildiği tarih belirtilmelidir (ICANN, 2024f).

RA, Şartname 6, madde 4.2'de belirtilen makul kanıt ifadesi tavsiye metnine göre; kayıt otoritesinin, alan adı üzerinden bir veya daha fazla DNS Abuse türünün gerçekleştirildiğini tespit etmek için sahip olması gereken bilgi olarak açıklanmıştır. Kayıt otoriteleri makul kanıtı, kötüye kullanım bildirimi vasıtasıyla veya Şartname 11 madde 3(b) kapsamında DNS Abuse için kullanılan alan adlarını belirlemek için teknik analiz gerçekleştirmesi sonucunda elde edebilmektedir. Bunların yanı sıra, kolluk kuvvetleri, kayıt otoritesinin güvenilir ve tanınmış kaynakları ve diğer kaynaklar tarafından da makul kanıt sunulabilmektedir (ICANN, 2024f).

Kayıt otoritesinin gelen bildirimlere binaen DNS Abuse'a ilişkin bir soruşturma başlatmak için yeterli bilgiye sahip olması gerekmektedir. Bu sebeple, kötüye kullanım bildiriminde bulunanların mümkün olduğunca fazla bilgi sağlamaları teşvik edilmelidir. Gelen bildirimin yeterli bilgiyi içermemesi halinde ise, kayıt otoritesinin bildirime konu alan adının DNS Abuse için kullanılıp kullanılmadığını tespit etmek için yeterli bilgiye erişim imkânı olması halinde, makul kanıta sahip olunduğu kabul edilebilecektir (ICANN, 2024f).

Meşru bir amaçla tahsis edilen ve alan adı sahibinin bilgisi ve rızası olmadan DNS Abuse'e konu olan bir alan adı "Güvenliği İhlal Edilmiş Alan Adı (*Compromised Domain)*" olarak adlandırılmaktadır. Bu durumlarda, alan adının kayıt otoritesi veya kayıt kuruluşu tarafından durdurulması halinde tali zararlar oluşabileceği için uygun azaltıcı eylem farklılık göstermelidir. Bu durum, DNS Abuse'un üçüncü derece veya daha üst dereceli alan adlarıyla ilişkili olduğu durumlarda da geçerlidir. Kayıt otoriteleri ve kayıt kuruluşları ikinci veya üçüncü derece alan adı düzeyinde işlem yapabilmektedir. Bu nedenle, ikinci veya üçüncü seviye alan adı durdurulursa, yalnızca DNS Abuse ile ilişkili olan değil, alan adıyla ilişkili tüm içerik ve hizmetlerde

durdurulmuş olacaktır. Bu durumlarda, alan adının kayıt otoritesi ve kayıt kuruluşu tarafından eylemde bulunulmadan alan adı sahibine, internet site yöneticisine ve/veya yer sağlayıcısına bildirimde bulunmak tercih edilebilecektir (ICANN, 2024f).

Makul kanıtlar elde edildikten sonra kayıt otoritesinin, alan adının DNS Abuse için kullanılmasını durdurmak veya başka bir şekilde engellemek için gerekli olan uygun azaltma eylemlerini derhal gerçekleştirmesi gerekmektedir. Uygun azaltma eylemlerini hızlı bir şekilde belirlemek için, DNS Abuse'un neden olduğu zararın büyüklüğü ve ilişkili tali zarar[6] olasılığının dikkate alınarak olayın kendi koşulları içerisinde incelenmesi önemlidir. Kayıt otoritesinin ayrıca, eyleme geçme konusunda hangi tarafın daha uygun olabileceğini değerlendirmesi gerekmektedir. Burada belirtilen taraflar; kayıt otoritesi, alan adına hizmet veren kayıt kuruluşu ve ilgili başka taraflardır. Örneğin, güvenliği ihlal edilmiş sistemler söz konusu olduğunda, etkilenen sistemlere erişim sağlayan alan adı sahibi veya yer sağlayıcısı sorunu daha uygun bir şekilde çözebilir. Çünkü, alan adının durdurulması meşru içerik üzerinde tali zarara neden olabileceğinden bu gibi durumlarda kayıt otoritesinin öncelikli olarak kayıt kuruluşuna konuyu yönlendirmesi daha uygun olacaktır. Öte yandan, köle bilgisayar ağları çoğaltmak için kullanılan alan adı oluşturma algoritmaları gibi birçok alan adı veya kayıt kuruluşunu kapsayan büyük ölçekli tehditleri ele almak için en iyi taraf kayıt otoritesi olabilmektedir (ICANN, 2024f).

DNS Abuse faaliyetini durdurmak veya engellemek için uygun azaltma eylemini belirlemek koşullara göre değişebilmektedir. Benzer bir şekilde, DNS Abuse kapsamında alan adını soruşturmak ve eylemde bulunmak için uygun süreler de farklılık gösterebilmektedir. Bu da bir eylemin hızlı olarak kabul edilmesi için sabit bir sürenin belirlenmesini zorlaştırmaktadır. Bu sebeple kayıt otoriteleri, alan adlarının DNS Abuse için kullanıldığına dair iddialara karşı mağdur edilenlerin uğrayacağı

[6] Burada ifade edilen tali zarar, alan adı sahibinin bilgisi ve rızası olmadan alan adının DNS Abuse faaliyetine konu olması ve bunun sonucu alan adının durdurulması halinde, alan adı sahibinin uğrayacağı zarar olarak açıklanabilir. Bu zarara örnek olarak, alan adının yasal olan içeriklerine de erişilememesi veya alan adıyla ilişkili elektronik posta hizmetinin kullanılamaz hale gelmesi verilebilir.

zararı da dikkate alarak gerekli özeni göstermelidir. Bu çerçevede, ICANN tarafından açılan bir soruşturmada kayıt otoritesinin, belirli koşullar altında eylemlerin nasıl hızlı alındığını açıklaması gerekecektir. Açıklamanın ve ilgili koşulların ICANN tarafından incelenmesi sonucunda, eylemlerin makul ölçüde hızlı olup olmadığına dair karar verilecektir (ICANN, 2024f).

ICANN tavsiye metninde, kayıt otoritelerinin yerine getirmesi beklenen eylemlere dair üç farklı örnek verilmiştir. Bu örneklerde belirtilen sürelerin bağlayıcı olmayıp örnek niteliğinde olduğu ifade edilmiş ve bir olayda daha fazla zaman harcanmasının bir ihlal olmayacağı belirtilmiştir. Diğer taraftan, çok sayıda kişinin zarar görebileceği büyük ölçekli tehditlerde kayıt otoritesinin daha hızlı hareket etmesi gerekebilecektir. Kayıt otoritesinden beklenen ise, DNS Abuse olayının tespiti için en kısa sürede soruşturma başlatması ve uygun eylemlerde bulunmasıdır (ICANN, 2024f).

Birinci örnekte kayıt otoritesi, bir kredi birliğinden kötüye kullanım web formu aracılığıyla bir bildirim almıştır. Bu bildirimde, alan adının altı gün önce tahsis edildiği ve alan adı üzerinde kimlik avı/oltama yapıldığı belirtilmiştir. Ayrıca, son kullanıcı kimlik bilgilerinin talep edildiğini gösteren bir internet sayfasının ekran görüntüsü de bildirime eklenmiştir. Tavsiye metnine göre kayıt otoritesinden, bildirimi almasından sonra soruşturma başlatması ve soruşturmanın iki iş günü içerisinde DNS Abuse tespiti şeklinde sonuçlandırılması beklenmektedir. Yapılan tespitten sonra kayıt otoritesi kayıt kuruluşuna, sahip olduğu bilgileri iletecek ve alan adının DNS Abuse için kullanımını durdurmak veya başka bir şekilde engellemek için uygun önlemleri araştırmasını ve uygulamasını içeren bir talepte bulunacaktır. Bu talebin belirli bir tarihe kadar yerine getirilmesi gerektiği de belirtilecektir (ICANN, 2024f).

İkinci örnekte kayıt otoritesi, kolluk kuvvetlerinden bir grup alan adının köle bilgisayar ağları ile ilişkili bir alan adı oluşturma algoritmasına dahil olduğuna veya olacağına dair kanıt içeren bir bildirim almaktadır. Köle bilgisayar ağları, bazı kayıtlı alan adlarını içermekle birlikte genel olarak henüz tahsis edilmemiş alan adlarından oluşmaktadır. Tavsiye metnine göre, örnek kapsamında kayıt otoritesi tarafından

başlatılan soruşturmasının DNS Abuse tespiti ile sonuçlanmasından sonraki altı saat içinde, kolluk kuvvetleri tarafından talep edilen veya kolluk kuvvetleri ile daha önce anlaşılan eylemlerin gerçekleştirilerek DNS Abuse'un durdurulması sağlanmalıdır. Kolluk kuvvetlerinin talebi üzerine kayıt otoritesi, DNS Abuse'a konu olan tahsisli alan adlarını, sahibi olduğu yetkili ad sunucusuna veya sunucularına yönlendirmelidir. Kayıt otoritesi ayrıca, kolluk kuvvetleri tarafından talep edilmesi halinde köle bilgisayar ağları ile ilişkili daha önce tahsis edilmemiş alan adlarını kendisi oluşturmalıdır. Alan adı oluşturma işleminin ICANN'in Güvenlik Müdahale Feragatnamesi *(Security Response Waiver - SRW*[7]*)* yoluyla izin gerektirdiğine dikkat edilmeli ve sözleşmeye dayalı bir feragatname almak için zamanında talepte bulunulmalıdır. Metinde ayrıca, SRW için olaydan sonra makul olan en kısa sürede başvurulabileceği ve ICANN'in kolluk kuvveti operasyonuna desteğin sağlanması için geriye dönük bir feragat ile yanıt verebileceği belirtilmektedir[8](ICANN, 2024f).

Üçüncü örnekte, kayıt otoritesinin Şartname 11 madde 3(b) çerçevesinde DNS Abuse faaliyetlerini araştırmak için yaptığı teknik analiz kapsamında, bir alan adına ait internet sayfasının kötü amaçlı yazılım yaymak için kullanıldığı, internet sitesinin geri kalanında ise uygun içeriklerin bulunduğu tespit edilmiştir. Alan adı üç yıl önce tahsis edilmiştir. Tavsiye metnine göre, örnek kapsamında kayıt otoritesi tarafından başlatılan soruşturmasının DNS Abuse tespiti ile sonuçlanmasından ve alan adının güvenliği ihlal edilmiş olarak tespit edilmesinden sonraki üç saat içinde, kayıt otoritesi tarafından alan adına hizmet veren kayıt kuruluşuna ilgili tüm bilgilerin ve belirli bir tarihe kadar eylemde bulunma talebinin yer aldığı bir bildirimde bulunulmalıdır. Kayıt

---

[7] Güvenlik müdahale feragat hizmeti, gTLD kayıt otoritelerinin bir gTLD ve/veya DNS'e yönelik mevcut veya yakın bir güvenlik olayını azaltmak veya ortadan kaldırmak için alabileceği veya aldığı önlemler için sözleşmeye dayalı bir feragatname talep etmesi için oluşturulmuştur. Sözleşmeye dayalı feragat, olaya müdahale etmek adına gerekli süre boyunca, RA'nın belirli bir hükmüne uymaktan muafiyettir. Daha fazla bilgi için bkz. (https://www.icann.org/resources/pages/srw-registries-requests-en), (05.03.2024)

[8] gTLD kayıt otoriteleri ile kolluk kuvvetlerinin, köle bilgisayar ağları ile kötü amaçlı yazılım kapsamındaki iş birliğine ilişkin daha fazla bilgi için bkz. (https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf), (05.03.2024)

kuruluşu bildirime binaen alan adı sahibini bilgilendir. Alan adı sahibi de içerik yönetim sistemini güncelleyerek DNS Abuse faaliyetini sonlandırır (ICANN, 2024f).

RA Şartname 6, madde 4.3 kapsamında kayıt otoritesinin, kötü niyetli davranışlarla bağlantılı olarak kullanıldığında sahipsiz birleştirici kayıtlarının kaldırılmasıyla ilgili yükümlülüğü bulunmaktadır. ICANN tavsiye metninde, bu madde çerçevesinde bir öneri bulunmamaktadır. İlgili maddede yer alan bağlantıda da politika tavsiyesi görülmemiştir.

RA, "Kamu Yararı Taahhütleri" başlıklı Şartname 11 madde 3(b) kapsamında, ICANN tarafından 2017 yılında bir tavsiye metni yayınlanmıştır. Bu metin yayınlandığı zaman RA'da DNS Abuse yerine güvenlik tehditleri ifadesi kullanıldığından metin içerisinde de güvenlik tehditleri ifadesi yer almaktadır[9] (ICANN, 2017b).

Tavsiye metnine göre teknik analiz, veri akışlarını inceleyerek veya "Alan Adı İtibar Hizmet Sağlayıcıları *(Domain Reputation Service Providers)"* tarafından yapılan otomatik analizlere eşdeğer analizlerin yapılması yoluyla gerçekleştirilebilir. Belirtilen eylemler, kayıt otoritesi tarafından doğrudan yapılabileceği gibi, alan adı itibar hizmet sağlayıcıları aracılığıyla da yapılabilecektir (ICANN, 2017b).

Tavsiye metninde alan adı itibar hizmet sağlayıcıları, alan adları ve bunların güvenlik tehditleri ile ilişkileri hakkındaki veri tabanlarını muhafaza eden veya yöneten ve "itibar hizmetleri" olarak bilinen hizmetleri sağlayan kuruluşlar şeklinde ifade edilmiştir. İtibar hizmetleri ise, alan adı kayıt bilgilerinin, alan adı kötüye kullanımıyla ilişkili olduğu bilinen diğer verilerle ilişkilendirmek için yapılan veri analizine dayanmaktadır. Bu hizmetlerde; sürekli güncellenen engelleme listeleri, kötü amaçlı yazılım imzaları ve doğrulanmış kaynaklardan bildirilen kötüye kullanım verileri

[9] RA'ya DNS Abuse ifadesi, 21 Ocak 2024'te ICANN Yönetim Kurulu tarafından onaylanan ve 5 Nisan 2024 tarihinden itibaren geçerli olan değişiklikler ile girmiştir.

toplanmaktadır. Toplanan veriler analiz edilmekte, tehdit kategorisine göre ayrılmakta ve eski bilgilere göre yanlış tespitin yapılmasını önlemek için alan adlarının geçici doğası hesaba katılarak ağırlıklı bir itibar puanı hesaplanmaktadır. (ICANN, 2017b).

ICANN, kayıt otoritelerinin alan adı itibar hizmet sağlayıcılarını tercih ederken veya hizmetleri kendilerini yerine getirirken aşağıdaki kriterleri göz önünde bulundurması gerektiğini belirtmiştir:

- İtibar hizmeti, kayıt otoritesinin istediği güvenlik tehditlerini kapsıyor mu?
- İtibar hizmeti, bir alan adının alan adı itibar hizmeti sağlayıcısının veri tabanına veya veri tabanlarına dahil olması üzerine kayıt otoritesine bildirim gönderiyor mu?
- Sorguları otomatikleştirmek için API gibi bir sistem var mı?
- Alan adı itibar hizmeti sağlayıcısı tarafından alan adı itibar verilerinin hazırlanmasında kullanılan metodoloji ve kriterleri kamuya açıklanıyor mu? (Örneğin, adların veri tabanlarına nasıl eklendiği, bunların ne kadar süre tutulabileceği ve veri tabanlarından nasıl kaldırıldığı) (ICANN, 2017b).

Kayıt otoritelerinin teknik analizlerini ayda en az bir kere olmak üzere makul aralıklarla yapması gerektiği tavsiye metninde belirtilmiştir. Güvenlik tehdidi faaliyetleri için tahsis edilmiş alan adlarının hızlı bir şekilde tespit edilmesi için ise günlük olarak analiz yapılması önerilmiştir. Yapılan analizler sonucu tespit edilen güvenlik tehditlerinin sayısı ve periyodik güvenlik kontrolleri sonucunda alınan önlemlere ilişkin istatistiksel raporlar, kanunlarca daha kısa bir süre gerekmedikçe veya ICANN tarafından aksi belirtilmedikçe sözleşme süresi boyunca saklanacaktır. İstatistiksel raporların genel olarak içermesi gerekenler tavsiye metninde şu şekilde belirtilmiştir:

- Analiz sırasında incelenen alan adlarının sayısı
- Potansiyel tehdit içeren alan adlarının listesi
- Kötü amaçlı yazılım ve köle bilgisayar ağları gibi tespit edilen tehdit türleri

- Tehditlere yanıt olarak alınan önlemlerin türü (durdurma vb.)
- Tehdidin durumu (açık/beklemede/kapalı) ve alınan önlemlere ilişkin istatistikler
- IP adresi, coğrafi konum ve alan adı sahibi bilgileri gibi tehditlerle ilgili ek bilgiler
- Trendler ve uyarılar (ICANN, 2017b)

ICANN, RA'da belirtilen yükümlülüklerin ihlali kapsamında kayıt otoritelerine soruşturma açabilmektedir. Bu soruşturmalar, gelen şikayet sebebiyle olabildiği gibi, doğrudan ICANN tarafından da başlatılabilmektedir. Soruşturma sürecinde kayıt otoritesi tarafından ihlal düzeltilmezse ICANN tarafından kamuya açık bir ihlal bildirimi yayınlanmaktadır (ICANN, 2012). İhlal bildiriminde belirtilen tarihe kadar ilgili yükümlülükler yerine getirilmediği durumda, RA madde 4.3 kapsamında kayıt otoritesinin sözleşmesi feshedilebilmektedir. ICANN bildirimde belirtilen süreyi uzatabilmektedir (ICANN, 2024g).

Örneğin, ICANN tarafından, 12 Temmuz 2018 tarihli ve Şartname 6'nın "Kötüye Kullanım İletişimi" başlıklı madde 4.1. kapsamındaki yükümlülük ihlalini içeren bir kamuya açık ihlal bildirimi yayımlanmıştır. Bildirimde, 11 Ağustos 2018 tarihine kadar belirtilen ihlallerin düzeltilmesi istenmiş, daha sonra süre 1 Ekim 2018'e kadar uzatılmıştır. İhlallerin düzeltildiği bilgisi ICANN tarafından 3 Ekim 2018 tarihinde ilan edilmiştir. (ICANN, 2018; ICANN, 2024g).

3.1.1.2. gTLD Kayıt Kuruluşu DNS Abuse Yükümlülükleri

RAA, *"Kayıt Kuruluşunun Kötüye Kullanım İletişimi ve Kötüye Kullanım Bildirimlerini Soruşturma Görevi (Registrar's Abuse Contact and Duty to Investigate Reports of Abuse)"* başlıklı ve 3.18 sayılı madde kapsamında, kayıt kuruluşuna aşağıda yer verilen bazı sorumluluklar yüklenmiştir:

*"**3.18.1** Kayıt Kuruluşu, DNS Abuse ve yasa dışı faaliyet bildirimleri de dahil olmak üzere, hizmet verilen alan adlarıyla ilgili kötüye kullanım bildirimleri almak için bir kötüye kullanım irtibat noktası oluşturacaktır. Kayıt Kuruluşu, bu tür bildirimleri almak için internet sitesinin ana sayfasında (veya ICANN tarafından belirlenebilecek başka bir yerde) görünür ve kolayca erişilebilen bir elektronik posta adresi veya web formu yayınlayacaktır. Bu tür bildirimlerin alınması üzerine Kayıt Kuruluşu, bildirimleri aldığını bildirim yapan tarafa iletecektir. Kayıt Kuruluşu, herhangi bir kötüye kullanım bildirimini araştırmak ve uygun şekilde yanıtlamak için makul ve hızlı adımlar atacaktır. Bu Sözleşmenin amaçları doğrultusunda, "DNS Abuse", SAC115 (<https://www.icann.org/en/system/files/files/sac-115en.pdf>) Bölüm 2.1'de tanımlandığı şekilde kötü amaçlı yazılım, bot ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türler için dağıtım mekanizması olarak kullanıldığında istenmeyen elektronik posta anlamına gelir.*

***3.18.2** Kayıt Kuruluşu, hizmet verdiği bir alan adının DNS Abuse için kullanıldığına dair makul kanıtlara sahip olduğunda, alan adının DNS Abuse için kullanılmasını durdurmak veya başka şekilde engellenmesi için gerekli olan uygun azaltma eylemlerini derhal gerçekleştirmelidir. Eylemler, DNS Abuse'tan kaynaklanan zararın büyüklüğü ve ilgili ikincil zarar olasılığı dikkate alınarak, her bir vakanın koşullarına bağlı olarak değişebilir.*

***3.18.3** Kayıt Kuruluşu, kurulmuş olduğu veya fiziksel bir ofisinin bulunduğu bölgenin ulusal veya bölgesel hükümeti tarafından yetkilendirilmiş kolluk kuvvetleri, tüketici koruma makamı, yarı hükümet[10] veya diğer benzer yetkililer tarafından yasa dışı faaliyet bildirimlerini almak için, yedi gün yirmi dört saat takip edilen bir elektronik posta adresi ve telefon numarası da dahil olmak üzere özel bir kötüye kullanım irtibat noktası oluşturacak ve sürdürecektir. Bu irtibat noktalarına gönderilen yasa dışı faaliyet bildirimleri, Kayıt Kuruluşu*

[10] Kanunla veya genel uygulamayla hem kamu hem de özel sektörün bazı hukuki özelliklerinin tahsis edildiği karma bir kuruluşlardır. Daha fazla bilgi için bkz. (https://www.everycrsreport.com/reports/RL30533.html), (25.02.2024)

*tarafından bildirime yanıt olarak gerekli ve uygun önlemleri alma yetkisi verilmiş bir kişi tarafından 24 saat içinde incelenmelidir. Bu tür bildirimlere yanıt verirken, Kayıt Kuruluşunun yürürlükteki yasalara aykırı herhangi bir işlem yapması gerekmeyecekt*ir.

***3.18.4** Kayıt Kuruluşu, kötüye kullanım bildirimlerinin alınması, işlenmesi ve izlenmesine ilişkin prosedürlerinin bir açıklamasını internet sitesinde yayınlayacaktır. Kayıt Kuruluşu bu tür tüm bildirimleri aldığını ve bunlara yanıt verdiğini belgeleyecektir. Kayıt Kuruluşu, bu tür bildirimlerle ilgili kayıtları en az iki (2) yıl veya yürürlükteki yasaların izin verdiği en uzun süre boyunca saklayacak ve bu süre boyunca bu kayıtları makul bir bildirim üzerine ICANN'e sunacaktır"* (ICANN, 2024b).

ICANN tarafından yayınlanan tavsiye metnine göre, madde 3.18.1 kapsamında kayıt kuruluşunun; DNS Abuse veya yasa dışı faaliyet iddiasında bulunan tarafların bildirimlerini kolayca iletebilmeleri için internet sitesi ana sayfasında açıkça görülebilen bir elektronik posta adresi veya web formu yayınlanması gerekmektedir. Web formu yoluyla kötüye kullanım bildirimi göndermek isteyen tarafların oturum açmadan bu işlemi yerine getirebilmeleri sağlanmalıdır (ICANN, 2024f).

Kayıt kuruluşu internet sitesi ana sayfasında, "Kötüye Kullanım Bildir" veya kötüye kullanım irtibat bilgisini içeren "İletişim" sayfasında bir bağlantının açıkça yer alması ve bildirimde bulunanların bu sayfalarda kolayca bildirim yapabilmesine olanak tanınması tavsiye metnine göre yeterli kabul edilmektedir. Ayrıca, kötüye kullanım bildiriminde bulunan taraflara kayıt kuruluşu tarafından bildirimin alındığına dair bilgi verilmelidir. Bu alındı bilgisi, bildirimde bulunan tarafa gönderilebilir veya bildirim işleminin tamamlanmasından sonra ekranda görüntülenebilir. Alındı bilgisinin, bildirim yapan tarafın kötüye kullanıma dair yaptığı bildirimi kanıtlayabilmesi için yeterli bilgiyi içermesi gerekmektedir. Alındı bilgisinde asgari olarak; kayıt kuruluşu, bildirime konu alan adı veya adları ve gönderildiği tarih belirtilmelidir (ICANN, 2024f).

ICANN tarafından yayınlanan tavsiye metninde madde 3.18.2 kapsamında, içerisinde iki farklı örneğin de bulunduğu ayrıntılı bir açıklama yapılmıştır. Bu açıklamada ilk olarak, makul kanıt ifadesi açıklanmış, daha sonra uygulanacak eylemin orantılılığına ilişkin açıklama yapılmış ve eylemlerin derhal yerine getirilmesinden anlaşılması gerekenin ne olduğu belirtilmiştir. Son olarak, iki örnek üzerinden kayıt kuruluşunun yapması gerekenler belirtilmiştir.

Tavsiye metninde, kayıt otoriteleri için yapılan makul kanıt ifadesi kayıt kuruluşları için de yapılmış ve iletilen bilgilerin değerlendirilmesinin her olayın koşullarına göre değişeceği ayrıca belirtilmiştir.

ICANN, kayıt kuruluşlarının hizmet verdiği alan adlarını proaktif olarak izlemesini tavsiye etmektedir Bunun yanı sıra, kayıt kuruluşuna makul kanıt kapsamında yeterli bilgi içermeyen bir bildirim yapılması halinde bile, madde 3.18 kapsamında soruşturma yapması gerektiği tavsiye metinde belirtilmiştir. Kayıt kuruluşunun bazı durumlarda bildirim yapan kişinin erişemeyeceği bilgilere erişebileceği ve bu bilgileri dikkate alarak soruşturmanın yapılması gerektiği metinde ifade edilmiştir (ICANN, 2024f).

Makul kanıtlar elde edildikten sonra kayıt kuruluşunun, alan adının DNS Abuse için kullanılmasını durdurmak veya başka bir şekilde engellemek için gerekli olan uygun azaltma eylemlerini derhal gerçekleştirmesi gerekmektedir. Uygun azaltma eylemlerini hızlı bir şekilde belirlemek için, DNS Abuse'un neden olduğu zararın büyüklüğü ve ilişkili tali zarar olasılığının dikkate alınarak olayın kendi koşulları içerisinde incelenmesi önemlidir (ICANN, 2024f).

DNS Abuse faaliyetini durdurmak veya engellemek için uygun azaltma eylemini belirlemek koşullara göre değişebilmektedir. Benzer bir şekilde, DNS Abuse kapsamında alan adını soruşturmak ve eylemde bulunmak için uygun süre de değişebilmektedir. Bu da bir eylemin hızlı olarak kabul edilmesi için sabit bir sürenin belirlenmesini imkânsız hale getirmektedir. Bu sebeple kayıt kuruluşları, hizmet

verdiği alan adlarının DNS Abuse için kullanıldığına dair iddialara karşı mağdur edilenlerin uğrayacağı zararı da dikkate alarak gerekli özeni göstermelidir. Bu çerçevede, ICANN tarafından açılan bir soruşturmada kayıt kuruluşunun, belirli koşullar altında eylemlerin nasıl hızlı alındığını açıklaması gerekecektir. Açıklamanın ve ilgili koşullarının ICANN tarafından incelenmesi sonucunda eylemlerin makul ölçüde hızlı olup olmadığına dair karar verilecektir (ICANN, 2024f).

ICANN tavsiye metninde, madde 3.18.2 kapsamında iki farklı örnek verilmiştir. Bu örneklerde, iki farklı senaryo üzerinden kayıt kuruluşlarının yapması beklenen eylemler belirtilmiştir.

Birinci örnekte kayıt kuruluşu, hizmet verdiği bir alan adının kimlik avı/ oltalama için kullanıldığını iddia eden ve makul bir kanıt içeren kötüye kullanım bildirimi almıştır. Bildirim, kayıt kuruluşu tarafından hizmet verilen alan adını içeren bir URL'in, kendisini büyük bir banka olarak tanıtan ve alıcılardan hesaplarının kilidini açmalarını isteyen elektronik posta veya kısa mesaj yoluyla gönderildiğine dair kanıtlar içermektedir. Kayıt kuruluşu, kötüye kullanım bildirimde yer alan ilgili tüm bilgileri dikkate alarak bir soruşturma başlatmaktadır. Kayıt kuruluşu soruşturması sonunda, alan adının bir internet site içeriğine sahip olmadığı, yalnızca alan adını içeren bir URL'in büyük bir bankanın giriş ekranı gibi göründüğü tespit edilmiştir. Bu URL, elektronik posta veya kısa mesaj yoluyla gönderilen URL ile aynıdır. Kayıt kuruluşu ayrıca, kullanıcının yeni olduğunu ve alan adının beş gün önce tahsis edildiğini tespit etmiştir (ICANN, 2024f).

Yukarıda belirtilen koşullar altında, kayıt kuruluşunun alan adı üzerinden DNS Abuse faaliyeti yürütüldüğünü tespit ederek alan adını durdurması ve süreci iki iş günü içinde sonuçlandırması ICANN tavsiye metnine göre uygun azaltma eylemi olarak görülmektedir. Ayrıca, ICANN transfer politikasındaki şartlara uyulması halinde, alan adı sahibinin alınan önlemden kaçınmak amacıyla alan adını farklı bir kayıt kuruluşuna transfer etmesini engellemek için kayıt kuruluşu tarafından transfer kilidi uygulanabilecektir (ICANN, 2024f).

İkinci örnekte, kayıt kuruluşu hizmet verdiği bir alan adının kimlik avı/oltalama için kullanıldığına dair makul kanıtın da yer aldığı bir kötüye kullanım bildirimi almaktadır. Bildirim, belirli bir URL'in kimlik avı/oltalama için kullanıldığına dair kanıtlar içermektedir. Kayıt kuruluşu, kötüye kullanım bildiriminde yer alan bilgilerin yanında kendisinin kolayca erişebileceği bilgileri de dikkate alarak soruşturma başlatmaktadır. Soruşturma, kötüye kullanım bildirimindeki URL'in kimlik avı/oltalama için kullanıldığını göstermektedir ancak kötüye kullanım tahsis edilen alan adı üzerinden değil, alt bir seviyede (örneğin trabis.btk.gov.tr) gerçekleştirilmektedir. Bu seviyedeki alan adı ise bir bayi tarafından kullanılmaktadır. Ayrıca, kayıt kuruluşu tarafından alan adının üç yıl önce tahsis edildiği, bir otomobil bayiliği içeriğine sahip olduğu, kurumsal elektronik postalar için kullanıldığı ve birden fazla bayi tarafından alt seviyelerde kullanıldığı tespit edilmiştir (ICANN, 2024f).

Belirtilen şartlar altında kayıt kuruluşunun, alan adının DNS Abuse için kullanıldığını tespit etmesi ancak bunun alan adı sahibinin bilgi ve rızası dışında gerçekleştirildiği sonucuna varması gerekmektedir. Bu durumda, alan adının durdurulması tali zarara neden olacağından uygun bir eylem olmayacaktır. Bunun yerine, kayıt kuruluşunun alan adı sahibine bildirimde bulunması ve kimlik avı/oltalama içeriğinin belirlenen bir tarihe kadar kaldırmasını talep etmesi gerekmektedir. Soruşturma süreci ise, kötüye kullanım bildirimi alınmasından sonraki üç iş günü içinde tamamlanmalıdır (ICANN, 2024f).

ICANN tavsiye metninde RAA madde 3.18.3 için, daha önceki versiyonda madde 3.18.2'de yer alan, kolluk kuvvetlerinden ve yetkili diğer makamlardan bildirim almaya yönelik ilgili yükümlülüklerin artık madde 3.18.3'te yer aldığı belirtilmiş ve bu yükümlülüklerin aynı şekilde devam ettiği ifade edilmiştir. RAA madde 3.18.4 için ise herhangi bir açıklama yapılmamıştır (ICANN, 2024f).

Yukarıda ifade edilen yükümlülüklerin yanı sıra, kayıt kuruluşunun kötüye kullanım iletişim elektronik posta adresini ve telefon numarasını RDDS aracılığıyla yayınlaması yükümlülüğünün devam ettiği belirtilmiştir (ICANN, 2024f).

ICANN, RAA'da belirtilen yükümlülüklerin ihlali kapsamında kayıt kuruluşlarına soruşturma açabilmektedir. Bu soruşturmalar, gelen şikayet sebebiyle olabildiği gibi doğrudan ICANN tarafından da başlatılabilmektedir. Soruşturma sürecinde kayıt kuruluşu tarafından ihlal düzeltilmezse ICANN tarafından kamuya açık bir ihlal bildirimi yayınlanmaktadır (ICANN, 2012). İhlal bildiriminden sonraki yirmi gün içinde ilgili yükümlülükler yerine getirilmediği durumda, RAA madde 5.5.4 kapsamında kayıt kuruluşunun sözleşmesi feshedilebilmektedir. ICANN yirmi günlük süreyi uzatabilmektedir (ICANN, 2024g).

Örneğin, ICANN tarafından 10 Ocak 2022 tarihli ve içerisinde kötüye kullanım bildirimleri kapsamındaki yükümlülüklerin ihlalini de içeren kamuya açık bir ihlal bildirimi yayımlanmıştır. Bildirimde, 31 Ocak 2022 tarihine kadar belirtilen ihlallerin düzeltilmesi talep edilmiştir. Ancak, bu süre zarfında gerekli düzeltme işlemleri gerçekleştirilmediği için 7 Şubat 2022 tarihli kamuya açık bir fesih bildirimi ile kayıt kuruluşunun sözleşmesinin feshedildiği duyurulmuştur (ICANN, 2022ç; ICANN, 2022d).

3.2. Avrupa Birliği Tarafından Yapılan Çalışmalar

Avrupa Birliği düzeyinde siber güvenliğe ilişkin ilk düzenleme, üye devletler genelinde yüksek siber güvenlik düzeyi sağlamak amacıyla oluşturulan Ağ ve Bilgi Güvenliği *(The Network and Information Security - NIS)* Direktifi'dir. Direktif, üye devletlerin siber güvenlik kapasitelerini artırmış olsa da uygulamada üye devletler nezdinde farklılıklar oluşmuştur. Avrupa Komisyonu, NIS Direktifini değiştirmek ve böylece güvenlik gerekliliklerini güçlendirmek, tedarik zincirlerinin güvenliğini ele almak, raporlama yükümlülüklerini düzenlemek ve Avrupa Birliği genelinde uyumlaştırılmış yaptırımlar da dâhil olmak üzere daha sıkı denetim tedbirleri ve daha katı uygulama gereklilikleri getirmek üzere NIS 2 Direktifi'ni teklif etmiştir. Kasım 2022'de resmen kabul edilen Direktif, 16 Ocak 2023 tarihinde yürürlüğe girmiştir. Üye devletlerin, 17 Ekim 2024 tarihine kadar NIS 2 Direktifi ile uyumlu olmak için yasal

düzenlemelerini tamamlamaları gerekmektedir (European Parliamentary Research Service, 2023).

NIS 2 Direktifi dışında, Avrupa Komisyonu tarafından DNS Abuse ile ilgili olarak bir rapor hazırlatılmıştır. Çalışmanın genel amacı, Avrupa Komisyonuna DNS Abuse olgusunun kapsamlı bir değerlendirmesini yapmak ve nasıl mücadele edileceğine ilişkin bilgi sunmaktır (European Commission, 2022, s.6, s.28).

DNS Abuse ile mücadelede kapsamında Avrupa Birliği düzeyinde yapılan çalışmalar çerçevesinde ilk olarak NIS 2 Direktifi ilgili maddeleri incelenecek, daha sonra Avrupa Komisyonu tarafından hazırlatılan rapor hakkında bilgi verilecektir.

3.2.1. NIS 2 Direktifi

NIS 2 Direktifi'nde kayıt otoriteleri, üst düzey alan adı kayıt otoriteleri ve TLD ad kayıt otoriteleri *(top-level domain name registry/TLD name registry)* olarak tanımlanırken, kayıt kuruluşları alan adı kayıt hizmetleri sağlayan kuruluş *(entity providing domain name registration services)* tanımı içerisinde yer almıştır. Kayıt otoriteleri ve kayıt kuruluşlarının Direktif kapsamında oldukları ise ikinci maddede belirtilmiştir (NIS 2 Directive, 2023).

NIS 2 Direktifi'nde, DNS Abuse ile mücadeleye ilişkin doğrudan bir düzenlememe olmamasına rağmen kayıt otoriteleri ve kayıt kuruluşlarının topladığı alan adı kayıt bilgilerinin doğru ve eksiksiz olması, bunun sağlanması için doğrulama prosedürleri de dahil olmak üzere politika ve prosedürlere sahip olmalarının zorunlu kılınması ve yasal ve usulüne uygun olarak alan adı kayıt verilerinin istenilmesi durumunda talep edenlere verilmesi bakımından ilişkili düzenlemeler bulunmaktadır.

NIS 2 Direktifi'nde DNS Abuse tanımlanmamış, sadece önsöz yüz onuncu maddede ifade edilmiş olduğu için kavramın kapsamı belirsizdir. Bu madde; kayıt otoriteleri ve

kayıt kuruluşları tarafından, alan adı kayıt verilerinin "Meşru Erişim Talep Edenler"e zamanında verilmesi ve verilen bilgilerin kullanılabilir olması gerektiği ile ilgilidir:

> *"(110) Alan adı kayıt verilerinin meşru erişim talep eden kişiler tarafından kullanılabilir ve zamanında erişilebilir olması, DNS Abuse'un önlenmesi ve bununla mücadele edilmesi ve siber olayların önlenmesi, tespit edilmesi ve bunlara müdahale edilmesi için esastır. Meşru erişim talep edenler, Birlik hukuku veya ulusal hukuk uyarınca talepte bulunan herhangi bir gerçek veya tüzel kişi olarak anlaşılmalıdır. Bunlar, Direktif kapsamında yetkili olan makamlar ve Birlik veya ulusal hukuk kapsamında cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması için yetkili olan makamlar ve CERT[11]'ler veya CSIRT[12]'leri içerebilir. TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşların, erişim talebinin amaçları için gerekli olan belirli alan adı kayıt verilerine, Birlik ve ulusal hukuka uygun olarak meşru erişim talep edenlere yasal erişim sağlaması gerekmektedir. Meşru erişim talep edenlerin talebine, verilere erişim gerekliliğinin değerlendirilmesine izin veren bir gerekçe beyanı eşlik etmelidir."*

Bu maddeye göre; DNS Abuse ile mücadelede kayıt otoriteleri ve kayıt kuruluşları daha edilgen bir durumda olup, meşru erişim talep edenlere alan adı kayıt verilerini iletmekle görevlidir. Direktife göre meşru erişim talep edenler, Avrupa Birliği hukuku veya ulusal hukuk uyarınca talepte bulunan herhangi bir gerçek veya tüzel kişi olarak çok geniş bir şekilde tanımlanmıştır. Ancak, verilen örnekler ile çerçevenin daraltılmaya çalışıldığı değerlendirilmektedir. Mezkûr maddede ayrıca, meşru erişim talep edenlerin ilgili verilere erişim başvurularının, kayıt otoritesi ve kayıt kuruluşları tarafından değerlendirilmeye uygun olacak şekilde bir gerekçe beyanı ile yapılması gerektiği ifade edilmiştir.

---

[11] Bilgisayar Acil Müdahale Ekibi
[12] Bilgisayar Güvenliği Olay Müdahale Ekibi

Meşru erişim talep edenlerle ilgili olarak Direktif'in önsöz yüz on ikinci maddesinde, kayıt otoriteleri ve kayıt kuruluşları tarafından yapılması gerekenlere dair bilgi verilmiştir:

> *"(112) TLD alan adı kayıt kuruluşları ve alan adı kayıt hizmetleri sağlayan kuruluşların, 2016/679 (AB) sayılı Tüzüğün giriş bölümüne uygun olarak, tüzel kişilerle ilgili veriler gibi Birlik veri koruma kanunu kapsamı dışında kalan alan adı kayıt verilerini kamuya açık hale getirmeleri gerekmektedir. Tüzel kişiler için, TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, en azından alan adı sahibinin adını ve irtibat telefon numarasını kamuya açık hale getirmelidir. E-posta takma adları[13] veya işlevsel hesaplar gibi herhangi bir kişisel veri içermemesi koşuluyla, iletişim e-posta adresi de yayınlanmalıdır. TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, gerçek kişilerle ilgili belirli alan adı kayıt verilerine, Birlik veri koruma yasasına uygun olarak, meşru erişim talep edenlerin yasal erişimini de sağlamalıdır. Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların, meşru erişim talep edenlerden gelen alan adı kayıt verilerinin ifşa edilmesi taleplerine gecikmeksizin yanıt vermesini zorunlu kılmalıdır. TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, meşru erişim talep edenlerin erişim taleplerini değerlendirmek için hizmet seviyesi anlaşmaları da dahil olmak üzere, kayıt verilerinin yayınlanması ve ifşa edilmesine yönelik politika ve prosedürler oluşturmalıdır. Bu politika ve prosedürler, mümkün olduğu ölçüde, uluslararası düzeyde çok paydaşlı yönetişim yapıları tarafından geliştirilen rehber ve standartları dikkate almalıdır. Erişim prosedürü, kayıt verilerinin talep edilmesi ve bunlara erişilmesi için etkin bir sistem sağlamak üzere bir arayüz, portal veya başka bir teknik aracın kullanılmasını içerebilir. İç pazar*

---

[13] E-posta takma adı olarak da bilinen diğer e-posta adresi, yöneticinin bir kullanıcıya ait birincil e-posta adresine eklediği bir yönlendirme e-posta adresidir. E-posta takma adına gönderilen iletiler otomatik olarak kullanıcının birincil e-posta hesabına yönlendirilmektedir. Daha fazla bilgi için bkz. (https://support.google.com/a/answer/33327?hl=tr#:~:text=E%2Dposta%20takma%20ad%C4%B1%20olarak,bir%20y%C3%B6nlendirme%20e%2Dposta%20adresidir.), (11.05.2024)

genelinde uyumlaştırılmış uygulamaları teşvik etmek amacıyla Komisyon, Avrupa Veri Koruma Kurulu'nun yetkilerine halel getirmeksizin, mümkün olduğu ölçüde uluslararası düzeyde çok paydaşlı yönetişim yapıları tarafından geliştirilen standartları dikkate alan bu tür prosedürlere ilişkin kılavuz ilkeler oluşturulabilir. Üye Devletler, kişisel ve kişisel olmayan alan adı kayıt verilerine her türlü erişimin ücretsiz olmasını sağlamalıdır."

Bu maddeye göre; kayıt otoritesi ve kayıt kuruluşları tarafından, alan adı sahibi olan tüzel kişilerin asgari olarak alan adı sahiplik bilgileri ile irtibat telefon numaraları kamunun erişimine sunulmalı, alan adı sahibi gerçek kişilere ait veriler meşru erişim talep edenlerle paylaşılmalıdır. Meşru erişim talep edenlerin yaptığı başvurulara, kayıt otoritesi ve kayıt kuruluşları tarafından gecikmeksizin yanıt verilmesi üye devletler tarafından zorunlu kılınmalı ve kişisel ve kişisel olmayan alan adı kayıt verilerine her türlü erişimin ücretsiz olması sağlanmalıdır. Meşru erişim talep edenlerin yaptığı başvuruların değerlendirilmesi için, kayıt otoritesi ve kayıt kuruluşları tarafından politika ve prosedürler oluşturulmalıdır. Hazırlanacak prosedürlerin kullanışlı olabilmesi adına arayüz, portal veya başka bir teknik araç kullanılabilir. Bunların yanı sıra, meşru erişim talep edenlerle ilgili prosedürlere ilişkin olarak Avrupa Komisyonu tarafından kılavuz ilkeler oluşturulabileceği de belirtilmiştir.

Meşru erişim talep edenlerle ilgili olarak *"Alan adı kayıt verilerinin veri tabanı"* başlıklı yirmi sekizinci madde sürecin nasıl işleyeceğine dair bilgiler içermektedir. Bu madde ayrıca, alan adı kayıt bilgilerinin doğru ve eksiksiz olması ve bunun sağlanması için zorunlu kılınan politika ve prosedürlere ilişkin hükümler de içermektedir:

"Madde 28
Alan adı kayıt verileri veri tabanı
1. DNS'in güvenliğine, istikrarına ve dayanıklılığına katkıda bulunmak amacıyla Üye Devletler, kişisel verilerle ilgili olarak Birlik veri koruma kanununa uygun bir şekilde TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların, doğru ve eksiksiz alan adı kayıt verilerini

özel bir veri tabanında gerekli özeni göstererek toplamasını ve muhafaza etmesini zorunlu kılacaktır.

2. Paragraf 1'in amaçları doğrultusunda Üye Devletler, alan adı kayıt verileri veri tabanının, alan adlarının sahiplerini ve TLD'ler kapsamında alan adlarını yöneten yetkili kişileri belirlemek ve onlarla iletişim kurmak için gerekli bilgileri içermesini zorunlu kılacaktır. Bu tür bilgiler şunları içerecektir:

(a)alan adı;

(b)tahsis tarihi;

(c)alan adı sahibi, iletişim e-posta adresi ve telefon numarası;

(d)alan adının sahibi dışında yönetilmesi durumunda alan adını yöneten kişinin iletişim e-posta adresi ve telefon numarası,

3. Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların, paragraf 1'de atıfta bulunulan veri tabanlarının doğru ve eksiksiz bilgi içermesini sağlamak için doğrulama prosedürleri de dahil olmak üzere politika ve prosedürlere sahip olmalarını zorunlu kılacaktır. Üye Devletler bu tür politika ve prosedürlerin kamuya açık olmasını talep edeceklerdir.

4. Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların, kişisel veri olmayan alan adı kayıt verilerini, alan adı tahsisinden sonra gecikme olmaksızın kamuya açık hale getirmesini zorunlu kılacaktır.

5. Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların, Birlik veri koruma hukukuna uygun olarak, meşru erişim talep edenlerin yasal ve usulüne uygun olarak doğrulanmış talepleri üzerine belirli alan adı kayıt verilerine erişim sağlamasını zorunlu kılacaktır. Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların herhangi bir erişim talebini aldıktan sonra gecikme olmaksızın ve her halükarda 72 saat içinde yanıt vermesini talep edeceklerdir. Üye Devletler, bu tür verilerin kamuya açık hale getirilmesine ilişkin politika ve prosedürleri zorunlu kılacaktır.

6. 1'den 5'e kadar olan paragraflarda belirtilen yükümlülüklere uygunluk, alan adı kayıt verilerinin toplanmasında mükerrerlik yapılmasına yol açmayacaktır. Bu amaçla Üye Devletler, TLD ad kayıt otoritelerinin ve alan adı kayıt hizmetleri sağlayan kuruluşların birbirleriyle iş birliği yapmasını zorunlu kılacaktır."

Bu maddeye göre; kayıt otoritesi ve kayıt kuruluşlarının, kişisel veri olmayan alan adı kayıt verilerini tahsis işleminden hemen sonra kamuya açık hale getirmesi ve meşru erişim talep edenler tarafından yasal ve usulüne uygun olarak yapılan başvuruları verilerin paylaşılması şeklinde sonuçlandırması üye devletlerce zorunlu kılınacaktır. Meşru erişim talep edenlerin başvuruları yetmiş iki saat içerisinde yanıtlanacak ve bu sürece ilişkin politika ve prosedürler kayıt otoritesi ve kayıt kuruluşları tarafından kamuya açık hale getirilecektir.

NIS 2 Direktifi, alan adı kayıt verilerinin kayıt otoriteleri ve kayıt kuruluşları tarafından paylaşılmasına büyük önem vermektedir. Elbette paylaşılan verilerin doğru olması da aynı derecede önemlidir. Bu bağlamda, Direktif'in yirmi sekizinci maddesi verilerin doğruluğuna ilişkin düzenlemeler içermektedir. Bu maddeye göre; kayıt otoriteleri ve kayıt kuruluşları, alan adı kayıt verilerini doğru ve eksiksiz bir şekilde almalı, bunun için gerekli doğrulama prosedürlerini içeren kamuya açık politika ve prosedürlere sahip olmalı ve alan adı kayıt verilerini özel bir veri tabanında gerekli özeni göstererek toplamalı ve muhafaza etmelidir. Bu yükümlülükler, üye devletler tarafından kayıt otoriteleri ve kayıt kuruluşlarına getirilmelidir.

Direktif'in yirmi sekizinci maddesi yanında önsöz yüz on birinci madde de alan adı kayıt verilerinin doğru ve eksiksiz olması için uygulanacak politika ve prosedürlere ilişkin bilgiler içermektedir:

"(111) Doğru ve eksiksiz alan adı kayıt verilerinin kullanılabilirliğini sağlamak için, TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, alan adı kayıt verilerinin bütünlüğünü ve kullanılabilirliğini

sağlamalı ve garanti etmelidir. Özellikle, TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, Birlik veri koruma kanununa uygun olarak, doğru ve eksiksiz alan adı kayıt verilerinin sağlanması ve muhafaza edilmesinin yanı sıra yanlış kayıt verilerinin önlenmesi ve düzeltilmesi için politika ve prosedürler oluşturmalıdır. Bu politika ve prosedürler, mümkün olduğu ölçüde, uluslararası düzeyde çok paydaşlı yönetişim yapıları tarafından geliştirilen standartları dikkate almalıdır. TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, alan adı kayıt verilerini doğrulamak için orantılı prosedürler benimsemeli ve uygulamalıdır. Bu prosedürler, sektörde kullanılan en iyi uygulamaları ve mümkün olduğu ölçüde elektronik kimlik belirleme alanında kaydedilen ilerlemeyi yansıtmalıdır. Doğrulama prosedürlerine örnek olarak, kayıt sırasında gerçekleştirilen ön kontroller ve kayıt sonrasında gerçekleştirilen nihai kontroller verilebilir. TLD ad kayıt otoriteleri ve alan adı kayıt hizmetleri sağlayan kuruluşlar, özellikle, alan adı sahibinin en az bir iletişim aracını doğrulamalıdır."

Bu maddeye göre; kayıt otoriteleri ve kayıt kuruluşlarının, orantılı ve sektörde kullanılan en iyi uygulamaları ve mümkün olduğu ölçüde elektronik kimlik belirleme alanında kaydedilen ilerlemeyi yansıtan prosedürler benimsemesi gerektiği belirtilmiş, doğrulama prosedürlerine örnek olarak, tahsis sırasında gerçekleştirilen ön kontroller ve tahsis sonrasında gerçekleştirilen kontroller verilmiş ve alan adı sahibinin en az bir iletişim bilgisinin doğrulanması gerektiği belirtilmiştir. Mezkûr maddede ayrıca, hatalı kayıt verilerini önlemek ve düzeltmek için politikalar ve prosedürler oluşturması gerektiği de belirtilmiştir.

Önsöz yüz on birinci madde, *"Alan adı kayıt verilerinin veri tabanı"* başlıklı yirmi sekizinci maddeye göre daha ayrıntılı bilgi içermesine rağmen kayıt otoriteleri ve kayıt kuruluşlarının, hatalı alan adı kayıt verilerini düzeltmek için yapacağı politikalar ve prosedürlerin nasıl oluşturulabileceğine dair bilgi içermemektedir.

NIS 2 Direktifi'nde DNS Abuse ile mücadeleye ilişkin çok fazla detay bulunmamakla birlikte, ilgili maddeler incelendiğinde oluşturulmaya çalışılan politika hakkında bazı bilgilere ulaşmak mümkündür. Direktif'e göre kayıt otoritesi ve kayıt kuruluşları DNS Abuse ile mücadelede, alan adı kayıt verilerinin doğru ve eksiksiz olarak muhafaza edilmesi ve bunların ilgili kişilerle paylaşılması şeklinde edilgen bir biçimde konumlandırılmıştır. DNS Abuse ile etkin mücadelenin ise, yetkili kamu kurum ve kuruluşlara bırakıldığı değerlendirilmektedir.

3.2.2. Avrupa Komisyonu - DNS Abuse Raporu

Avrupa Komisyonu, DNS Abuse'un kapsamını, etkisini ve büyüklüğünü değerlendirmek ve tespit edilen eksiklikler noktasında hazırlanacak politikalara katkı olması için "DNS Abuse Raporu (*Study on Domain Name System (DNS) Abuse*)"nu hazırlatmıştır. Raporda, DNS Abuse tanımı incelenmiş; boyutu, yapılan ölçümler ve anketler ile ikincil araştırmaların sonuçları çerçevesinde tespit edilmeye çalışılmış; nesnelerin interneti ve 5G[14]'nin DNS Abuse faaliyetlerine olan etkisi ele alınmış; DNS Abuse'e ilişkin düzenlemeler hakkında bilgi verilmiş; DNS Abuse faaliyetlerinin azaltılmasına yönelik en iyi uygulamalar incelenmiş ve son olarak DNS Abuse'un azaltılmasında ilişkin önerilerde bulunulmuştur.

Raporda yer alan ölçümlerin, Mart 2021'den Haziran 2021'e kadar olan süre zarfında yapıldığı belirtilmiştir. Bu ölçümlerde; en çok new gTLD'ler üzerinden DNS Abuse faaliyeti yürütüldüğü ve bunun yaklaşık yarısının iki new gTLD kapsamında gerçekleştiği, kötü amaçlı yazılım dağıtımı yapılan alan adlarının yaklaşık yarısının meşru amaçlarla tahsis edildiği ve kötü amaçla kaydedilen alan adlarının %48'inin beş kayıt kuruluşu tarafından tahsis edildiği gibi çarpıcı tespitler yapılmıştır:

[14] 5G, önceki ağlardan daha yüksek yükleme ve indirme hızları, daha tutarlı bağlantılar ve gelişmiş kapasite sunan, beşinci nesil kablosuz hücresel teknolojisidir. Daha fazla bilgi için bkz. (https://aws.amazon.com/tr/what-is/5g/), (05.04.2024)

"a) Tahmini pazar payı %6,6' olan new gTLD uzantılı alan adları en çok kötüye kullanılan TLD grubudur.

b) Tüm new gTLD'ler aynı oranda DNS Abuse'a konu olmamaktadır. En çok kötüye kullanılan iki new gTLD, kötüye kullanılan tüm new gTLD uzantılı alan adlarının %41'ini oluşturmaktadır.

c) Avrupa Birliği ülke kodlu TLD'leri (AB ccTLD'leri), mutlak anlamda ve genel pazar paylarına oranla en az kötüye kullanılan uzantılardır.

d) İstenmeyen elektronik posta ve köle bilgisayar ağları komuta ve kontrol faaliyeti yürütülen alan adlarının büyük çoğunluğu kötü niyetle kaydedilmiştir.

e) Kimlik avı/oltalama yapılan alan adlarının yaklaşık %25'i ve kötü amaçlı yazılım dağıtımı yapılan alan adlarının %41'i meşru amaçlarla tahsis edilen ancak yer sağlayıcı düzeyinde saldırganlar tarafından yapılan eylemler sonucu kötüye kullanılan alan adlarıdır.

f) Kötü amaçla kaydedilen alan adlarının %48'i beş kayıt kuruluşu tarafından tahsis edilmiştir.

g) Aşırı düzeyde istenmeyen elektronik posta iletilen alan adı yoğunluğuna sahip yer sağlayıcılarında, 10.000 kayıtlı alan adı başına 3.000 kötüye kullanılan alan adına ulaşılmaktadır

h) DNSSEC'in genel olarak benimsenme düzeyi düşüktür.

i) Dünya çapında, dağıtılmış hizmet reddi saldırılarında güçlendirici olarak etkili bir şekilde kullanılabilecek 2,5 milyon açık yinelemeli çözümleyici bulunmaktadır." (European Commission, 2022, s.7).

DNS Abuse Raporu'nda beş başlık altında öneriler ifade edilmiştir. Bunlar; DNS meta verileri, iletişim bilgileri ve kötüye kullanım bildirimi, DNS Abuse faaliyetlerinin önlenmesi, tespit edilmesi ve azaltılması, DNS işlemlerinin korunması, ilgili DNS Abuse faaliyetlerinin önlenmesi ve Avrupa Birliği düzeyinde farkındalık, bilgi oluşturma ve risk azaltma iş birliğidir (European Commission, 2022, s.8-9). Bu başlıklar altında verilen öneriler, alan adı sektöründen daha kapsamlı olarak internet paydaşlarına yöneliktir. Bununla birlikte, raporda belirtilen tavsiyeler tam olarak aşağıda ifade edilmiştir:

DNS Meta Verileri

- ccTLD kayıt otoriteleri, gTLD'lerde olduğu gibi "Kayıt Veri Erişim Protokolünü (*Registration Data Access Protocol -RDAP*)[15]" kullanarak eksiksiz kayıt (WHOIS[16]) bilgilerine erişmek için ölçeklenebilir ve birleşik bir sistem oluşturmalı ve DNS bölge dosya verilerini DNS bölge aktarımı veya ICANN tarafından sürdürülen Merkezi Bölge Veri Hizmetine (*Centralized Zone Data Service - CZDS*)[17] benzer bir sistem aracılığıyla yayınlamayı değerlendirmelidir.

İletişim bilgileri ve kötüye kullanım bildirimi

- Alan adı sahiplerinin ve alan adı yöneticilerinin WHOIS'de görünmeyen elektronik posta adresleri anonimleştirilmiş olarak yer alabilir.
- Alan adı idarecileri, kötüye kullanım bildirimi yapılabilecek standart elektronik posta takma adları oluşturmalıdır.
- Hem kayıt verilerine (WHOIS verileri) erişim hem de kötüye kullanım bildirimi için standartlaştırılmış sistemler kurulmalıdır.

DNS Abuse faaliyetlerinin önlenmesi, tespiti ve azaltılması

TLD kayıt otoriteleri, kayıt kuruluşları veya bayileri, görev alanlarına bağlı olarak aşağıda belirtilenleri yapmalıdır:

- Alan kaydı (WHOIS) bilgilerinin doğruluğu, Ticari İşletmeyi Tanı *(Know Your Business Customer -KYBC)* prosedürleri ve eID kimlik doğrulama gibi yöntemler aracılığıyla teyit edilmelidir;

---

[15] Kayıt Veri Erişim Protokolü (RDAP), kullanıcıların mevcut alan adı kayıt verilerine erişmesine olanak tanıyan ve nihai olarak WHOIS protokolünün yerini alacak şekilde İnternet Mühendisliği Görev Gücü tarafından geliştirilen protokoldür. Daha fazla bilgi için bkz. (https://www.icann.org/rdap), (05.04.2024)

[16] Whois; alan adı tahsis tarihi, tahsis bitiş tarihi, sahiplik ve iletişim bilgileri, alan adının yetkili ad sunucusu bilgileri, alan adının satın alındığı kayıt kuruluşu vb. gibi bilgileri sorgulamak için kullanılan kamuya açık bir protokol ve veri tabanı sistemidir. Whois, ".tr" uzantılı alan adlarına ilişkin mevzuatta "rehber" olarak tanımlanmıştır.

[17] Merkezi Bölge Veri Hizmeti, gTLD kayıt otoriteleri tarafından oluşturulan bölge dosyalarına erişimin, merkezi bir nokta üzerinden sağlanması için geliştirilmiştir. Her new gTLD kayıt otoritesinin, yetkili talep sahiplerine (örn. kolluk kuvvetleri, fikri mülkiyet avukatları, araştırmacılar) bölge verilerini sağlaması gerekmektedir. Daha fazla bilgi için bkz. (https://www.icann.org/resources/pages/czds-2014-03-03-en), (05.04.2024)

- Üçüncü tarafların, potansiyel olarak haklarını ihlal edecek alan adlarını tespit etmelerini sağlamak için benzerlik arama araçları veya gözetim hizmetlerinin geliştirilmesi ve sunulması teşvik edilmelidir;
- Fikri mülkiyet hakkı sahiplerinin, haklarını ihlal edecek alan adı tahsislerini engellemelerine olanak tanıyan hizmetler sunulmalıdır;
- Kötüye kullanım amaçlı tahsisleri önlemek için tahmine dayalı algoritmalar veya diğer yöntemlerin kullanılması teşvik edilmelidir;
- Ekosistemlerindeki DNS Abuse kullanımının yoğunluğu ve oranları tespit edilmelidir;
- Kötüye kullanım oranları kurumlar ve düzenleyici kurumlarla iş birliği içinde bağımsız araştırmacılar tarafından sürekli olarak izlenmelidir;
- Belirli bir süre zarfında, kötüye kullanım oranlarının önceden belirlenmiş eşikleri aşmaya devam etmesi halinde yetkilendirmeler iptal edilmelidir;
- Kötüye kullanım oranı düşük olanlar, alan adı tahsis ücretlerinde indirim yapılarak mali olarak ödüllendirilmelidir.

Yer sağlayıcıları:

- Ekosistemlerindeki DNS ve barındırma altyapısı kötüye kullanımlarının yoğunluğu ve oranları açısından tanımlanmalıdır;
- Kötüye kullanım oranları, kurumlar ve düzenleyici kurumlarla iş birliği içinde bağımsız araştırmacılar tarafından sürekli olarak izlenmeli ve kötüye kullanımlar önceden belirlenmiş eşikleri aşmamalıdır;
- Barındırma ve içerik istismarını etkili bir şekilde engelleyen teknik çözümler geliştirmeye ve kullanmaya teşvik edilmelidir;
- Barındırma altyapısı ve üç veya daha fazla dereceli alan adlarının kötüye kullanımını hızla engellemek için gelişmiş önleme ve düzeltme çözümleri kullanılmalıdır.

DNS işlemlerinin korunması ve ilgili DNS Abuse faaliyetlerinin önlenmesi

- TLD kayıt otoritesi ve kayıt kuruluşları, TLD bölge dosyalarını (kayıt otoriteleri) ve alan adlarını (kayıt kuruluşları) DNS güvenlik uzantıları

DNSSEC ile imzalamalı, iyi uygulamalara göre dağıtımını kolaylaştırmalı ve DNSSEC imzalı alan adları için indirimler sunmalıdır.

- Yinemeli çözümleyicileri işleten internet servis sağlayıcıları DNSSEC doğrulamasını yapılandırmalıdır.
- Ulusal hükümetler ve CERT ekipleri, dağıtılmış yansıtıcı hizmet reddi (DRDoS) saldırılarını önlemek için açık yinelemeli çözümleyicilerinin ve diğer açık hizmetlerin sayısını azaltmaya yönelik bilgilendirme çalışmalarını yoğunlaştırmalıdır.
- Siber güvenlik topluluğu, alan adı dolandırıcılığını önleyen elektronik posta güvenlik standartlarının benimsenmesini ölçmek için çalışmalarını arttırmalıdır.
- Ağ operatörleri[18] IP sahtekarlığı, dağıtık yansıtıcı hizmet reddi (DRDoS) ve DNS altyapı saldırılarına karşı interneti koruyan IP kaynak adresi doğrulamasını devreye sokmalıdır.

Avrupa Birliği düzeyinde farkındalık, bilgi oluşturma ve risk azaltma iş birliği

- İyi uygulamaların benimsenmesi yoluyla ccTLD faaliyetleri birbiriyle uyumlu hale getirilmelidir.
- Avrupa Birliği ve üye devletlerin kurumları, DNS hizmet sağlayıcılarının kolluk kuvvetleri (*Law enforcement agency - LEA*) ve güvenilir bildirimde bulunanlarla iş birliği yapmasını zorunlu kılmalıdır.
- Hedef kitlenin DNS Abuse ile mücadelede kullanılan tedbirlerden haberdar olması için farkındalık artırma ve bilgi oluşturma faaliyetleri teşvik edilmelidir.
- DNS Abuse ile mücadelede yer alan kurumlar ve ilgili paydaşlar arasında bilgi paylaşımı ve kapasite geliştirme faaliyetleri teşvik edilmelidir (European Commission, 2022, s.8-9).

[18] Ağ operatörü, mobil ağ operatörlerine, sanal ağ operatörlerine ve son kullanıcılara hizmet satmak ve sunmak için gerekli altyapıya sahip olan veya bunları kontrol eden kablolu ve kablosuz iletişim hizmetleri sağlayıcısıdır.

4. CCTLD KAYIT OTORİTELERİNİN ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI (DNS ABUSE) İLE MÜCADELE UYGULAMALARI

ccTLD kayıt otoriteleri, tahsis modellerinde ve tahsis politikalarında farklı uygulamaları tercih edebilmektedir. Tahsis modelleri; belgeli tahsis, belgesiz tahsis, belgeli ve belgesiz tahsislerin birlikte uygulandığı karma model olarak sınıflandırılabilirken, alan adı sahiplerine ilişkin olarak; ülkede yerleşik olan veya olmayan şeklinde sınıflandırma yapılabilmektedir.

Belgeli tahsis modelinde, alan adını talep eden kişinin belirli belgeleri sunması gerekmektedir. Belgeler, genellikle başvuru sahibinin kimliğini, ticaret unvanını, kurumsal yapısını veya diğer belirli kriterleri doğrulayan bilgileri içermektedir. Belgesiz tahsis modelinde ise, genellikle belge sunma zorunluluğu bulunmamaktadır. Alan adını isteyen herhangi bir kişi, tahsis ücretini ödeyerek belgesiz bir şekilde alan adını alabilmektedir. Bu iki modelin birlikte kullanımından oluşan model ise karma model olarak tanımlanabilir. Karma modelde, belgeli ve belgesiz ayrımı ikinci seviye alan adı (SLD) üzerinden yapılabilmektedir.

Alan adı sahiplerine yönelik yapılan sınıflandırma kapsamında bazı ccTLD kayıt otoriteleri, alan adı sahibinin taşıması gereken şartları belirlerken diğer ccTLD kayıt otoriteleri herhangi bir sınırlandırma getirmemiştir. Belirlenen şartlar genellikle ülkede yerleşik olma üzerine oluşturulmuştur.

DNS Abuse ile mücadele konusunda da kayıt otoriteleri arasında farklı politika tercihleri bulunmaktadır. Bu farklılıkların anlaşılması amacıyla DNS Abuse kapsamında incelenecek ülkeler; ccTLD kayıt otoritelerinin DNS Abuse politikaları, tahsis modelleri ve alan adı sahibine ilişkin belirlenen şartlar göz önüne alınarak seçilmiştir.

4.1. Almanya

Almanya'nın ccTLD'si ".de" dir ve bir kooperatif olan DENIC tarafından yönetilmektedir (DENIC, 2023b). ".de" uzantılı alan adları, ilk gelen ilk alır kuralına göre Almanya'da ikamet etsin veya etmesin herkes tarafından tahsis edilebilmektedir. Bazı durumlarda DENIC, Almanya'da yerleşik olmayan alan adı sahiplerinden, Almanya'da yerleşik olan ve tebligat alma yeterliliğine sahip bir kişiyi yetkilendirmesini isteyebilmektedir. Bu durumda alan adı sahibine iki haftalık bir süre tanınmaktadır (DENIC, 2023c; DENIC, 2024ç).

DENIC kurumsal internet sitesinde, alan adları içeriğinin ve yasallığının kontrol edilmediği belirtilmiştir. Ancak "DENIC Alan Adı Hüküm ve Koşulları (*DENIC Domain Terms and Conditions*)" "Fesih (*Termination*)" başlıklı 7'inci maddesinde bu kapsama girebilecek ifadelere yer verildiği görülmüştür (DENIC, 2023c; DENIC, 2023ç):

> *"§ 7 Fesih*
> *...*
> *(2) DENIC sözleşmeyi sadece aşağıdaki durumlarda geçerli bir sebepten dolayı feshedebilir:*
> *...*
> *d) özel kullanımına bakılmaksızın, alan adının sahibi adına tahsisinin üçüncü tarafların haklarını açıkça ihlal etmesi veya başka bir şekilde yasa dışı olması ..."*

Belirtilen madde dışında DENIC'in düzenlemelerinde DNS Abuse'a ilişkin hükümler bulunmamaktadır (DENIC, 2023c). Kurumsal internet sitesinde yer alan bilgiler ışığında DENIC'in DNS Abuse politikasına doğrudan müdahalesinin olmadığı, son kullanıcıların farkındalığını arttırmaya çalışan bir politika izlediği görülmektedir (DENIC, 2024a).

DENIC, DNS Abuse ile mücadelede doğrudan aksiyon almadığını belirtmesine rağmen ".de Kayıt Otoritesi Kilidi *(.de Registry Lock)*" hizmeti ile alan adı yetkili ad sunucu bilgilerinin izinsiz olarak değiştirilmesini engellemektedir (DENIC, 2023a). ".de" kayıt otoritesi kilidi hizmetinin yanı sıra DNSSEC teknolojisi de ".de" uzantılı alan adlarında kullanılmaktadır (DENIC, 2024c)

DENIC'in DNS Abuse politikası kapsamında ilk olarak farkındalık çalışmaları belirtilecek, sonrasında .de kayıt otoritesi kilidi hizmeti açıklanacak ve son olarak DNSSEC kapsamında bilgi verilecektir.

- **Farkındalık Çalışmaları**

DENIC'in kurumsal internet sitesinde, sahte internet mağazaları ile yasa dışı internet içerikleriyle ilgili sayfalar bulunmaktadır. Bu sayfalarda, DENIC'in belirtilen konulara yaklaşımı belirtilmekte ve başvuruda bulunabilecek kuruluşlar hakkında bilgi verilmektedir (DENIC, 2024a; DENIC 2024b). Yasa dışı internet içerikleriyle ilgili olan sayfada yer alan başlıklar, DNS Abuse özelinde olmamakla birlikte çoğu DNS Abuse türünü ihtiva etmektedir. İlgili sayfada yer alan kurumlar ve bildirime konu olan içerikler aşağıda yer almaktadır:

- Gençleri etkileyen yasa dışı içeriğe sahip internet siteleri (örneğin nefrete teşvik, şiddet tasvirleri, aşırı pornografi). **İletişim kurulacak kurum:** İnternet Şikayetleri Ofisi
- İstenmeyen elektronik postalar (pornografik içerikle veya reşit olmayanlar için zararlı içerikle bağlantısı olmayan, istenmeyen reklam elektronik postaları. Bunlar genellikle virüslü dosyalar veya virüslü internet sitelerine yönlendiren bağlantılar içermektedir). **İletişim kurulacak kurum:** Eyalet polis güçlerinin siber suç yardım portalı
- Haber gruplarında, tartışma forumlarında ve sohbet odalarındaki yasa dışı internet içeriği. **İletişim kurulacak kurum:** İnternet Şikayetleri Ofisi
- Yasa dışı mobil içerik. **İletişim kurulacak kurum:** İnternet Şikayetleri Ofisi

- Dosya paylaşım ağları/P2P'deki yasa dışı internet içeriği. **İletişim kurulacak kurum:** İnternet Şikayetleri Ofisi
- Kötü amaçlı yazılımlar (virüsler, solucanlar, truva atları, köle bilgisayar ağları gibi kötü amaçlı programlar). **İletişim kurulacak kurum:** Eyalet polis güçlerinin siber suç yardım portalı
- Kimlik Avı/ Oltalama (sahte internet siteleri, elektronik postalar veya kısa mesajlar aracılığıyla bir internet kullanıcısının PIN'leri veya şifreleri gibi kişisel verilerini elde etme, çevrimiçi bankacılık veya alışveriş alanında kimlik hırsızlığı/dolandırıcılık suçları işleme girişimleri). **İletişim kurulacak kurum:** Tüketici danışma merkezi
- Veri koruma suçları. **İletişim kurulacak kurum:** Federal eyaletlerin veri koruma denetim makamları (Eyalet Veri Koruma ve Bilgi Özgürlüğü Komiseri)
- Sağlayıcı etiketleme yükümlülüklerinin/künye yükümlülüğünün ihlali. **İletişim kurulacak kurum:** Haksız Rekabetle Mücadele Merkezi (DENIC, 2024a).

- **.de Kayıt Otoritesi Kilidi**

DENIC, bir alan adı kilidi hizmeti olan ".de Kayıt Otoritesi Kilidi *(.de Registry Lock)*"ni alan adı sahiplerine sunmaktadır. Bu hizmet genel hatlarıyla "DENIC Alan Adı Hüküm ve Koşulları"nın birinci maddesinin beşinci fıkrasında açıklanmıştır (DENIC, 2023c; DENIC, 2023a).

.de kayıt otoritesi kilidi konulan bir alan adının bilgilerinde değişiklik yapılması, daha önce yetkilendirilmiş "Kilit İrtibat Kişisi *(Lock Contact)*" onayı ile gerçekleşmektedir. Kilit irtibat kişisi, alan adı sahibi tarafından yetkilendirilen üçüncü bir kişidir (DENIC, 2023a).

.de kayıt otoritesi kilidi kapsamında dört taraf bulunmaktadır. Bunlar; kayıt otoritesi, kayıt kuruluşu, alan adı sahibi ve kilit irtibat kişisidir. Alan adı sahibi, .de kayıt

otoritesi kilidi ile ilgili tüm işlemlerini kayıt kuruluşu aracılığı ile yapmaktadır. Alan adı sahibinin, yapmak istediği işlemler için ilgili formları doldurması ve kimlik belgesini ibraz etmesi gerekmektedir. Kayıt kuruluşu da kendisine gelen talepleri DENIC'e iletmektedir (DENIC, 2023a).

Kilitli bir alan adının bilgilerinde değişiklik talebi, kayıt kuruluşu tarafından DENIC'e iletildiği durumda talep DENIC tarafından kontrol edilmektedir. Yapılan kontrol sürecinde uygun bulunmayan talepler yerine getirilmemektedir. Kontrolün başarılı olduğu durumda ise DENIC, kilit irtibat kişisinden talep edilen işlemi onaylamasını istemektedir. Onay verilmesi halinde talep edilen işlem gerçekleştirilmekte ve kayıt kuruluşu ile kilit irtibat kişisi bilgilendirilmektedir (DENIC, 2023a).

Kilit irtibat kişisi, alan adı bilgilerinde yapılacak tüm değişiklikler için irtibat noktasıdır. DENIC, kayıt kuruluşu aracılığıyla alan adı bilgilerinin değiştirilmesi için bir talep aldığında, kilit irtibat kişisinin cep telefonu numarasına kod, mail adresine elektronik posta göndermektedir. Kilit irtibat kişisi tarafından işlemin onaylanabilmesi için, cep telefonuna iletilen kodun gelen elektronik posta ile DENIC'e iletilmesi gerekmektedir. Kilit irtibat kişisi tarafından yedi gün içinde değişiklik talebi onaylanmadığı takdirde talep yerine getirilmemektedir (DENIC, 2023a; DENIC, 2023d).

- **DNSSEC**

DNSSEC teknolojisi, ".de" uzantılı alan adlarında kullanılmaktadır. DNSSEC'in kullanılabilmesi için alan adının imzalanması ve genel anahtarın kayıt kuruluşu aracılığıyla DENIC'e iletilmesi gerekmektedir (DENIC, 2024c).

DENIC kurumsal internet sitesinde DNSSEC başlıklı bir sayfa yayınlanmıştır. Bu sayfada; DNSSEC'in ne olduğu, nasıl çalıştığı, ".de" uzantılı alan adlarında sürecin nasıl işlediği hakkında bilgiler verilmiş ve ilgili doküman ve internet sitelerine yönlendiren bağlantılar paylaşılmıştır (DENIC, 2024c).

4.2. Avustralya

Avustralya'nın ccTLD'si ".au" dur ve kar amacı gütmeyen bir kuruluş olan .au Domain Management Limited *(auDA)* tarafından yönetilmektedir (auDA, 2023a). auDA'nın kurallarına göre; ".au" altında doğrudan alan adı tahsis etmek mümkünken, (örn. x.au) SLD altında da alan adı tahsis edilebilmektedir (örn. x.com.au, x.org.au vb.) (auDA, 2023b).

".au" uzantılı bir alan adı alabilmek için, başvuru sahibinin "Avustralya varlığına[1]" sahip olması ve .au Alan Adı Yönetim Kuralları: Lisanslama *(.au Domain Administration Rules: Licensing)* da belirtilen kriterleri belgelendirmesi gerekmektedir. Örneğin, başvuranın "x.com.au" alan adını alabilmesi için ticari bir kuruluş olduğunu belgelendirmesi, "x.org.au" alan adını alabilmesi için kar amacı gütmeyen bir kuruluş olduğunu belgelendirmesi gerekmektedir. Ayrıca, tahsis edilmek istenen ad (x) ile başvuru sahibinin ticaret unvanı, verdiği hizmet, sattığı mal, yönettiği program gibi unsurların adlarıyla aynı veya eş anlamlı olması gerekmektedir (auDA, 2023b).

Yukarıda belirtilen kriterler dışında bazı adların tahsisi belirli kişilere yapılabilmektedir. .au Alan Adı Yönetim Kuralları: Lisanslama'da "Rezerve Adlar *(Reserved Names)*" olarak tanımlanan bu adlar madde 2.6'da: "Avustralya yasalarına göre kısıtlanan veya yasaklanan bir kelime, kısaltma; Avustralya kelimesi de dahil olmak üzere bir Avustralya eyaletinin veya bölgesinin adı veya kısaltması; .au ve DNS'in güvenliği, istikrarı ve bütünlüğü açısından risk oluşturabilecek adlar" olarak ifade edilmiştir (auDA, 2023b.)

---

[1] Avustralya varlığına" sahip olmak, .au Alan Adı Yönetim Kuralları: Lisanslama'da tanımlanan ve Avustralya vatandaşı veya Avustralya daimi ikamet vizesi sahibi olma, Şirketler Yasası 2001(Cth) uyarınca kayıtlı bir şirket olma gibi farklı durumları içeren terimdir. Daha fazla bilgi için bkz. (https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-11), (08.12.2023)

.au Alan Adı Yönetim Kuralları: Lisanslama'da DNS Abuse tanımı yapılmış ve DNS Abuse "Yasaklanmış kullanımlar *(Prohibited uses)*" arasında sayılmıştır (auDA, 2023b). Yapılan tanımda ICANN'e atıf yapıldığı görülmüştür:

> *"Alan Adı Sisteminin Kötüye Kullanımı veya DNS Abuse, bu terimlerin İnternet Tahsisli Sayılar ve İsimler Kurumu'nun 19 Mart 2021 tarihinde yayınlanan SAC115 (ICANN Güvenlik ve İstikrar Danışma Komitesi'nin DNS'de Kötüye Kullanımın Ele Alınmasına Yönelik Birlikte Çalışabilir Yaklaşıma İlişkin Raporu) raporunun 2.1. Bölümünde tanımlandığı veya bunu takip eden herhangi bir eşdeğer belgede tanımlandığı şekliyle kötü amaçlı yazılım, köle bilgisayar ağları, site trafiği yönlendirme, kimlik avı/oltalama ve istenmeyen elektronik posta (bu tanımda belirtilen diğer DNS Abuse türleri için bir dağıtım mekanizması olarak kullanıldığında) anlamına gelir."* (auDA, 2023b).

.au Alan Adı Yönetim Kuralları: Lisanslama'da DNS Abuse'a ilişkin uygulanacak eylemler özelinde bir hüküm bulunmamakla birlikte, auDA'nın tamamen kendi takdirine göre ".au" uzantılı bir alan adını durdurabileceği veya iptal edebileceği belirtilmiştir (auDA, 2023b).

auDA, DNS Abuse ile mücadele prosedürünü kurumsal internet sitesinde yayınladığı ".au'da DNS Abuse ile Mücadele - Bilgi Notu"nda açıklamıştır. Bu bilgi notunda ".au" uzantılı alan adlarının DNS Abuse'e maruz kalma oranının çok az olduğu belirtilmiştir (auDA, 2023c). Bu oranın az olmasında ".au" uzantılı alan adlarının belgeli olarak ve Avustralya varlığına sahip olan kişilere tahsis edilme şartının etkili olduğu değerlendirilmektedir. Bilgi notunda ayrıca, DNS Abuse'a maruz kalan alan adlarının neredeyse tamamının internet sitesi güvenliğinin ihlal edilmesinden kaynaklandığı belirtilmiş ve güvenlik ihlallerinin genellikle internet sitesi yazılımının güncellenmemesi veya yetersiz güvenlik düzeyi nedeniyle gerçekleştiği ifade edilmiştir (auDA, 2023c). İnternet sitesinin DNS Abuse'e karşı korunmasına ilişkin

olarak da auDA kurumsal internet sitesinde “İnternet Sitenizi DNS Abuse’e Karşı Koruyun - Bilgi Notun” yayınlanmıştır (auDA, 2023ç).

auDA, DNS Abuse ile mücadelede aşağıdaki yöntemleri uygulamaktadır:

- Tahsis sırasında kimlik bilgisi kontrolü
- Tahsis sonrası doğrulama kontrolleri
- DNS Abuse tehdit istihbaratı yayınlarının “.au” uzantılı alan adları kapsamında günlük incelenmesi ve kontrollerin yapılması
- Açık ve erişilebilir şikayet süreci (auDA, 2023c).

auDA, “.au” uzantılı alan adlarını DNS Abuse kapsamında resen inceleyebildiği gibi, kendisine yapılan şikayetler sonucu da inceleme başlatabilmektedir. Ancak, şikayetin ilk olarak alan adının yönetildiği kayıt kuruluşuna yapılması gerekmekte, kayıt kuruluşu tarafından şikayet çözülemediği durumda auDA’ya şikayet edilebilmektedir (auDA, 2023c).

auDA tarafından yapılan DNS Abuse tespitinden sonra, ilgili alan adı sahibi ile iletişime geçilmekte ve DNS Abuse’un ortadan kaldırılması için 72 saatlik süre tanınmaktadır. Ayrıca, ilgili kayıt kuruluşuna da alan adı sahibi ile iletişime geçmesi için istekte bulunulmaktadır. 72 saatlik süre zarfında DNS Abuse devam ederse alan adı durdurulmaktadır (auDA, 2023c).

auDA, farkındalık çalışmaları çerçevesinde “İnternet sitenizi DNS Abuse’a Karşı Koruyun” başlıklı bir bilgi notunu kurumsal internet sitesinde yayınlamıştır. Bilgi notunda DNS Abuse’un ne olduğu, internet sitesinin ele geçirilmesi halinde neler yapılması gerektiği ve internet sitesi güvenliğini sağlamak için alınması gereken önlemler hakkında bilgi verilmiştir (auDA, 2023ç).

Hesap güvenliği kapsamında auDA, “auDA Kayıt Kuruluşu Sözleşmesi (*auDA Registrar Agreement*)”’nde kayıt kuruluşlarına bazı sorumluluklar yüklemiştir. Bu

sorumluluklar çerçevesinde kayıt kuruluşu müşteri hesaplarına girişte ve alan adı sahibi verilerindeki değişikliklerde çok faktörlü kimlik doğrulamanın yapılması gerekmektedir (auDA, 2020, s.73):

> *"**Çizelge D - Asgari Kontroller***
>
> ***1. Çok faktörlü kimlik doğrulama***
>
> *1.1 Çok faktörlü kimlik doğrulama en azından aşağıdakiler için uygulanmalıdır:*
>
> *(a) Kayıt kuruluşu müşterileri*
>
> *(i) Kayıt kuruluşu hizmetlerine erişimi sağlayan müşteri arayüzlerine girişte*
>
> *(ii) Müşterinin alan adı sahibi verilerinde herhangi bir değişiklik yapmasını halinde*
>
> *(b) Kayıt kuruluşu personeli*
>
> *(i) Alan adı sahibi verilerine herhangi bir düzeyde erişim sağlayan tüm arayüzlerde*
>
> *1.2 E-posta, telefon ve SMS çok faktörlü kimlik doğrulama biçimleri olarak kullanılmayacaktı*r."

Bunlara ek olarak auDA, ".au" uzantılı alan adlarının güvenilir olması için Avustralya kolluk kuvvetleri, istihbarat kurumları, düzenleyici kurumlar ve tüketici işleri ve ticaret kurumları ile düzenli olarak iletişim halinde olduğunu belirtmiştir (auDA, 2023c).

auDA, DNSSEC kapsamında ".au" bölgesini 20 Kasım 2014 tarihinde imzalamış, ilgili kayıtları da 20 Kasım 2014 tarihinde IANA'ya sunmuştur. Bu kayıtlar 26 Kasım 2014 tarihinde kök bölge dosyasında yayınlanmıştır. 2014 Aralık ayında da "csiro.au" ve "oz.au" ikinci derece alan adları kayıtları ".au" bölgesine eklenmiştir (auDA, 2024).

4.3. Belçika

Belçika'nın ccTLD'si ".be"dir ve kar amacı gütmeyen bir kuruluş olan DNS Belgium tarafından yönetilmektedir (DNS Belgium, 2024c). ".be" uzantılı alan adları herkes tarafından belgesiz olarak tahsis edilebilmekte ve tahsis işlemlerinde ilk gelen ilk alır kuralı[2] işletilmektedir (DNS Belgium, 2024a, DNS Belgium, 2022).

".be alan adı kayıtları için şartlar ve koşullar (*Terms and conditions for .be domain name registrations)*"'da, DNS Abuse'a benzer olarak "alan adı kötüye kullanımı (*domain name abuse*)" ifadesi yer almaktadır. İlgili madde; DNS Belgium'un alan adı kötüye kullanımıyla mücadele çerçevesinde, alan adı sahibi iletişim bilgilerinin ve alan adıyla ilgili teknik bilgilerin diğer kayıt otoriteleriyle paylaşımıyla ilgilidir (DNS Belgium, 2023a).

DNS Belgium, DNS Abuse ile mücadelede birçok yöntem kullanmaktadır. Bu yöntemlerin merkezinde ise alan adı kayıt bilgilerinin kontrolü yer almaktadır. Bunun yanı sıra, makine öğreniminin kullanıldığı sistemler, alan adı kilidi hizmetleri, kurum ve kuruluşlar ile iş birliği, farkındalık çalışmaları ve DNSSEC teknolojisi DNS Abuse ile mücadelede kullanılan diğer yöntemler arasındadır. Bu yöntemler sırasıyla şu şekildedir:

- **Alan Adı Kayıt Bilgilerinin Kontrolü**

".be" uzantılı bir alan adının tahsis işlemi sonrasında, kayıt bilgileri otomatik olarak makine öğrenmesine dayalı bir dizi parametreye göre kontrol edilmektedir. Kontrol sonrası sorunlu görülen alan adının yetkili ad sunucu bilgileri etkisiz kılınmakta ve alan adı sahibi kimlik bilgileri kontrol süreci başlatılmaktadır. Bu süreç genel hatlarıyla ".be alan adı kayıtları için şartlar ve koşullar" 11 inci maddede ifade edilmiştir (DNS Belgium, 2023a; DNS Belgium, 2024a; DNS Belgium, 2024b).

---

[2] Alan adının, ilk başarılı başvuru yapan kişiye tahsis edilmesidir.

Sürecin başında alan adı sahibi, kimlik bilgilerini kanıtlaması gerektiğini belirten bir elektronik posta almaktadır. Bu elektronik postada, alan adı sahibinin kimlik bilgilerini doğrulayabileceği, kayıt otoritesi internet sitesine ait bir bağlantı bulunmaktadır. Eğer kayıt kuruluşu, alan adı sahibinin kendisini bilgilendirmek istediğini sistem ayarlarında seçtiyse, ilgili bağlantıyı göndermekle sorumlu olmaktadır. Alan adı sahibinin yanı sıra kayıt kuruluşu da doğrulama yapılanana kadar alan adının aktif edilmeyeceği ve aynı kişi tarafından yapılacak başka başvurular için doğrulama sağlanana kadar bu mesajın alınacağı şeklinde bilgilendirilmektedir (DNS Belgium, 2024a).

Alan adı sahibi iletilen bağlantıya erişerek, elektronik kimlik doğrulama yöntemleriyle[3]veya ilgili belgeleri güvenli yerlere yükleyerek doğrulama adımını gerçekleştirebilmektedir (DNS Belgium, 2024a). DNS Belgium yüklenecek belgeleri ayrıntılı bir şekilde açıklamıştır. Açıklamada, alan adı sahibinin Avrupa Birliği veya Avrupa Ekonomik Bölgesi'nde yerleşik olup olmaması ve özel kişi-tek kişilik işletme veya tüzel kişi olması bakımından sınıflandırmaya gidilmiştir. Tüm sınıflarda kimlik tespiti için doğum yeri ve tarihi, cinsiyet ve fotoğraf gibi gerekli olmayan bilgilerin paylaşılmasının gerekli olmadığı, doğrulama işleminin ad ve adres bilgisi kontrolü olduğu ve kimlik belgesinin bir sureti, elektrik faturası gibi gerekli tüm belgelerin iletilmesi gerektiği belirtilmiştir (DNS Belgium, 2024ç). DNS Belgium istenecek belgeler bakımından dört farklı sınıf oluşturmuştur:

> *"1. Alan adınızı Avrupa Birliği veya Avrupa Ekonomik Alanı dahilinde özel bir kişi veya tek kişilik bir işletme olarak mı kaydettirdiniz?*
>
> - *Alan adı sahibinin ulusal kimlik belgesinin ön yüzünün sureti*
> - *Alan adı sahibinin ulusal pasaportundaki bilgilerin sureti*

[3] Elektronik kimlik, çevrimiçi hizmetlere güvenli erişim sağlamak ve elektronik işlemleri daha güvenli bir şekilde yürütmek için kullanılan araçlardan biridir. Daha fazla bilgi için bkz. (https://digital-strategy.ec.europa.eu/en/policies/electronic-identification), (26.03.2024)

- *Alan adı sahibinin ulusal sürücü belgesinin kredi kartı versiyonunda ön yüzünün, kağıt versiyonunda iç tarafının sureti*
- *Alan adı sahibinin uluslararası sürücü belgesinin iç tarafının sureti*
- *Alan adı sahibinin adına bir altyapı şirketi tarafından (gaz, elektrik, su, internet) düzenlenmiş yakın tarihli bir faturanın sureti*
- *Alan adı sahibini içeren noter tasdikli belgenin aslı veya sureti*
- *Alan adı sahibinin mahkeme tarafından tüzel kişiliğinin tasdik edildiği belgenin sureti*
- *Alan adı sahibinin kimliğini açıkça gösteren ve kamuya açık olmayan diğer herhangi bir belge sureti veya sertifika*

2. Alan adınızı Avrupa Birliği veya Avrupa Ekonomik Alanı dışında özel şahıs veya tek kişilik bir işletme olarak mı kaydettirdiniz?

- *Alan adı sahibinin ulusal kimlik belgesinin sureti*
- *Alan adı sahibinin ulusal pasaportundaki bilgilerin sureti*
- *Alan adı sahibinin ulusal sürücü belgesindeki bilgilerin sureti*
- *Alan adı sahibinin adına bir altyapı şirketi tarafından (gaz, elektrik, su, internet) düzenlenmiş yakın tarihli bir faturanın sureti*
- *Alan adı sahibini içeren noter tasdikli belgenin aslı veya sureti*
- *Alan adı sahibinin kimliğini açıkça gösteren ve kamuya açık olmayan diğer herhangi bir belge sureti veya sertifika*

3. Alan adınızı Avrupa Birliği veya Avrupa Ekonomik Alanı dahilinde bir tüzel kişilik (şirket veya kuruluş) için mi kaydettirdiniz?

- *Tüzel kişiliği temsil eden bir kişinin ulusal kimlik kartının ön yüzünün sureti*
- *Tüzel kişilik adına bir altyapı şirketi tarafından (gaz, elektrik, su, internet) düzenlenmiş yakın tarihli bir faturanın sureti*

- *UBO kaydında[4] belirtildiği gibi tüzel kişinin iletişim verilerinin aslı veya çıktısı*
- *Tüzel kişiliğin iletişim bilgilerini belirten noter onaylı bir senedin aslı veya sureti*
- *Tüzel kişilik belgesi aslının katiplikten alınmış mühürlü sureti*
- *Aslının herkesin erişimine açık olmadığı durumlarda, Avrupa Birliği veya Avrupa Ekonomik Alanı üyesi devletinin ulusal ticaret odası tarafından düzenlenen, tüzel kişinin iletişim verilerini içeren yeni ve mümkünse onaylı dijital aslı*
- *Aslının herkesin erişimine açık olmadığı durumlarda, Avrupa Birliği veya Avrupa Ekonomik Alanı üye devleti ulusal ticaret sicilinin, tüzel kişinin iletişim verilerini içeren yeni ve mümkünse onaylı dijital aslı*
- *Tüzel kişinin kimliğini açıkça gösteren ve kamuya açık olmayan diğer herhangi bir belge sureti veya sertifika*

4.Alan adınızı Avrupa Birliği veya Avrupa Ekonomik Alanı dışında bir tüzel kişilik (şirket veya kuruluş) için mi kaydettirdiniz?

- *Tüzel kişiliği temsil eden bir kişinin ulusal kimlik kartının sureti*
- *Tüzel kişilik adına bir altyapı şirketi tarafından (gaz, elektrik, su, internet) düzenlenmiş yakın tarihli bir faturanın sureti*
- *Tüzel kişiliğin iletişim bilgilerini belirten noter onaylı belge aslının kendisi veya sureti*
- *Aslının herkesin erişimine açık olmadığı durumlarda, ulusal ticaret odası tarafından düzenlenen, tüzel kişinin iletişim verilerini içeren yeni ve mümkünse onaylı dijital özeti*

---

[4] UBO kaydı, bir şirketin veya başka bir tüzel kişiliğin tüm "Nihai İntifa Hakkı Sahiplerinin" veya "nihai lehtarlarının" kayıtlı olduğu bir kayıttır. Daha fazla bilgi için bkz. (https://financien.belgium.be/nl/E-services/Ubo-register), (27.03.2024)

- *Aslının herkesin erişimine açık olmadığı durumlarda, ulusal ticaret sicilinin, tüzel kişinin iletişim verilerini içeren yeni ve mümkünse onaylı dijital özeti*
- *Tüzel kişinin kimliğini açıkça gösteren ve kamuya açık olmayan diğer herhangi bir belge sureti veya sertifika"* (DNS Belgium, 2024ç).

Alan adı sahibi, kimlik bilgilerini doğrulayabilmesi için kendisine iletilen bağlantıya erişerek elektronik kimlik doğrulama yöntemleriyle veya ilgili belgeleri güvenli yerlere yükleyerek doğrulama adımını gerçekleştirebilmektedir. Alan adı sahibinin elektronik kimlik doğrulama yöntemini kullandığı durumda, alan adı otomatik olarak onaylanmakta ve bir saat içinde aktif hale gelmektedir. İlgili belgelerin yüklenmesi halinde DNS Belgium destek personeli tarafından bu belgeler kontrol edilmektedir. Kontrol işlemi beş güne kadar sürebilmekte ve ihtiyaç olması halinde alan adı sahibiyle iletişime geçilmektedir (DNS Belgium, 2024a).

Yapılan kontrol sonucu iletilen belgelerin uygun görülmesi halinde alan adı sahibi, alan adının aktif edildiği ve sistemdeki bu kullanıcı kimliği ile başka bir alan adı için başvuru yapılması halinde başvurunun otomatik olarak kabul edileceği konusunda bilgilendirilmektedir. Alan adı sahibinin farklı kullanıcı kimliğiyle başvuruda bulunması halinde ise, kimlik bilgileri kontrol süreci tekrar işletilebilecektir (DNS Belgium, 2024a).

Alan adı sahibinin doğrulama için yeterli bilgi iletmemesi halinde DNS Belgium destek personeli tarafından ek bilgi talep edilmektedir. Yeterli bilgi iletilinceye kadar alan adı kullanılamamaktadır ancak kayıtlı olmaya devam etmektedir. Alan adı sahibinin hiç belge iletmediği durumda da benzer olarak alan adı kullanılamamakta fakat kayıtlı olmaya devam etmektedir. Aynı kullanıcı kimliğiyle tahsis edilen diğer tüm yeni alan adları da doğrulama sürecine girmekte ve bu alan adları DNS Belgium'un açılış sayfasına yönlendirilmektedir. Daha önce aynı kullanıcı kimliğiyle kaydedilen alan adları bu durumdan etkilenmemektedir (DNS Belgium, 2024a).

Alan adı sahibi kimlik bilgilerinin doğrulama işlemi DNS Belgium'un izni halinde kayıt kuruluşu tarafından da yapılabilmektedir. Kayıt kuruluşunun bu işlemi yapabilmesi için doğrulamanın yapıldığı tarihin ve doğrulamaya dayanak oluşturacak belgelerin temin edilmesi gerekmektedir. DNS Belgium bu belgelerin neler olabileceğini yine ayrıntılı bir şekilde açıklamıştır:

- "*Avrupa tarafından, yüksek düzeyde güvenilir bir kimlik doğrulama aracı olduğu resmi olarak onaylanan "itsme®" elektronik kimlik doğrulama yöntemi*
- *Alan adı sahibinin ulusal kimlik belgesi*
- *Alan adı sahibinin ulusal pasaportu*
- *Alan adı sahibinin oturma izni*
- *Alan adı sahibinin ulusal sürücü belgesi*
- *Alan adı sahibinin uluslararası sürücü belgesi*
- *Alan adı sahibine bir altyapı şirketi tarafından (gaz, elektrik, su, internet) düzenlenmiş fatura*
- *UBO kaydında belirtildiği gibi tüzel kişinin iletişim verilerinin aslı*
- *Alan adı sahibinin adını belirten noter onaylı senedin aslı*
- *Alan adı sahibinin mahkeme tarafından tüzel kişiliğinin tasdik edildiği belgenin aslı*
- *Tüzel kişi alan adı sahibinin ticaret odasından aldığı belge*
- *Alan adı sahibinin tüzel kişiliğini gösteren ticaret sicilinin aslı*
- *Alan adı sahibinin tüzel kişiliğine ait lisanslı sertifikası*
- *Alan adı sahibinin tüzel kişiliğini gösteren kayıt kuruluşu ile yapılan sözleşme*
- *LEI yayınlayıcısının faturası ve/veya alan adı sahibinin tüzel kişiliğini belirten LEI numarası*[5]
- *Alan adı sahibinin tüzel kişiliğini gösteren LEI portalının ekran görüntüsü*

---

[5] LEI Yayınlayıcısı (LEI Publisher), "Tüzel Kişi Kimlik Kodu *(Legal Entity Identifier - LEI)"* numaralarını yayınlayan ve bu numaraları güncelleyen kuruluşlardan biridir.. LEI, bir işletmenin küresel olarak benzersiz bir tanımlayıcısıdır ve finansal işlemlerde, raporlamada ve diğer işlemlerde kullanılmaktadır.

- *Alan adı sahibine yapılan banka ödemesi*
- *Alan adı sahibinin iletişim bilgilerini içeren ve hesabın sahibi olduğunu teyit eden bankadan alınmış beyan*
- *Alan adı sahibinin yetkili bir temsilcisi tarafından usulüne uygun olarak imzalanmış olan ve alan adı sahibinin tüzel kişiliğini, temsil etmeye veya onun adına hareket etmeye yetkili vekili belirten belge*
- *Hollanda bankaları tarafından geliştirilen ve kişilerin kendi bankalarının güvenli ve güvenilir giriş yöntemlerini kullanarak kendilerini diğer kuruluşlarda tanıtmalarını sağlayan bir hizmet olan IDIN*
- *Alan adı sahibinin kimliğini açıkça gösteren ve kamuya açık olmayan diğer belge veya sertifikalar"* (DNS Belgium, 2024a).

Kayıt kuruluşunun doğrulama sürecinde en azından elektronik posta adresi, isim ve adres bilgilerini kontrol etmesi gerektiği DNS Belgium tarafından belirtilmiştir. DNS Belgium ayrıca, yürütülen doğrulama süreci dokümantasyonunun, süreç akışının doğru ve ayrıntılı bir açıklamasını içermesini ve müşteri bilgilerinin ne zaman ve nasıl kontrol edildiğini göstermesi gerektiğini ifade etmiştir (DNS Belgium, 2024a).

Yeni tahsis edilen ".be" uzantılı alan adlarının kayıt bilgileri, makine öğrenmesine dayalı yapılan inceleme sonucu başlatılan süreç dışında manuel olarak da incelenmektedir. Bu incelemeye, kimlik bilgileri kontrol sürecini başarıyla tamamlayan alan adları da girmektedir. Alan adı sahibi bilgilerinin doğru veya tam olmadığı durumlarda, bilgilerin güncellenmesi hususunda alan adı sahibiyle iletişime geçilmektedir. Alan adı sahibinin bu bilgileri on dört gün içinde değiştirmemesi halinde ise alan adının kullanımı durdurulmaktadır. Bu tarihten sonraki on dört gün içerisinde de bilgiler güncellenmezse alan adı iptal edilmekte ve alan adı karantinaya alınmaktadır. Karantinaya alınan alan adları kırk gün sonra başvuruya açılmakta ve tahsis edilebilmektedir (DNS Belgium, 2024b). Kırk günlük süre, süreç özelinde olmayıp, iptal gerekçesi ne olursa olsun beklenen bir süredir (DNS Belgium, 2023a). Alan adının dolandırıcılık yapılan alan adlarının bulunduğu listede yer alması halinde ise on dört günlük süre beklenmeyerek alan adının kullanımı durdurulmaktadır. Bu

durumda, alan adı sahibine bilgileri güncellemesi için dört haftalık süre tanınmaktadır. Açıklanan bu süreç, ".be alan adı kayıtları için şartlar ve koşullar" 3 üncü maddenin (d) bendi ile 8 inci maddenin (b) bendinde ifade edilmiştir (DNS Belgium, 2023a; DNS Belgium, 2024b).

".be" uzantılı bir alan adının, irtibat bilgilerinin veya elektronik posta adresinin yanlış olduğu üçüncü taraflarca tespit edilmesi halinde ilgili alan adı şikayet edilebilmektedir. Bu şikayet, alan adı kayıt bilgilerinin bulunduğu sayfadan veya DNS Belgium internet sitesinde yer alan iletişim formu aracılığıyla yapılabilmektedir. İletişim formunda; alan adı, isim ve soyisim, elektronik posta adresi ve şikayetin yazılacağı bölümler bulunmaktadır. DNS Belgium, ".be alan adı kayıtları için şartlar ve koşullar", 8 inci madde (b) bendi gereğince; üçüncü tarafın şikayetine bağlı olarak da alan adı sahibi kimlik bilgileri kontrol sürecini başlatabilmektedir (DNS Belgium, 2023a; DNS Belgium, 2024b; DNS Belgium, 2024d).

Makine öğrenmesine dayalı bir dizi parametreye göre yapılan kontrol sürecinin yanında potansiyel şüpheli kayıtları kısa sürede tespit etmek için makine öğrenmesinin kullanıldığı ve ".nl" uzantılı alan adları kayıt otoritesi SIDN tarafından geliştirilen RegCheck sistemi kullanılmaktadır. RegCheck'in kaynak kodları SIDN tarafından geliştirilmesine rağmen ".be" uzantılı alan adları için DNS Belgium tarafından özelleştirilmiştir. RegCheck'in bu versiyonunda sistem, iptal edilen alan adları ile alan adı sahibi kimlik doğrulama sürecini tamamlayamadığı için aktif edilmeyen alan adları ile eğitilmektedir. RegCheck sistemi tarafından yüksek risk puanı tespit edilen ".be" uzantılı alan adı tahsislerinde, alan adı sahibinden kimlik bilgilerini kanıtlanması istenmektedir. Kimlik bilgileri doğrulanana kadar da alan adı aktif edilmemektedir (DNS Belgium, 2023b; DNS Belgium, 2024e).

- **Kurum ve Kuruluşlar ile İş birliği**

DNS Belgium, DNS Abuse ile mücadelede bazı güvenlik firmaları ve tarayıcı geliştiricisiyle birlikte çalışmaktadır. Bu firmalar, ".be" uzantılı bir alan adında kötüye

kullanım tespit ettiği zaman, alan adı sahibine ve hizmet veren kayıt kuruluşuna DNS Belgium tarafından otomatik bir mesaj gönderilmektedir. Mesajda; dolandırıcılık faaliyeti içeren internet sitesi sayfalarını kaldırma sorumluluğunun alan adı sahibinde olduğu belirtilmektedir. Bunun yanı sıra, alan adının kötüye kullanıldığının veya internet sitesine normal bir şekilde erişilemediğinin fark edilmesi durumunda, yetkili makamların uygun önlemleri alabilmesi için, alan adı sahibinin hızlı bir şekilde müdahalede bulunması tavsiye edilmektedir (DNS Belgium, 2024b).

DNS Belgium ayrıca, Belçika'nın "Ekonomi Bakanlığı" olan FPS Economy ile sahte internet mağazaları ve kimlik avı/oltalama konusunda iş birliği yapmaktadır. Sahte internet mağazaları, internet siteleri üzerinden alışveriş yapılan ancak ücretin ödenmesine rağmen ürünün teslim edilmeyerek dolandırıcılık faaliyetinin gerçekleştirildiği platformlardır. Bu platformlarda kişilerin kredi kartı bilgileri de ele geçirildiği için kısa sürede müdahalede bulunulması gerekmektedir. Bu kapsamda, FPS Economy tarafından DNS Belgium'e ".be" uzantılı bir alan adı için bildirim yapıldığında alan adının kullanımı durdurulmaktadır. Alan adı sahibi, yapılan işlemin haksız olduğuna ilişkin iki hafta içerisinde itirazda bulunabilmektedir. İtirazda bulunulmadığı veya yapılan itirazın kabul görmediği durumlarda alan adı, durdurulma tarihinden altı ay sonra iptal edilmektedir. Bu prosedürün ciddi suç teşkil eden durumlarda uygulandığı DNS Belgium tarafından ifade edilmektedir. DNS Belgium ayrıca, sahte internet mağazalarını tespit için kendi yöntemleri geliştirdiğini belirtmiştir (DNS Belgium, 2018; DNS Belgium, 2024b).

- **Alan Adı Koruması**

DNS Belgium DNS Abuse ile mücadele alan adı kilidi hizmeti sunmaktadır. Bu hizmet; "Alan Adı Koruması *(Domain Guard)*" ve "Alan Adı Kalkanı *(Domain Shield)*" olmak üzere iki farklı şekilde sunulmaktadır. Alan adı korumasında süreç daha çok kayıt otoritesi tarafından yürütülürken, alan adı kalkanında kayıt kuruluşu daha aktif rol almaktadır. Ayrıca, alan adı koruması kontrol süreçleri alan adı kalkanına göre daha sıkıdır. Her iki hizmet de ".be alan adı kayıtları için şartlar ve

koşullar" 3 üncü maddenin (f) bendinde genel olarak belirtilmiştir. (DNS Belgium, 2023a; DNS Belgium, 2024f; DNS Belgium, 2024g).

Alan adı koruması hizmeti alınan alan adlarında; yetkisiz olarak alan adı kayıt bilgilerinin değiştirilmesi, alan adı sahibinin değiştirilmesi, alan adının transferi ve alan adından feragat edilmesi engellenmektedir. Alan adı korumasına, hizmet alınan kayıt kuruluşu aracılığıyla DNS Belgium tarafından oluşturulan talep formu ile başvuruda bulunulmaktadır. Başvuru; alan adı sahibi, alan adı sahibi tarafından yetkilendirildiğini belgelendiren kişi ve alan adı sahibi tarafından vekalet verilen kişi tarafından yapılabilmektedir. Talep formu ile birlikte formda belirtilen ilgili belgelerin de iletilmesi gerekmektedir. DNS Belgium tarafından, başvuruda yazılmış alan adı sahiplik bilgisi ile Whois'deki alan adı sahibi bilgilerinin uyuşup uyuşmadığı, formun imzalanıp imzalanmadığı, belirtilen telefon numarasının doğru olup olmadığı incelenmekte, form ile birlikte gönderilen ekler kontrol edilmektedir. Gelen başvurunun uygun bulunması halinde alan adı koruma hizmeti etkinleştirilmekte ve bunun bilgisi alan adı sahibi ve kayıt kuruluşuna otomatik olarak bildirilmektedir. Uygun bulunmama durumunda ise kayıt kuruluşu ile iletişime geçilmektedir. (DNS Belgium, 2024a; DNS Belgium, 2024f; DNS Belgium, 2024ğ).

Alan adı koruması hizmetinin başlamasından sonra, alan adı kayıt veya sahiplik bilgilerinin değiştirilebilmesi için alan adı korumasının geçici olarak devre dışı bırakılması gerekmektedir. Devre dışı bırakılma isteği kayıt kuruluşu aracılığıyla yapılmaktadır. DNS Belgium gelen isteğe binaen alan adı sahibi tarafından yetkilendirilen kişilerden birisini aramakta ve talebe onay vermesini istemektedir. Yetkili kişiye saat dilimi farklılığından dolayı telefonla ulaşılamaması durumunda, telefon görüşmesi için elektronik posta yoluyla tarih ve saat belirlenebilmektedir (DNS Belgium, 2024a; DNS Belgium, 2024f).

İşleme onay verilmesinden sonra alan adı sahibi ve kayıt kuruluşuna, alan adı korumasının geçici olarak devre dışı bırakılması için DNS Belgium tarafından bir onay elektronik postası iletilmektedir. Alan adı sahibi ve kayıt kuruluşu tarafından onay

verilmesi halinde, alan adı koruması kırk sekiz saat süreyle geçici olarak devre dışı bırakılmaktadır. Bu sürenin sonunda veya kayıt kuruluşu tarafından hizmetin tekrar devreye alınması isteğinin iletilmesi halinde alan adı koruması tekrar devreye alınmaktadır (DNS Belgium, 2024a; DNS Belgium, 2024f).

Alan adı koruma hizmeti geçici olarak bir yılda en fazla dört kez devre dışı bırakılabilmektedir. Hizmetin geçici olarak devreden alındığı hallerde alan adı transferi veya feragat işlemleri talep edilememekte, bu işlemlerin yapılabilmesi için hizmetin sonlandırılması gerekmektedir. Alan adı koruması hizmetinde yetkilendirilen kişilerin değiştirilmesi için ise DNS Belgium tarafından hazırlanan formun kayıt kuruluşu aracılığıyla iletilmesi gerekmektedir (DNS Belgium, 2024f; DNS Belgium, 2024h).

Alan adı koruma hizmeti herhangi bir zamanda sonlandırılabilmektedir. Bunun için DNS Belgium tarafından hazırlanan formun imzalanarak kayıt kuruluşu aracılığıyla iletilmesi gerekmektedir. Hizmetin sonlandırılması halinde alan adı sahibi ve kayıt kuruluşu bilgilendirilmektedir. Bu hizmetten tekrar yararlanabilmek için başvuru sürecinin tekrarlanması ve hizmet ücretinin ödenmesi gerekmektedir (DNS Belgium, 2024f; DNS Belgium, 2024ı). Alan adı koruma hizmeti için kayıt kuruluşundan alınan tutar vergi hariç yıllık € 80,00'dur (DNS Belgium, 2024a).

- **Alan Adı Kalkanı**

".be" uzantılı alan adlarında alan adı koruma hizmetinin yanı sıra çalışma mantığı çok benzer olan alan adı kalkanı hizmeti de sunulmaktadır. Bu hizmet için kayıt kuruluşlarından herhangi bir ücret alınmamaktadır (DNS Belgium, 2024a). Alan adı kalkanı hizmeti alınan alan adlarında da yetkisiz olarak alan adı kayıt bilgilerinin değiştirilmesi, alan adı sahibinin değiştirilmesi, alan adının başka bir kayıt kuruluşuna transferi ve alan adından feragat edilmesi engellenmektedir. Bu hizmet sadece alan adı kalkanı kapsamında DNS Belgium ile bir sözleşme yapan kayıt kuruluşları tarafından sunulmaktadır. Bu sebeple, ilk olarak kayıt kuruluşunun bu hizmeti sunup

sunmadığının kontrol edilmesi gerekmektedir. Eğer hizmet sunuluyor ise, alan adı sahibi tarafından alan adı kalkanını etkinleştirmek veya devre dışı bırakmak için kayıt kuruluşundaki bir veya daha fazla kişiye yetki vermesi gerekmektedir (DNS Belgium, 2024a; DNS Belgium, 2024g).

Alan adı kalkanı hizmetinde, alan adı sahibinin yukarıda engellendiği belirtilen işlemleri yapabilmek için hizmet alınan kayıt kuruluşu ile iletişime geçmesi gerekmektedir. Alan adı kayıt veya sahiplik bilgilerinin değiştirilebilmesi için alan adı kalkanının geçici olarak devre dışı bırakılması yeterliyken, transfer veya feragat işlemleri için hizmetin sonlandırılması gerekmektedir. Hizmet geçici olarak yirmi dört saat süreyle devre dışı bırakılmakta, bu sürenin sonunda veya kayıt kuruluşunun bildirimine binaen daha kısa sürede tekrar devreye alınmaktadır. Hizmetin etkinleştirilmesi veya devre dışı bırakılmasıyla ilgili işlemleri yapan kayıt kuruluşu personeli ile bilgileri değiştiren kayıt kuruluşu personeli farklı kişilerden oluşmaktadır (DNS Belgium, 2024a; DNS Belgium, 2024g).

- **Farkındalık Çalışmaları**

DNS Belgium, alan adı sahiplerini ve son kullanıcıları DNS Abuse kapsamında bilgilendirmek ve farkındalık oluşturmak için çalışmalar yürütmektedir. Alan adı sahiplerini bilgilendirmek üzere oluşturulan süreç "Safebrowsing" olarak adlandırılmaktadır. Bu süreçte, saldırganlar tarafından ele geçirilip kötüye kullanılan alan adlarının yayınlandığı listeler günlük olarak kontrol edilmektedir. Bu listelerde yer alan ".be" uzantılı alan adları tespit edilmekte ve bu alan adlarının sahiplerine bir uyarı elektronik postası iletilmektedir. Elektronik postada hangi alan adlarının kötüye kullanıldığını gösteren bir bağlantı yer almaktadır. Safebrowsing kapsamında DNS Belgium, alan adı sahiplerinin ne yapabileceğine ilişkin olarak da kurumsal internet sitesinde tavsiyeler yayınlamıştır:

1. *"İnternet sitenizin yöneticisi ile iletişime geçin. Virüslü dosyaların tespit edilmesine ve kaldırılmasına yardımcı olacak en iyi konumda*

olan kişi internet sitesi yöneticisidir. Virüs bulaşmış tüm dosyaların kaldırılması önemlidir. Her zaman internet sitesinin yeni bir yedekleme ile değiştirilmesini tavsiye ederiz.

2. *Yer sağlayıcı hesabınızın tüm şifrelerinin değiştirerek saldırganlar tarafından eski verilere erişimi engelleyin.*
3. *Güvenlik taraması yapın veya yaptırın. Saldırganların internet sitenize nasıl erişim sağladığını tespit edemiyorsanız, internet sitenizi geri yüklemek için bir yedekleme sürümü kullansanız bile bunu tekrar yapma ihtimalleri olacaktır.*" (DNS Belgium, 2024i).

DNS Belgium, safebrowsing kapsamında yayınladığı tavsiyelerin yanı sıra kimlik avı yöntemleri, sahte internet mağazaları ve çevrimiçi dolandırıcılık ile ilgili farkındalığı artırmak amacıyla kurumsal internet sitesinde bilgilendirme sayfaları yayınlamaktadır. Bu sayfalarda, internette nasıl güvende olunabileceğine ilişkin bilgiler ve mağdur olunduğu zaman ne yapılması gerektiğine ilişkin tavsiyelerde bulunulmaktadır. DNS Belgium ayrıca, DNS Abuse kapsamında iş birliği yaptığı kurum ve kuruluşları internet sitesinde yayınlamıştır (DNS Belgium, 2024j).

- **DNSSEC**

DNS Abuse ile mücadelede kullanılan araçlardan biri olan DNSSEC teknolojisi ".be" uzantılı alan adlarında kullanılmaktadır. Alan adı sahipleri, kayıt kuruluşları aracılığıyla alan adlarını DNSSEC ile güvence altına alabilmektedir (DNS Belgium, 2024k). DNS Belgium, DNSSEC'e ilişkin olarak; DNSSEC uygulaması, DNSSEC anahtarları ve anahtar grupları başlıklı bir bilgilendirme metnini kurumsal internet sitesinde yayınlamıştır (DNS Belgium, 2024a).

4.4. Danimarka

Danimarka'nın ccTLD'si ".dk" dır ve kar amacı gütmeyen bir kurum olan Punktum dk tarafından yönetilmektedir (Punktum dk, 2023b).[6] ".dk" uzantılı alan adları, Danimarka'da yerleşik olanlar tarafından tahsis edilebildiği gibi yerleşik olmayan kişiler tarafından da tahsis edilebilmektedir (Punktum dk, 2023c; Punktum dk, 2023ç). Her iki durumda da alan adı sahiplik bilgilerine dair Punktum dk tarafından, Danimarka Alan Adları Yasası'nın 18. Maddesi gereğince[7] çeşitli kontrol mekanizmaları uygulanmaktadır. (Punktum dk, 2023d; Punktum dk, 2023e; Punktum dk, 2023f; Punktum dk, 2023g; Punktum dk, 2023a).

Danimarka'da yerleşik olan başvuru sahiplerinin tahsis esnasında isim ve adres bilgileri kontrol edilmektedir. Kontrol işlemi; başvuruda iletilen isim ve adres bilgisi ile Danimarka Ulusal Kişiler/Şirketler Sicilinde tanımlı bilgilerin karşılaştırılması yoluyla yapılmaktadır (Punktum dk, 2023d).

Punktum dk, tahsis sonrası yapılan kontroller kapsamında; Danimarka'da yerleşik olan veya olmayan kişiler için iki farklı kimlik kontrol süreci oluşturmuştur. Oluşturulan bu süreçler de kendi içerisinde; yeni alan adı sahibi bilgilerinin kontrolü ve mevcut alan adı sahibi bilgilerinin kontrolü olmak üzere ikiye ayrılmaktadır (Punktum dk, 2023ç). Yeni alan adı sahibi, bir alan adını yeni tahsis eden veya mevcut bir alan adını devralan kişi olarak tanımlanmıştır (Punktum dk, 2023e; Punktum dk, 2023g).

Danimarka'da yerleşik olan kişilerin, kayıt kuruluşları aracılığıyla alan adı tahsis işlemini gerçekleştirdikten sonra Punktum dk'nın talebi üzerine MitID[8] kontrol

---

[6] ".dk"nın kayıt otoritesi Dansk Internet Forum (DIFO) olmasına rağmen ".dk"nın yönetimi, DIFO'nun kurmuş olduğu Punktum dk A/S üzerinden gerçekleştirilmektedir. Daha fazla bilgi için bkz. (https://punktum.dk/en/articles/the-dk-domain), (09.12.2023)

[7] Daha fazla bilgi için bkz. (https://www.retsinformation.dk/eli/ft/201312L00066), (19.12.2023)

[8] MitID, Danimarka'da kullanılan dijital kimliktir. MitID sayesinde kişiler, çevrimiçi bankacılıkta para transferi yapabilmekte veya skat.dk, borger.dk ve sundhed.dk gibi kamu hizmeti verilen çevrimiçi platformlarda oturum açabilmektedir. Daha fazla bilgi için bkz. (https://www.mitid.dk/en-gb/about-mitid/), (20.12.2023)

işlemini gerçekleştirmesi gerekmektedir. Bu kontrol sürecinden, başka bir alan adının kaydıyla bağlantılı olarak süreci başarıyla tamamlamış olup, sistemde tanımlı aynı kullanıcı kimliği ile yeni alan adı sahibi olanlar muaf tutulmaktadır. Alan adı sahibinin kontrol sürecinde, Punktum dk internet sitesindeki "self-servis" bölümüne MitID ile giriş yapması ve giriş yaptıktan sonra gerçek kişi ise sivil kayıt numarasını (CPR), tüzel kişi ise işletme kayıt numarasını (CVR) girmesi gerekmektedir. Punktum dk sistemindeki alan adına ait tanımlı bilgiler ile CPR veya CVR bilgileri eşleştiği durumda alan adı sahiplik bilgileri doğru kabul edilmektedir (Punktum dk, 2023e).

Alan adı sahibi, Punktum dk tarafından belirlenen sürede MitID ile yapılan kontrol işlemini tamamlayamazsa sahip olduğu alan adı veya adları Punktum dk tarafından durdurulmaktadır. Alan adı veya adları durdurulan alan adı sahibinin, MitID kontrolü hakkında Punktum dk müşteri hizmetleri ile iletişime geçmesi ve kontrol işlemini tamamlaması gerekmektedir. Alan adı veya adlarının durdurulduğu tarihten itibaren otuz günlük süre içerisinde MitID kontrolü tamamlanmadığı takdirde, Punktum dk tarafından söz konusu alan adı veya adları iptal edilmektedir. Ayrıca, bazı durumlarda Punktum dk tarafından, alan adı sahibinden kimliğini ve iletişim bilgilerini (örneğin adı, adresi ve telefon numarası) gösteren belgeler de talep edilmektedir (Punktum dk, 2023e).

Danimarka'da yerleşik olan mevcut ".dk" uzantılı alan adı sahibi bilgilerine dair yürütülen kontrol süreci ile yeni alan adı sahibi kapsamında yürütülen kontrol süreci aynı şekilde gerçekleşmektedir (Punktum dk, 2023f).

Yeni alan adı sahibi veya mevcut alan adı sahibi olan ancak Danimarka'da yerleşik olmayan kişiler için, Punktum dk tarafından alan adı sahibi iletişim bilgilerinin ve kimliğinin doğruluğuna ilişkin risk bazlı kontroller gerçekleştirilmektedir (Punktum dk, 2023g; Punktum dk, 2023a). Risk bazlı kontrollerde, sahte alışveriş sitesi olarak kullanılan alan adlarının kayıtlarıyla ilgili bilgiler *(*örneğin mantıksız veri kombinasyonları, bir alan adının ne kadar hızlı yeniden kaydedildiği ve kayıt kuruluşu*)*

otomatik değerlendirme için temel alınmaktadır. (European Commission, 2022, s.159).

Risk değerlendirmesi sonucunda Punktum dk, Danimarka'da yerleşik olmayan yeni alan adı sahibinden; .dk Alan Adının Kullanım "Hakkı İçin Şartlar ve Koşullar *(Terms And Conditions For The Right Of Use To A .dk Domain Name)*" madde 4.3 kapsamında, sistemlerinde kayıtlı iletişim bilgilerinin ve kimliğinin doğruluğunu kanıtlamasını isteyebilmektedir. Bu durumda alan adı sahibinin, resimli kimlik belgesi ve iletişim bilgilerine ilişkin olarak meşru ve yetkili makamlarca yayınlanmış belgeleri Danca veya İngilizce olarak iletmesi gerekmektedir. Punktum dk, belge talebine dair bildiriminde ayrıntılı bilgi verdiğini ifade etmektedir (Punktum dk, 2023c; Punktum dk, 2023a).

Danimarka'da yerleşik olmayan yeni alan adı sahibinden talep edilen belgelerin belirlenen süre içerisinde alınamaması durumunda, alan adı sahibi tarafından tahsis edilen tüm alan adları durdurulmaktadır. Durdurulma tarihinden otuz gün sonra da alan adları iptal edilmektedir. Alan adı sahibi tarafından iletilen belgelerin Punktum dk tarafından uygun bulunmama durumunda alan adı durdurulmaktadır. Punktum dk, durdurulma tarihinden itibaren ilk beş gün içerisinde yeni belge gönderilebileceğini belirtmektedir ancak durdurma süreci boyunca da yeni belge iletilebileceği ifade edilmiştir. Durdurulma tarihinden otuz gün sonra ise alan adı sahibinin alan adı/adları iptal edilmektedir (Punktum dk, 2023a).

Danimarka'da yerleşik olmayan mevcut alan adı sahibi bilgilerine dair yürütülen kontrol süreci ile yeni alan adı sahibi kapsamında yürütülen kontrol süreci aynı şekilde gerçekleşmektedir. Punktum dk, mevcut alan adı sahibi bilgilerinin kontrol edilme sebeplerinin risk bazlı değerlendirmeler dışında, Punktum dk tarafından iletilen elektronik postalara alan adı sahibi tarafından yanıt verilmemesi veya alan adının internet suçlarıyla belirli bir bağlantısı olup olmadığına ilişkin bir değerlendirme olabileceğini belirtmiştir. (Punktum dk, 2023a).

Alan adı sahiplik bilgilerinin doğruluğuna ilişkin uygulanan kontrol mekanizmalarının yanı sıra DNS Abuse ile mücadelede doğrudan aksiyon alınabilmektedir. .dk Alan Adının Kullanım Hakkı İçin Şartlar ve Koşullar'ın "Alan Adının Yasa dışı Kullanımı" başlıklı 9'uncu maddesinin[9] ikinci fıkrası, Punktum dk'ya bu kapsamdaki alan adlarını durdurma yetkisi verilmiştir:

> *"9.2 Punktum dk aşağıdaki durumlarda bir alan adını durdurabilir:*
>
> - *Alan adının açık bir ekonomik suç riski, kimlik avı ve kötü amaçlı yazılım dağıtımı gibi BT ekipmanının tehlikeye atılması ve/veya oldukça saldırgan nitelikteki içerikle bağlantılı olarak kullanılması…"* (Punktum dk, 2023c).

Bu kapsamdaki alan adları dört haftalık bir süre için durdurulmaktadır. Alan adı durdurma kararının Şikayet Kurulu'na[10] götürülmesi halinde ise alan adı karar verilinceye kadar durdurulmaktadır. Durdurma süresinin sona ermesinden sonra alan adı sahibi, durdurmaya neden olan durumun artık mevcut olmadığını Punktum dk'ye kanıtlayamadığı takdirde alan adı Punktum dk tarafından iptal edilmektedir (Punktum dk, 2023c).

Punktum dk, alan adı kilidi hizmeti kapsamında "Very Important Domain (*VID*)" hizmetini sunmaktadır. Bu hizmet, "Alan Adı Sahibi Yönetimi (*Registrant Management*[11])"ni seçen alan adı sahipleri tarafından alınabilmektedir. Alan adı sahibi veya vekili, Punktum dk internet sitesindeki "self-servis" bölümünden ilgili işlemleri yaparak hizmetten yararlanabilmektedir (Punktum dk, 2023ğ).

---

[9] Bu maddenin diğer fıkralarında, tahsisli alan adının neredeyse aynısı olan alan adları; güvenlik veya kamu yararına ilişkin önemli hususları ihlal edip açıkça yasa dışı eylemler veya ihmallerle bağlantılı olarak kullanılan alan adları ve açıkça yasa dışı eylemler veya ihmallerle bağlantılı olarak kullanılan alan adlarına ilişkin hükümler bulunmaktadır.

[10] Danimarka Alan Adları Şikayet Kurulu, ".dk" uzantılı alan adlarıyla ilgili anlaşmazlıkları çözen bağımsız şikayet kuruludur. Daha fazla bilgi için bkz. (www.domaeneklager.dk) (20.12.2023)

[11] .dk Alan Adının Kullanım Hakkı İçin Şartlar ve Koşullar'da alan adı sahibi yönetimi, alan adı kullanım hakkının alan adı sahibi tarafından bizzat yönetilmesi veya anlaşma yoluyla başkalarının bu konuda yardımcı olmasına izin verilmesi olarak tanımlanmıştır.

VID hizmetindeki alan adı için, belirli işlemleri onaylama yetkisine sahip olacak en az bir en fazla üç VID irtibat kişisi atanabilmektedir. Birden fazla VID kişisi atanırsa bunlar eşit statüye sahip olmaktadır. Alan adı sahibi veya vekili, VID kişisini herhangi bir zaman değiştirebilmekte ve yeni VID kişi veya kişileri atayabilmektedir (Punktum dk, 2023ğ).

VID hizmeti kapsamındaki alan adları için yapılacak işlemler farklı süreçler sonucunda gerçekleşmektedir. Alan adı sahibi; "alan adının yenilenmesi, VID kişisinin oluşturulması, VID kişisinin silinmesi, yeni fatura yetkilisi veya vekili atanması" işlemlerini tek başına yapabilirken, "DNSSEC kaydı, DNSSEC iptali, DNSSEC anahtarlarının kaldırılması, DNSSEC anahtarlarının atanması, DNSSEC anahtarlarının yayınlanması ve alan adı sahibi adresinin manuel olarak değiştirilmesi" işlemlerini VID kişisi onayı ile yapılabilmekte, "yetkili ad sunucu değişiklikleri, alan adı transferi, alan adı feragati ve VID hizmet iptali" işlemlerini VID kişisi onayı dışında Punktum dk'nın gönderdiği ve içinde yetki kodu olan taahhütlü mektubu alması halinde yapılabilmektedir (Punktum dk, 2023ğ).

VID hizmeti yıllık olarak verilmektedir. Punktum dk diğer kayıt otoritelerinden farklı olarak hizmetin iptali için de ücret almaktadır. VID hizmetinin yıllık fiyatı vergi dahil 150 Danimarka Kronu iken hizmetin iptal ücreti 180 Danimarka Kronu'dur (Punktum dk, 2024a).

Yukarıda belirtilen çalışmaların yanı sıra Punktum dk tarafından farkındalık çalışmaları yapılmıştır. Bu çalışmalarda güvenli e-ticarete odaklanılmış ve nasıl yapılabileceğine ilişkin olarak kurumsal internet sitesinde bir sayfa yayınlanmıştır (Punktum dk, 2024b).

".dk" uzantıları alan adlarında DNSSEC teknolojisi kullanılmaktadır. Punktum dk kurumsal internet sitesinde yer alan bilgiye göre ".dk", 870 binden fazla DNSSEC imzalı alan adı ile Avrupa'da en çok DNSSEC imzalı ccTLD'dir. Punktum dk bu başarıda en büyük pay sahibi olarak internet servis sağlayıcılarını göstermiş ve diğer

ülkelerdekilerin aksine Danimarka'daki internet servis sağlayıcıların sorumluluk alarak DNSSEC teknolojisi ile uyumlu olmak için çalışmalar yürüttüğünü belirtmiştir (Punktum dk, 2023h).

Punktum dk, DNSSEC ile ilgili olarak bilgilendirme amaçlı bir sayfayı kurumsal internet sitesinde yayınlamıştır. Bu sayfada, DNSSEC'in ne olduğu, ne işe yaradığı ve nasıl yönetileceği hakkında kısaca bilgi verilmiştir (Punktum dk, 2024c).

4.5. Hollanda

Hollanda'nın ccTLD'si ".nl" dir ve kar amacı gütmeyen bir kuruluş olan SIDN tarafından yönetilmektedir (SIDN, 2023b). ".nl" uzantılı alan adları herkes tarafından tahsis edilebilmektedir (SIDN, 2023c). Alan adı tahsis işlemleri otomatik sistemler tarafından ilk gelen ilk alır kuralına göre yapılmaktadır. Kullanılan bu sistemler, alan adının tahsise uygun olup olmadığını ve başvuruda iletilen bilgilerin tamlığını ve doğruluğunu kontrol etmektedir (SIDN, 2023c). Başvuru sahibi, SIDN'e karşı olan yükümlülüklerini daha önce yerine getirmemişse başvurusu red edilebilmektedir (SIDN, 2023c, madde 1.5).

".nl Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar *(General Terms and Conditions for .nl Registrants)*" madde 21.1 madde kapsamında SIDN, DNS Abuse ve diğer kötüye kullanımlar ile mücadelede uygulanacak eylemler konusunda geniş bir yetkiye sahiptir. Bu yetki kapsamında SIDN, alan adını belirli bir süre veya kalıcı olarak bölge dosyasından kaldırabilir, iptal edebilir ve gerekli gördüğü diğer işlemleri yapabilir (SIDN, 2023c).

SIDN, DNS Abuse ile mücadelede farklı araçlar kullanmaktadır. Bunların çoğunluğu kendisi tarafından verilen hizmetler, uygulanan prosedürler ve kontrol mekanizmaları olmakla birlikte dış paydaşlar ile beraber yürüttüğü süreçler de bulunmaktadır. SIDN, DNS Abuse ile mücadelede ihbar ve kaldırma prosedürü ile alan adı kayıt bilgilerinin doğrulaması prosedürünü uygulamakta, ".nl Kontrol *(.nl Control)*, SIDN Marka

Koruması *(SIDN BrandGuard)* ve Sahte İnternet Mağazaları Tespiti" hizmetlerini sunmakta, RegCheck ile yeni tahsis edilen alan adlarının risk değerlendirmesini yapmakta ve Netcraft ile birlikte kötüye kullanılan alan adlarına ilişkin bir süreç işletmektedir. Ayrıca, ".nl Alan Adlarına İlişkin Şikayet ve İtiraz Kurulu *(Het College voor Klachten en Beroep voor .nl-domeinnamen - CvKB)*[12]" tarafından, ".nl" uzantılı alan adının ahlaka veya kamu düzenine aykırı olduğuna dair yapılan şikayetler karara bağlanmaktadır. Belirtilen araçlar aşağıda sırasıyla açıklanacaktır.

- **İhbar ve Kaldırma Prosedürü**

"İhbar ve Kaldırma Prosedürü *(Notice-and-Take-Down Procedure - NTD Procedure)*", internet sitelerindeki yasa dışı ve ceza gerektiren içeriklerle ilgili olarak yürütülen ve ilgili tarafların ne yapması gerektiğini belirten bir prosedürdür. DNS Abuse türleri dışında çocuk pornografisi, intihal, ayrımcılık ve yasa dışı veya çalıntı malların tedariki de prosedür kapsamında yer almaktadır. ".nl" uzantılı alan adları kapsamında SIDN ilgili taraflar arasında bulunmaktadır (SIDN, 2024c).

İhbar ve kaldırma prosedürü kapsamında başvuruda bulunacak kişilerin ilk olarak internet site içerik sağlayıcı ile iletişime geçmesi gerekmektedir. İçerik sağlayıcı, internet sitesine video yükleyen veya metin yayınlayan kişi olabilmektedir. Yapılan başvuruya binaen içerik sağlayıcıdan yanıt alınamadığı takdirde sırasıyla; internet site yöneticisine, alan adı sahibine, yer sağlayıcıya, kayıt kuruluşuna ve son olarak kayıt otoritesine başvuruda bulunulabilmektedir. ".nl" uzantılı alan adları özelinde SIDN, ilgili taraflara yapılan başvurulardan sonuç alınamaması durumunda başvuruda bulunabilecek son mercidir (SIDN, 2024c).

[12] ".nl" uzantılı alan adlarının ahlaka ve kamu düzenine aykırı olduğuna dair yapılan şikayetlerin incelemesinin yanı sıra, SIDN tarafından kayıt kuruluşları ve alan adı sahipleri için verilen kararlara ilişkin yapılan itirazlar da CvKB tarafından karara bağlanmaktadır. Daha fazla bilgi için bkz. (https://cvkb.nl/downloads/2SDwlMOdqSyHlzGQ3RqiTg/745fb920db130b66ab0d59db42197f1b/CvKB-regeling.pdf), (07.01.2024)

SIDN'e yapılacak başvurular özel bir form olan "İhbar ve Kaldırma Formu" ile yapılmakta ve başvuruya, daha önce iletişime geçilen taraflarla yapılan yazışma kopyalarının eklenmesi gerekmektedir. İlgili form ve ekler support@sidn.nl adresine iletilmektedir (SIDN, 2024a). SIDN, yapılan başvurularda hatalı olması halinde başvuru sahibinden başvuruyu düzeltmesini isteyebilmekte ve başvuruları uzmanlık alanına göre farklı kurumlara değerlendirmesi için yönlendirebilmektedir (SIDN, 2024ç).

Yapılan değerlendirme sonucu başvuruya konu alan adı durdurulabilmektedir. Alan adı durdurulmadan önce hizmet alınan kayıt kuruluşu ile iletişime geçilmekte, alan adı durdurulduktan sonra ise alan adı sahibi, başvuru sahibi ve kayıt kuruluşu bilgilendirilmektedir. SIDN, ihbar ve kaldırma prosedürü kapsamında alan adını durdurduktan sonra alan adını iptal de edebilmektedir. Başvurunun reddedilmesi halinde ise başvuru sahibi, başvurusunun neden reddedildiği konusunda bilgilendirilmektedir (SIDN, 2024ç; SIDN, 2023c).

SIDN, ihbar ve kaldırma prosedürü kapsamında hatalı olarak durdurulan veya iptal edilen alan adlarına dair oluşan her türlü zarar ve masrafın başvuru sahibinden talep edileceğini belirtmekte ve sorumluluğu başvuru sahibine yüklemektedir (SIDN, 2024ç).

- **Alan Adı Kayıt Bilgilerinin Doğrulanması**

SIDN, alan adı sahibinden kimliğini ve iletiği bilgilerin doğruluğunu kanıtlamasını isteyebilmektedir (SIDN, 2024d). SIDN bu yetkisini ".nl Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar'da yer alan 18. maddeye dayandırmaktadır:

> *"18. Usulsüzlüklerin önlenmesi için gereklilikler*
> *Kayıtla ilgili usulsüzlükleri mümkün olduğunca önlemeye çalışıyoruz ve bu amaçla ek yükümlülükler getirebiliriz. Bu tür yükümlülükleri uygulamaya koyduğumuzda www.sidn.nl adresinde yayınlanacaktır."* (SIDN, 2023c).

SIDN, alan adı kayıt bilgilerinin doğrulanmasına dair alan adı sahibine, alan adı idari irtibat kişisine, hizmet alınan kayıt kuruluşu irtibat kişisine ve biliniyorsa kayıt kuruluşu DNS Abuse ile mücadele irtibat kişisine mail göndermektedir. Gönderilen maile iki iş günü içerisinde cevap verilmezse mail tekrar iletilmektedir. Üç iş günü içerisinde bilgilerin alan adı sahibi tarafından kanıtlanamaması halinde ise alan adı durdurulmaktadır (SIDN, 2024d).

Alan adının durdurulmasından sonra alan adı sahibi ve kayıt kuruluşuna; alan adının durdurulduğu ve .nl Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar 16. madde gereğince iptal edileceği, bilgisini içeren bir mail iletilmektedir. Bu mailde ayrıca, alan adının tekrardan kullanılması ve/veya iptal işleminin engellenebilmesi için alan adı sahibi veya kayıt kuruluşunun neler yapabileceği de ifade edilmektedir (SIDN, 2024d).

SIDN, ".nl" Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar madde 1.2 gereğince; 1 Ekim 2023 tarihinden itibaren kişinin, üçüncü bir kişi adına alan adı tahsis etmesine izin verilmeyeceğini belirtmiştir (SIDN, 2024d).

SIDN'in alan adı kayıt verilerinin doğrulanmasını istediği kişinin, üçüncü bir kişi için alan adı tahsis ettiği anlaşılırsa, alan adı sahibi ve kayıt kuruluşuna elektronik posta iletilmektedir. Bu e-postada, üçüncü kişinin kanıtlarıyla birlikte açıklanması ve alan adı bilgilerinin üçüncü kişi bilgileri ile değiştirilmesi gerektiği belirtilmektedir (SIDN, 2024d).

Eğer, üç iş günü içerisinde üçüncü kişi bilgisi kanıtlarıyla birlikte açıklanmaz veya alan adı bilgileri güncellenmez ise alan adı durdurulmaktadır. Bu süreçte alan adı sahibi bilgilerinin kanıtlanamamasından farklı olarak alan adı iptal edilmemektedir (SIDN, 2024d).

- **“.nl” Kontrol**

SIDN, alan adı kilidi hizmeti kapsamında “.nl Kontrol *(.nl Control)*” hizmetini sunmaktadır. Bu hizmet, alan adı bilgilerinin izinsiz olarak değiştirilmesi, alan adının transferi ve alan adından feragat edilmesi gibi işlemlere karşı koruma sağlamak amacıyla sunulmaktadır. “.nl” kontrol hizmeti kayıt kuruluşları aracılığıyla alınmaktadır. SIDN, hizmet fiyatının kayıt kuruluşları tarafından belirlendiğini belirtmiştir (SIDN, 2024a; SIDN, 2024e).

“.nl” kontrol hizmeti alınan bir alan adı için yukarıda belirtilen işlemlerden birisi yapılmak istendiğinde alan adı sahibi aranmakta ve işleme onay vermesi istenmektedir. Onay verilmesi halinde işlem gerçekleştirilmektedir (SIDN, 2024a).

- **SIDN Marka Koruma**

Saldırganlar, çok bilinen internet sitelerinin kasıtlı olarak yanlış yazılmış hallerini içeren alan adlarını tahsis etmekte ve bu alan adları üzerinden kötü amaçlı faaliyetler yürütebilmektedir. SIDN marka koruma, kasıtlı yanlış yazılmış alan adları ile internetteki marka ihlallerini tespit eden ve buna karşı yasal yollara başvurma fırsatı sunan bir koruma hizmetidir. Bu hizmet sayesinde kişiler, sahip olduklarına çok benzeyen alan adları ile marka logolarının bulunduğu alan adlarını takip edebilmektedir (SIDN, 2024f).

SIDN marka koruma hizmetinde, tespit edilen alan adları hakkında isteğe bağlı olarak yasal işlemler hakkında bilgi alma ve işlem başlatabilme imkânı da sunulmaktadır. Bu kapsamda destek almak isteyen kişiler ICTRecht[13] üzerinden hizmet almaktadır. Yasal takip hizmetinin iki çeşidi bulunmaktadır:

[13] Bilgi ve iletişim teknolojileri, internet ve telekomünikasyon gibi alanlarda hukuki danışmanlık yapan kuruluştur. Daha fazla bilgi için bkz.(https://www.ictrecht.nl/en/legal-advice), (02.02.2024)

1. Hızlı taramalar[14], tavsiyeler ve sınırlı destek için temel modül;
2. İhbar ve kaldırma prosedürü dahil prosedürleri içeren ve ücreti daha yüksek olan kapsamlı modül (SIDN, 2024g).

SIDN marka koruma hizmeti alan kişiler, sahip olduklarına çok benzer olan ".nl" uzantılı alan adlarında tahsis edilmeden önce, ".com ve .org" gibi TLD uzantılı alan adlarında ise tahsisten sonraki yirmi dört saat içinde bilgilendirilmektedir. Logolara ilişkin kontrol ise sadece ".nl" uzantılı alan adları için gerçekleştirilmekte ve bilgilendirme aylık olarak yapılmaktadır. Hizmet alan kişiler, kişisel kontrol panelleri üzerinden yapılan incelemeleri görebilmekte, yasal takip hizmeti alabilmekte ve davalarını kolayca takip edebilmektedir. Ayrıca, elektronik postayla da bilgilendirme yapılmaktadır (SIDN, 2024f).

- **Sahte İnternet Mağazaları Tespiti**

Hollanda pazarına odaklanan bir çalışmada; yaklaşık doksan bin internet mağazasından tahmini yirmi beş bin ile otuz beş bin arasındaki mağazanın güvenilmez olduğu ifade edilmiştir (SIDN, 2019).

Sahte internet mağazalarının tespiti, SIDN tarafından geliştirilen ve makine öğrenmesinin kullanıldığı bir yazılım tarafından yapılmaktadır. Yapılan incelemelerde alan adının içeriği ile birlikte alan adı kayıt bilgileri de kontrol edilmektedir. Örneğin, bir alan adının diğer alan adlarıyla aynı anda kaydedilip kaydedilmediği, alan adının daha önce kaydedilip kaydedilmediği ve belirli anahtar kelimelerin kullanılıp kullanılmadığı kontrol edilmektedir. Ayrıca, bu alan adlarının çoğunun genellikle birkaç dakika gibi kısa bir sürede kaydedildiği gözlenmiştir. Bu durum şüphe uyandıran hallerden bir başkasıdır (SIDN, 2019).

[14] Hizmet alan kişinin talebi üzerine, tespit edilen alan adına dair hangi işlemlerin yapılabileceği ve alan adının kendisine devredilmesi ihtimalinin ne kadar olduğu gibi sorulara ilişkin bilgilendirmenin yapıldığı hizmettir.

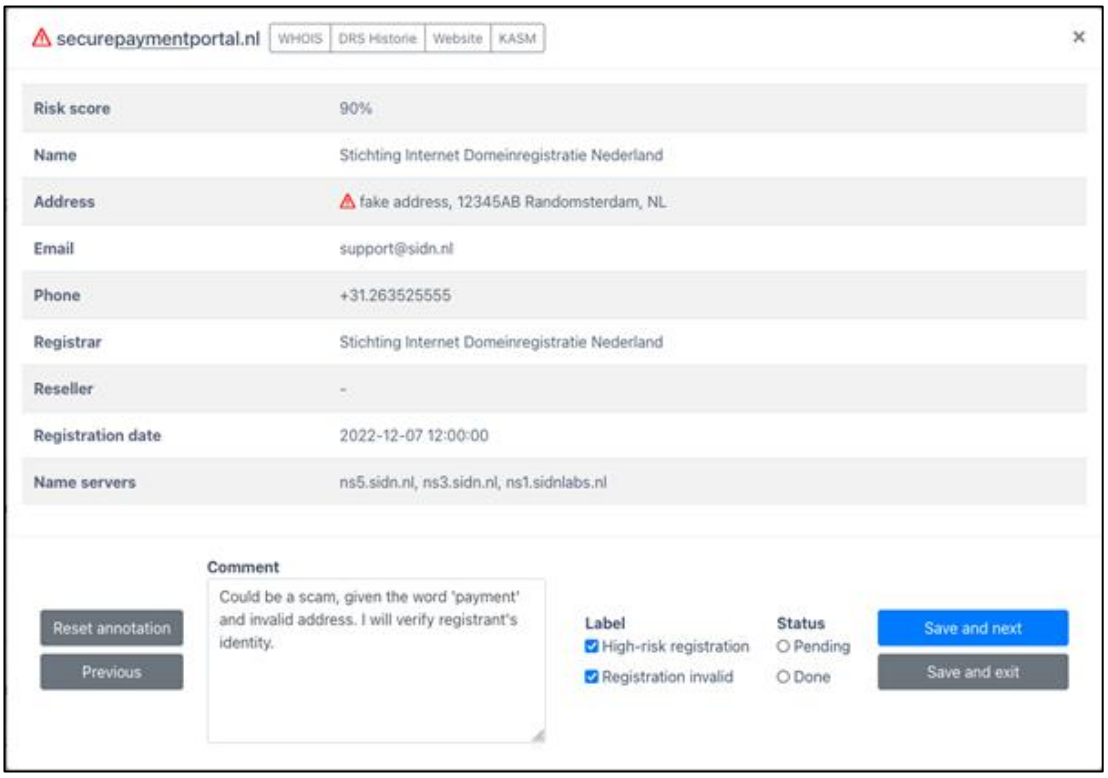
Yazılım tarafından tespit edilen alan adları daha sonra “SIDN Kayıt ve Servis (*Registration and Service Department*)” bölümüne gönderilerek kontrol edilmektedir. Kontrol sonrası yasal internet mağazalarına ilişkin alan adları listeden çıkarılmaktadır. Yapılan incelemeler sonucunda alan adının sahte internet mağazası için kullanıldığına dair şüphe olduğu durumda, alan adı sahibinden kimlik bilgilerinin beş gün içerisine kanıtlaması istenmektedir. Bu süre zarfında kimlik bilgisi kanıtlanmaz ise alan adı yetkili ad sunucu bilgileri TLD sunucusundan kaldırılmakta ve alan adı erişilemez hale gelmektedir (SIDN, 2019).

- **RegCheck**

RegCheck, SIDN tarafından geliştirilen ve makine öğrenmesinin kullanıldığı bir sistemdir. Bu sistem, alan adı tahsis esnasında yüksek risk içeren “.nl” uzantılı alan adlarını tespit etmek için geliştirilmiştir. RegCheck, tahsis esnasında internet sitesindeki bilgiler henüz mevcut olmadığı için, tahsis edilen alan adı ve alan adı sahibinin elektronik posta adresi gibi tahsis sırasında mevcut olan verilere dayanarak bir risk puanı oluşturmaktadır (SIDN, 2023a).

Belirli bir eşiğin üzerinde risk puanına sahip alan adları, SIDN analistleri tarafından incelenmesi için kontrol paneline aktarılmaktadır. Analistler bu kayıtları düzenli olarak incelemekte ve bunların gerçekten bir risk oluşturup oluşturmadığına karar vermektedir. Risk oluşturduğu karar verilen alan adlarının sahiplerinden kimlik bilgilerini kanıtlaması istenmektedir (SIDN, 2023a). Bu kapsamda başlatılan alan adı kayıt bilgilerinin doğrulanması prosedürü çerçevesine üç iş günü içerisinde alan adı sahibi kimlik bilgileri kanıtlanamaz ise alan adı erişilemez hale getirilmektedir (SIDN, 2023a; SIDN, 2024d).

Şekil 4.1. Kontrol Paneli Ekran Görüntüsü[15]



Kaynak: SIDN, 2023

- **Alan Adı Kötüye Kullanım Kontrolü**

".nl" uzantılı alan adları kapsamındaki "Alan Adı Kötüye Kullanım Kontrolü" süreci, SIDN ile Netcraft'ın birlikte yürüttüğü bir süreçtir. Bu süreçte, kötüye kullanıldığı düşünülen alan adlarının tespiti Netcraft tarafından yapılmakta, alan adının durdurulması ve kötüye kullanım tespitinin farklı kaynaklardan kontrolü SIDN tarafından gerçekleştirilmektedir. Netcraft, DNS Abuse türleri dışında farklı kötüye kullanım türleri için de inceleme yapmaktadır (SIDN, 2024b). DNS Abuse dışında incelemesi yapılan türler ve açıklamaları aşağıda yer almaktadır:

[15] RegCheck'in tespit ettiği risk faktörlerinin kırmızı ünlem işaretiyle işaretlendiği veya altının çizildiği ve bu sayede puanın yorumlanabilir olmasının sağlandığı SIDN tarafından belirtilmiştir.

- **Sahte internet mağazalar:** Ürünlerin düşük fiyatla satışa sunulduğu ancak ürünün satın alınmasından sonra ürünün gönderilmediği, taklit ürünün gönderildiği veya alakasız bir ürünün gönderildiği mağazalardır. Sahte internet mağazalarında kişinin banka giriş bilgileri ile kredi kartı bilgileri gibi bilgileri de ele geçirilebilmektedir.
- **Çevrimiçi kredi kartı hırsızlığı:** Alışveriş sitesi ödeme sayfasına girilen kredi kartı bilgilerinin saldırganlara aktarılmasıdır. Bu işlem virüslü ödeme sayfası aracılığıyla yapılmaktadır.
- **Tahrif edilmiş internet sitesi:** Meşru bir internet sayfasının saldırganlar tarafından değiştirilmesidir. Değiştirilen sayfa genellikle siyasi materyal içermektedir. Yapılan işlem de bir tür kötü amaçlı yazılımdır. Tahrif edilen internet siteleri genellikle zayıf güvenliğe sahiptir ve bu nedenle daha fazla suç istismarına açık olmaktadır.
- **Kripto para yatırım dolandırıcılığı**: Kişilere kripto para getiri vaatlerinin verildiği ancak verilen vaatlerin yerine getirilmediği internet siteleridir. Bu sitelerde kişilere, yatırım yapmaya devam edildiği sürece garantili getiri vaat edilmekte ancak vaat edilen tutarlar hiçbir zaman ödenmemektedir. Ayrıca, kişilerin gizli bilgileri de ele geçirilmektedir.
- **Kargo dolandırıcılığı:** Kişilere sahte bir mesaj atılarak yapılan dolandırıcılıktır. Bu mesajda bir kargo firmasından bir paket gönderildiği belirtilmekte ve kişilerden hassas bilgilerini girmesi istenmektedir.
- **Anket dolandırıcılığı:** Birçok anket dolandırıcılığının amacı, tüketicilerin kişisel verilerinin satış veya kimlik hırsızlığı amacıyla ele geçirilmesidir.
- **Kripto madencisi:** Kripto para madenciliği yapmak için kötü amaçlı JavaScript[16] kullanımını içermektedir. Bu, kişinin bilgisayar veya cep telefonu gücünün kötüye kullanılmasıdır.

[16] İnternet sitesi geliştirme, mobil uygulamalar, oyunlar ve ağ uygulamaları için kullanılan komut dosyası programlama dillerinden biridir. JavaScript, bir internet sayfasının temel içeriğini etkileşimli yapmaktadır. Statik metinden daha fazlası olan bir internet sitesi her kullandığında, JavaScript koduyla etkileşime girilmektedir. Daha fazla bilgi için bkz. (https://bulutistan.com/blog/javascript-nedir/), (04.01.2024)

- **Web Kabuğu:** Web kabuğu, genellikle siber saldırı amacıyla bir web sunucusuna uzaktan erişmeyi mümkün kılmaktadır (SIDN, 2024b).

Netcraft, ".nl" uzantılı bir alan adının kötüye kullanıldığını tespit ettikten sonra, alan adı kaydı ile bağlantılı herkese durumu bildiren bir elektronik posta göndermektedir. Bu elektronik postanın gönderilmesinden sonraki altmış altı saatlik süre zarfında, on sekiz saatlik aralıklarla elektronik posta tekrar gönderilmektedir. SIDN ise, alan adı sahibine, yer sağlayıcıya ve hizmet alınan kayıt kuruluşuna konu hakkında elektronik posta gönderilmektedir (SIDN, 2024b).

SIDN, alan adı kötüye kullanım kontrolü kapsamında elektronik posta gönderilen alan adı sahiplerine; internet sitesini yöneten kişi veya firma ile virüslü dosyaların kaldırılması için iletişime geçmelerini, Google'ın ilgili dokümanlarını incelemelerini, tüm şifrelerini değiştirmelerini ve kullanılan "İçerik Yönetim Sistemi *(Content Management System - CMS)"*[17]nin güncelliğini kontrol etmelerini tavsiye etmektedir (SIDN, 2024b).

Netcraft tarafından alan adı sahibine elektronik posta iletilmesinden altmış altı saat sonra, SIDN başka bir kaynak aracılığıyla alan adı kötüye kullanımının devam edip etmediğini kontrol etmektedir. İlgili kişilere gönderilen elektronik postalara yanıt gelmemesi ve başka bir kaynaktan yapılan kontrol sonucu kötüye kullanımın devam ettiğinin anlaşılması durumunda alan adı durdurulmaktadır. Durdurma işlemi, kayıt kuruluşu ve alan adı idari irtibat kişisine elektronik posta ile bildirilmektedir. SIDN, yapılan işlemin orantısız bir olumsuz etkiye sahip olup olmadığını değerlendirdiğini ve bu değerlendirmenin karar alma sürecinde dikkate alındığını belirtmektedir (SIDN, 2024b).

---

[17] Bir internet sitesinde ziyaretçi tarafından görüntülenebilen içeriklerin, dosyaların ve tasarımların kontrol edilmesini sağlayan bir tür bilgisayar yazılımıdır. Genellikle yönetici paneli olarak adlandırılan bir menü üzerinden kullanılmaktadır. Daha fazla bilgi için bkz. (https://www.ideasoft.com.tr/cms-icerik-yonetim-sistemi-nedir/), (04.01.2024)

Alan adı sahipleri, yapılan işlemin haksız olduğunu düşünmesi durumunda veya konu hakkında daha fazla destek alabilmek için takedown@netcraft.com adresi ile iletişime geçebilmektedir (SIDN, 2024b).

- **Alan Adı Kontrolü**

Alan adı kontrolü, SIDN tarafından üç yıllık süre için atanan ve en az beş üyeden oluşan ".nl Alan Adlarına İlişkin Şikayet ve İtiraz Kurulu (*Het College voor Klachten en Beroep voor .nl-domeinnamen - CvKB*)" tarafından yapılmaktadır. Kurul Başkanı, üyeler tarafından seçilmektedir. Seçilen üyeler üç yıllık süre için tekrar seçilebilmektedir (SIDN, 2023ç).

".nl" Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar madde 19.6 gereğince kişiler, ".nl" uzantılı bir alan adının ahlaka veya kamu düzenine aykırı olduğunu düşünüyorsa kurula şikayette bulunabilmektedir (SIDN, 2023c). Şikayet başvurusunun ücreti 50€'dur. Şikayetin kurul tarafından değerlendirme yapılmadan önce geri çekilmesi durumunda 25€ geri alınabilmektedir. Şikayetin haklı bulunması halinde ise, başvuru ücretinin tamamı on dört gün içerisinde geri ödenmektedir (SIDN, 2023ç).

".nl" Uzantılı Alan Adı Sahibi İçin Genel Hüküm ve Koşullar madde 20.1 gereğince, Kurul tarafından davaya konu olduğu SIDN'e bildirilen alan adı dondurulmaktadır. Dondurulan alan adları başkasına devredilememekte ve alan adından feragat edilememektedir. Ancak, dondurulma süresi boyunca alan adı başka bir kayıt kuruluşuna transfer edilebilir veya alan adının yetkili ad sunucu bilgileri değiştirilebilir (SIDN, 2023c).

Yapılan şikayetler için kurul tarafından duruşma yapılmaktadır. Duruşma tarihinin belirlenmesinden sonra alan adı sahibi ve şikayetçi taraf en kısa sürede bilgilendirilmektedir. Taraflar kendilerinin üçüncü bir kişi tarafından temsil edilmesini istiyorlarsa bunu duruşma tarihinden en az on dört gün önce kurula bildirmelidir.

Duruşmalar halka açık olarak yapılmakta ancak taraflardan birinin talebi ve kurulun uygun bulması üzerine gizli duruşmada da yapılabilmektedir. Kararın verilebilmesi için en az üç kurul üyesinin duruşmada bulunması gerekmektedir (SIDN, 2023ç).

Kurulun verdiği karar, taraflara yazılı olarak ve elektronik posta yoluyla gönderilmektedir. Kurulun şikayeti haklı bulması halinde SIDN, kararın kendisine ulaşması üzerine alan adını geçici olarak durdurmaktadır. Ayrıca, bu alan adları geçici bir süre tahsise kapatılabilmektedir. Şikayetin kurul tarafından haksız bulunması halinde ise alan adına dair bir işlem yapılmamaktadır (SIDN, 2023ç).

Kurulun kararı, SIDN üzerinde bağlayıcı bir etkiye sahiptir. Şikayet eden ve alan adı sahibi için, karar altı hafta içinde yetkili bir Hollanda mahkemesine taşınmazsa karar onlar için de bağlayıcı hale gelmektedir. Bu süre, kararın taraflara gönderildiği gün başlamaktadır (SIDN, 2023ç).

SIDN, ".nl" uzantılı bir alan adı için ahlaka veya kamu düzenine aykırı olarak yapılan şikayetin nadiren haklı bulunduğunu belirtmektedir (SIDN, 2024ğ).

- **Farkındalık Çalışmaları**

SIDN, kişileri bilgilendirmek ve farkındalık oluşturmak için internetin kötüye kullanımı başlıklı bir sayfa yayınlamıştır. Bu sayfada kimlik avı/oltalama, köle bilgisayar ağları gibi saldırılar açıklanmış ve yapılabilecekler hakkında önerilerde bulunulmuştur (SIDN, 2024h).

- **DNSSEC**

".nl" uzantılı alan adlarında DNSSEC teknolojisi kullanılmaktadır. SIDN, kurumsal internet sitesinde DNSSEC ile ilgili ayrıntılı bilgilerin yer aldığı bir sayfa yayınlamıştır. Bu sayfada, ana metnin dışında sıkça sorulan sorular formatında bölümler yer almaktadır. Bu bölümlerde; genel bilgiler, şifreleme algoritmaları,

DNSSEC uygulaması, Hollanda'daki durum gibi birçok başlıkta çok sayıda soruya cevap verilmiştir (SIDN, 2024ı).

4.6. İngiltere

İngiltere'nin ccTLD'si ".uk"dir ve kamu yararına çalışan bir şirket olan Nominet tarafından yönetilmektedir (Nominet, 2023c). Nominet, ".uk" uzantılı alan adlarının tahsisi ve kullanımına ilişkin olarak "Kurallar *(Rules)*"'u yayınlamıştır. Buna göre; alan adları ilk gelen ilk alır kuralına göre tahsis edilmekte ancak alt alan adlarına (örn. co, ltd, me, sch vb.) göre farklı tahsis kuralları da işletilmektedir. Örneğin, .uk, co.uk ve org.uk altında tahsis edilmek istenen alan adları[18] herhangi bir incelemeden geçmeden doğrudan tahsis edilebilmekteyken, diğer alt alan adları altında tahsisin gerçekleşebilmesi için Kurallar'da belirtilen şartların sağlanması gerekmektedir (Nominet, 2018, s.2-7).

".uk" uzantılı alan adlarının iptal edilmesi veya özel statüye[19] alınmasına dair hükümler "Alan Adı Kaydı Hüküm ve Koşullar (*Terms And Conditions Of Domain Name Registration)"'*da yer almaktadır. Bu hüküm ve koşullarda DNS Abuse ifadesi doğrudan değil, türleri ve etkileri itibariyle yer almakta ve alan adının iptal edilmesi veya özel statüye alınması kapsamına dahil edilmektedir (Nominet, 2020, s.7):

> *"10.1 Aşağıdaki durumlarda size bildirimde bulunarak bir alan adını iptal edebilir veya özel bir statüye alabiliriz:*
>
> ...
>
> *10.1.2 Tamamen kendi takdirimize bağlı olarak alan adının, alan adı sisteminin herhangi bir bölümünü, diğer internet kullanıcılarını (virüs ve kötü*

[18] Mart 2024 verilerine göre .uk, co.uk ve org.uk altındaki aktif alan adları tüm .uk uzantılı alan adlarının %99'unu oluşturmaktadır. Daha fazla bilgi için bkz. https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2024/), (15.05.2024)

[19] "Alan Adı Kaydı Hüküm ve Koşullar"da özel statünün; alan adının durdurulması, uyuşmazlık politikası veya hukuki ihtilaf sebebiyle alan adı transfer veya feragat işleminin engellenmesi, alan adının bilgi/yardım sayfasına yönlendirilmesi gibi çeşitli durumları içerebileceği ifade edilmiştir.

amaçlı yazılım yayımı, kimlik avı/oltalama faaliyeti veya dağıtılmış hizmet reddi saldırılarının kolaylaştırılması dahil ancak bunlarla sınırlı olmamak üzere) veya sistemlerimizi ve internet bağlantılarımızı tehlikeye atacak şekilde kullanıldığını veya kullanılma riskinin yüksek olduğunu düşündüğümüz durumda,

…"

Nominet, DNS Abuse ile mücadeleyi sadece kendi yetkisi altında değil, aynı zamanda kayıt kuruluşları ve kolluk kuvvetleri gibi çeşitli kurumların da katılımını içeren bir yapı üzerinden yürütmektedir. Bu yapıda Nominet, kayıt kuruluşlarına alan adı durdurma ve iptal yetkisi vermekte, Britanya kolluk kuvvetlerinden kendisine gelen resmi bildirimlere binaen de alan adını özel statüye almaktadır (Nominet, 2021, s.4; Nominet, 2023ç; Nominet, 2023e; Nominet, 2023g)

Nominet, DNS Abuse ile mücadele için "Alan Adı Sağlığı *(Domain Health)*, Alan Adı İzleme *(Domain Watch)*, Alan Adı Kilidi *(Domain Lock)* ve Soruşturma Kilidi *(Investigation Lock)*" yöntemlerini geliştirmiş ve alan adının suç faaliyetinde kullanılması kapsamında Britanya kolluk kuvvetleri ile ilişkisini düzenleyen "Ceza Uygulamaları Politikası *(Criminal Practices Policy)*"'nı geliştirmiştir (Nominet, 2021; Nominet, 2023ç; Nominet, 2023b; Nominet, 2023a; Nominet, 2023g). Belirtilen yöntem ve prosedürler aşağıda sırasıyla açıklanacaktır.

- **Alan Adı Sağlığı**

Alan Adı Sağlığı *(Domain Health)*, ".uk" uzantılı alan adı işlemlerini yürüten tüm kayıt kuruluşlarının hizmet verdikleri alan adları kapsamında; istenmeyen elektronik posta, kimlik avı/oltalama, kötü amaçlı yazılım ve köle bilgisayar ağlarına karışanlar hakkında bilgi sahibi olmasını ve bu sorunları çözmek için neler yapabilecekleri konusunda tavsiyeler alabilmesine olanak sağlayan bir hizmettir. Nominet tarafından ücretsiz olarak sunulan bu hizmetin kayıt kuruluşları tarafından alınması zorunlu değildir (Nominet, 2023ç).

Nominet, alan adı sağlığı verilerinin DNS Abuse ile ilgili farklı kaynaklardan edinilen bilgilerle oluştuğunu belirtmiş ancak saldırganların yararlanmaması için bu kaynakları açıklamayacağını ifade etmiştir. Bununla birlikte, belirli bir kötüye kullanım raporunun kaynağının talep edilmesi durumunda şeffaflık adına gösterilebileceği de ifade edilmiştir (Nominet, 2023ç).

Alan adı sağlığında her bir etikete[20] yani kayıt kuruluşuna, DNS Abuse ile ilişkilendirilen alan adlarının seviyelerini ölçmek ve izlemek için birden ona kadar puan verilmektedir. DNS Abuse'un olmadığı durumda kayıt kuruluşu on puan almaktadır. Nominet, puanın bir etiket üzerindeki "kötü" alan adlarının oranı kullanılarak hesaplandığını ve tüm DNS Abuse verilerinin puan hesaplaması için kullanılmadığını belirtmiştir. Kullanılan verilerin, önemli kategorilerde yüksek istismar olasılığını gösteren alan adları dikkate alınarak oluşturulduğu ayrıca ifade edilmiştir (Nominet, 2023ç).

Alan adı sağlığında kayıt kuruluşları benzer büyüklükteki diğer kayıt kuruluşları ile karşılaştırılmakta ve DNS Abuse düzeyine göre sıralanmaktadır. Kayıt kuruluşları yalnızca kendi puanlarını ve sıralamalarını görebilmekte, diğer kayıt kuruluşlarının puan ve sıralamalarını görememektedir (Nominet, 2023ç).

Kayıt kuruluşları, alan adı sağlığında bulunan alan adlarını Nominet kurumsal internet sitesi çevrimiçi hizmetler bölümünden görüntüleyebilmekte ve csv dosya[21] formatında indirebilmektedir. Çevrimiçi hizmetler bölümdeki veriler on günlük süre baz alınarak oluşturulmakta ve günlük olarak güncellenmektedir. Ayrıca bu bölümde arama olanakları da mevcuttur (Nominet, 2023ç).

---

[20] Etiket *(tag),* kayıt kuruluşlarının ".uk" uzantılı alan adlarını tahsis edebilmesi veya yönetebilmesi için kendilerine verilen bir kayıt sistemi tanımlayıcısıdır. Daha fazla bilgi için bkz. (https://nominet.uk/wp-content/uploads/2020/12/UK-Registry-Registrar-Agreement-26-11-2021-1.pdf), (02.12.2023)

[21] Verilerin tablo yapısında kaydedilmesine olanak tanıyan özel bir biçimle kaydedilmiş metin dosyalarıdır.

Kayıt kuruluşları çevrimiçi hizmetlerin yanı sıra günlük elektronik posta, "Alan Adı Sağlığı Rest API" ve grafiksel raporlama aracılığıyla da alan adı sağlığı tarafından tespit edilen alan adlarına dair bilgi edinebilmektedir. Günlük elektronik postada, kötü amaçlı yazılım ve kimlik avı/oltalama gibi kötüye kullanımla ilişkili tüm alan adları hakkında elektronik posta yoluyla ve csv formatındaki dosya ile bilgilendirilme yapılmaktadır (Nominet, 2023ç).

Alan Adı Sağlığı Rest API, kayıt kuruluşunun ilgili API'ye entegre olması sonucu alan adı sağlığı ile ilgili tüm bilgileri otomatik olarak çekmesine olanak sağlayan sistemdir. Kayıt kuruluşları bu sistem sayesinde alan adı sağlığında olan alan adlarıyla ilgili olarak aşağıdaki işlemleri yapabilmektedir:

- Kötüye kullanım ile ilişkili tüm alan adlarını getir
- Kötüye kullanım ile ilişkili alan adını getir
- Kötüye kullanım ile ilişkili alan adlarını tek bir etiketten getir
- Kötüye kullanım kategorisine göre alan adlarını getir (Nominet, 2023ç, Nominet, 2023d).

Son olarak, kayıt kuruluşları grafiksel raporlama sayesinde alan adı sağlığı verilerini görselleştiren, etiketini, etiket sıralamasını ve kötüye kullanım kategorilerini ayrıntılandıran yararlı grafiklere ulaşabilmektedir (Nominet, 2023ç).

Nominet, Alan Adı Sağlığı hizmeti kapsamında kayıt kuruluşları ile paylaştığı alan adlarına karşı hangi önlemler alınabileceğine dair tavsiye niteliğinde olan aşağıdaki bilgileri paylaşmıştır:

Tablo 4.3. DNS Abuse Azaltma Önerileri

DNS Abuse Türleri	**Tanım**	**Etki Azaltma Önerileri**
Komuta Kontrol (K&K)	Alan adının, köle bilgisayar ağları için kontrol merkezi görevinde olmasıdır.	Alan adının K&K olma amacıyla kaydedilmiş olması muhtemeldir. Sorunu çözmek için mümkün olan en kısa sürede daha ayrıntılı araştırma yapılması önerilmektedir. Yapılan araştırmanın ardından alan adını durdurmanız gerekebilir.
Alan Adı Ele Geçirilme	Alan adının kötü niyetli kişiler tarafından ele geçirilmesidir. Ele geçirilen alan adları bu kişilerin kontrolü altındadır.	Saldırının nasıl gerçekleştiğinin araştırılması ve bu alan adından beklenmeyen içeriğin kaldırılması önerilmektedir. Tüm şifreleri değiştirmeniz ve bilgisayarınızdaki tüm yazılımları güncellemeniz önerilmektedir. Alan adının içeriğini barındırmıyorsanız, kaydedeni bilgilendirmeniz ve yukarıdaki tavsiyeyi sunmanız önerilmektedir.
Alan Adı Oluşturma Algoritması *(Domain Generating Algorithm - DGA)*	Alan adının, genellikle kötü amaçlı yazılımlarda veya köle bilgisayar ağlarında kullanılan bir DGA ile ilişkilendirilmesidir.	Alan adı bir köle bilgisayar ağın parçası olmak amacıyla veya kötü amaçlı yazılım olarak kaydedilmiş olabilir. Alan adını durdurmanın gerekip gerekmediğine karar vermeden önce daha fazla araştırma yapmanız önerilmektedir. Güvenlik uzmanlarının bazen analiz yapmak için DGA alan adı kaydettiğinin unutulmaması gerekmektedir.

Tablo 4.1. DNS Abuse Azaltma Önerileri

Kötü Amaçlı Yazılım	Kötü amaçlı yazılımların alan adları aracılığıyla bilgisayarlara yüklenmesidir. Kötü amaçlı yazılım; bilgisayarları bozmak, hassas bilgileri toplamak veya özel bilgisayar sistemlerine erişim sağlamak için kullanılan yazılımdır. Virüsler ve truva atları yaygın örneklerdir.	Alan adının ele geçirilip geçirilmediğini araştırılması, etkilenen dosyaların/hesapların temizlenmesi, tüm şifrelerin değiştirilmesi ve sunucudaki yazılımların güncellenmesi tavsiye edilmektedir. Alan adının içeriğini barındırmıyorsanız, kaydedeni bilgilendirmeniz ve yukarıdaki tavsiyeleri sunmanız önerilmektedir.
Kimlik Avı/Oltalama	Kimlik avı/oltalama, saldırganların asıl alan adı içeriğine benzer bir içerikte alan adını kullanarak kullanıcı adlarını, şifreleri, banka bilgilerini vb. ele geçirmesidir. Alan adı üzerinden doğrudan kimlik avı/oltalama elektronik postaları gönderebileceği gibi farklı kimlik avı/oltalama elektronik postaları içerisinde de yer alınabilmektedir.	Alan adından beklenmeyen içeriği kaldırmanız ve bu alan adında toplu elektronik posta pazarlaması için en iyi uygulamaları kullanmanız önerilmektedir. Alan adının içeriğini barındırmıyorsanız, kaydedeni bilgilendirmeniz ve yukarıdaki tavsiyeyi sunmanız önerilmektedir.
İstenmeyen Elektronik Posta	Alan adı üzerinden istenmeyen elektronik posta gönderilmesi veya istenmeyen elektronik posta yoluyla alan adı bilgisi paylaşılmasıdır.	Alan adından beklenmeyen içeriği kaldırmanız ve bu alan adında toplu elektronik posta pazarlaması için en iyi uygulamaları kullanmanız önerilmektedir. Alan adının içeriğini barındırmıyorsanız, kaydedeni bilgilendirmeniz ve yukarıdaki tavsiyeyi sunmanız önerilmektedir.

Kaynak: Nominet, 2023

- **Alan Adı İzleme**

Nominet tarafından alan adı sağlığı hizmetinin sunulmasından sonra yapılan incelemelerde, DNS Abuse kapsamındaki faaliyetlerin büyük bir kısmının kimlik avı/oltalama olduğu görülmüştür. Nominet, ".uk"'nin güvenilirliğini artırmak ve son kullanıcılarının kötü niyetli faaliyetlerden korumak adına Alan Adı İzleme *(Domain Watch)* programını geliştirmiştir. Program, kimlik avı/oltalama amacıyla tahsis edilen alan adlarını hızlı bir şekilde tespit etmek ve durdurmak üzere geliştirilmiştir. Nominet, alan adı izleme sisteminin teknik algoritmalar ve manuel müdahalelerin birleşimi olarak çalıştığını belirtmiş ancak saldırganların verilecek bilgilerden yararlanmaması adına ayrıntı vermeyeceğini ifade etmiştir (Nominet, 2023b; Nominet, 2023e).

Alan adı izleme tarafından, kimlik avı/oltalama amacıyla tahsis edildiği düşünülen alan adları tespit edildikten kısa bir süre sonra durdurulmakta ve durdurulma bilgisi hizmet alınan kayıt kuruluşuna ve alan adı sahibine iletilmektedir. Kayıt kuruluşları bu bilgiyi Extensible Provisioning Protocol (EPP) ve/veya elektronik posta yoluyla alırken, alan adı sahipleri durdurma bilgisi ile birlikte yapılan işlemin yanlış olduğunu düşünmesi halinde yapması gereken işlemleri içeren bir elektronik posta almaktadır. Durdurulan alan adları hakkında alan adı sahibi veya kayıt kuruluşu tarafından yapılan, alan adının meşru kullanımına dair açıklamaların Nominet tarafından uygun bulunması halinde durdurma işlemi geri alınabilmektedir[22] (Nominet, 2023b; Nominet, 2023e).

Alan adı izleme programı ile alan adı sağlığı hizmeti birbirinden farklı süreçleri içermektedir. Alan adı sağlığı hizmetinde; DNS Abuse kapsamındaki veriler kayıt

[22] Alan adı izleme hakkında bilgi verilen Nominet internet sayfasında; sadece alan adı sahibi tarafından yapılan açıklamanın uygun bulunması sonucu işlemin geri alınacağı belirtilirken, alan adı izleme kapsamındaki sıkça sorulan sorular sayfasında yer alan dokuzuncu sorunun cevabında; kayıt kuruluşu tarafından da açıklama yapılabileceği ifade edilmiştir.

kuruluşlarına iletilip kayıt kuruluşu tarafından işlem yapılması beklenirken, alan adı izleme programında Nominet doğrudan işlem yapmaktadır (Nominet, 2023e).

- **Alan Adı Kilidi**

Nominet, alan adı kilidi kapsamında ".uk" uzantılı alan adı hizmeti sunan kayıt kuruluşlarına "Alan Adı Kilidi *(Domain Lock)"* hizmeti sunmakta, ".uk" uzantılı alan adı sahibi olan herkes de bu hizmetten yararlanabilmektedir. Bu hizmetle; alan adı yetkili ad sunucu bilgisi, sahiplik bilgisi, adres ve iletişim bilgisi yetkisiz olarak değiştirilememekte, alan adının başka bir kayıt kuruluşuna yetkisiz transferi engellenmektedir. Kilitli bir alan adı, iki faktörlü kimlik doğrulama yoluyla önceden yetkilendirilmiş bir temsilci tarafından kilitlenip açılabilmektedir. Alan adı kilidi hizmetinin ücreti, alan adı başına yıllık vergi hariç £90 olup, bu ücret on iki aylık taksit halinde ödenebilmektedir (Nominet, 2023a).

Alan adı kilidi hizmetinde iki faktörlü kimlik doğrulama ve zaman tabanlı bir sistem kullanılmaktadır. Kayıt kuruluşları, alan adı kilidi işlemini Nominet kurumsal internet sitesinde yer alan çevrimiçi hizmetler bölümünden yapmaktadır. Kayıt kuruluşu tarafından alan adı kilidi işleminin yapılabilmesi için, 2FA Authenticator uygulamasında oluşturulan tek kullanımlık kodun çevrimiçi hizmetlerdeki ilgili bölüme girilmesi gerekmektedir. Tek kullanımlık kodun sisteme girilmesinden sonra ise, sistemde tanımlı kayıt kuruluşu yetkili kişilerine bir onay elektronik postası gönderilecektir (Nominet, 2023a; Nominet, 2023f).

Alan adı kilidinin açılabilmesi için kilitlemeye benzer bir şekilde 2FA Authenticator uygulamasında oluşturulan tek kullanımlık kodun ilgili bölüme girilmesi ve kayıt kuruluşu yetkili kişilerine iletilen elektronik postaya onay verilmesi gerekmektedir. Alan adı kilidi yirmi dakikalık bir süre için açılmakta bu sürenin sonunda otomatik olarak kilitlenmektedir. Ayrıca, yirmi dakikalık süre içerisinde manuel olarak da alan adı tekrar kilitlenebilmektedir (Nominet, 2023f).

Alan adı kilidinin kaldırılması için, kayıt kuruluşu tarafından çevrimiçi hizmetlerdeki ilgili bölüme 2FA Authenticator uygulamasında oluşturulan tek kullanımlık kodun girilmesi ve kayıt kuruluşu yetkili kişilerine iletilen elektronik postaya onay verilmesi gerekmektedir (Nominet, 2023f).

- **Soruşturma Kilidi**

Soruşturma kilidi, ".uk" uzantılı bir alan adının yasa dışı faaliyetlerde kullanıldığının polis tarafından bildirilmesi, yasa dışı faaliyet gerçekleştirildiğine dair kanıta dayanan şikayetlerin alınması veya fark edilmesi durumunda, kayıt kuruluşlarının kullanması için Nominet tarafından geliştirilen bir yöntemdir. Soruşturma kilidi konulan alan adının; internet site içeriğine erişilememekte, alan adı bilgileri değiştirilememekte, alan adından feragat edilememekte ve başka bir kayıt kuruluşuna transferine izin verilmemektedir. Ayrıca, alan adının whois'deki durumunda durdurulmuş bilgisi yer almaktadır (Nominet, 2023g).

Kayıt kuruluşları tek bir alan adı için soruşturma kilidi işlemini yapabileceği gibi kendi sistemlerinde kayıtlı bir hesaptaki tüm alan adları için de soruşturma kilidi işlemini yapabilmektedir. Soruşturma kilidi konulan alan adları tahsis süresi boyunca durdurulmakta ve tahsis süresi sona erdikten doksan gün sonra iptal edilmektedir. Kayıt kuruluşu tarafından yapılan incelemenin tamamlanmasından sonra soruşturma kilidi kaldırılabileceği gibi alan adı kilitli kalmaya devam da edebilmektedir (Nominet, 2023g).

Soruşturma kilidi işleminin ağır etkileri olduğundan dolayı, Nominet bu işlemin yasa dışı faaliyet şüphesine dair güvenilir kanıt bulunduğu durumda kullanabileceğini belirtmiş, kayıt kuruluşu tarafından işlemin istismar edilmesi durumunda ise kayıt kuruluşu ile yaptığı ".UK Kayıt Otoritesi-Kayıt Kuruluşu Sözleşme *(.UK Registry-Registrar Agreement)*"sini askıya alabileceğini belirtmiştir. Buna ek olarak, soruşturma kilidi konulabilecek alan adı sayısına sınırlama getirmiştir (Nominet, 2023g). Nominet'in kayıt kuruluşları ile yaptığı sözleşmede bu sınır, kayıt

kuruluşunun iptal ettiği alan adları ile soruşturma kilidi koyduğu alan adları sayısının toplamına göre belirlenmiştir. Bu sınıra göre, kayıt kuruluşunun iptal ettiği alan adı sayısı ile soruşturma kilidi koyduğu alan adı sayısı toplamının hizmet verdiği alan adı sayısının %5'ini aşmaması gerekmektedir. Kayıt kuruluşu tarafından bu sınırın aşılmaya çalışıldığı durumlarda alan adı iptal edilmekte ve soruşturma kilidi işlemleri otomatik olarak reddedilmektedir. Kayıt kuruluşunun belirlenen sınırı aşması gereken durumlarda ise Nominet ile iletişime geçmesi gerekmektedir (Nominet, 2023ğ).

- **Ceza Uygulamaları Politikası**

Nominet, suç faaliyetleri için kullanılan alan adlarına yönelik "Ceza Uygulamaları Politikası (*Criminal Practices Policy*)" geliştirmiştir. Bu politika, Birleşik Krallık kolluk kuvvetleri tarafından ".uk", ".cymru" veya ".wales" uzantılı alan adlarının suç faaliyeti için kullanıldığını belirten resmi yazılı bildirim alınmasından sonraki süreci içermektedir. Nominet, bildirime konu alan adı hakkında daha önce bir önlem alınmadığı, idari kontrollerin yapıldığı ve ihbar süresinin sona erdiği durumda alan adını özel statüye[23] almaktadır. Alan adı özel statüye alınmadan kırk sekiz saat önce alan adı sahibine; suç faaliyeti değerlendirmesini gerçekleştiren ilgili Birleşik Krallık kolluk kuvveti iletişim bilgilerini içeren bildirim yapılmaktadır. Alan adı sahibi yapılan değerlendirmeye katılmıyorsa bu iletişim bilgileri yoluyla şikayette bulunabilmektedir. Kamu zararının yakın zamanda oluşabileceğine dair ciddi kanıtlar olduğu durumda ise ilgili alan adı derhal durdurulabilmektedir (Nominet, 2021, s.4).

Ceza Uygulamaları Politikası'nda özel statüye alınan alan adının bu statüden çıkarılabilmesi için suç faaliyeti değerlendirmesini yapan ilgili Birleşik Krallık kolluk kuvvetinin, alan adının artık suç teşkil eden faaliyetlerde kullanılmadığını Nominet'e bildirmesi gerekmektedir (Nominet, 2021, s.4).

---

[23] Ceza Uygulamaları Politikası'nda özel statü, alan adını durdurulması veya alan adının bir bilgi/yardım sayfasına yönlendirmesi olarak ifade edilmiştir.

Alan adı, “.uk” uzantılı olması durumunda en az 24 ay, “.cymru/.wales” uzantılı olması durumunda geçerlilik süresi dolana kadar özel statüde kalmaktadır. Özel statü süresi sonunda alan adı iptal edilerek yeniden tahsis edilebilir hale gelmektedir (Nominet, 2021, s.4).

- **DNSSEC**

“.uk” uzantılı alan adlarında DNSSEC teknolojisi kullanılmaktadır. Nominet kurumsal internet sitesinde kayıt kuruluşları özelinde olmak üzere DNSSEC ile ilgili bilgiler paylaşılmıştır. Bu sayfalarda kayıt kuruluşlarının DNSSEC’i, EPP ve diğer kayıtlar özelinde nasıl yöneteceğine ilişkin bilgiler paylaşılmış ve DNSSEC destek diyagramları yayınlanmıştır (Nominet, 2024a; Nominet, 2024b; Nominet, 2024c; Nominet, 2024ç).

- **Alan Adı Kayıt Bilgileri Kontrolü**

Alan Adı Kaydı Hüküm ve Koşullar madde 3.1.2, alan adı kayıt bilgileri kontrolüne ilişkin bir düzenleme içermektedir. Bu maddeye göre alan adı sahibi; adını, adresini, telefon numarasını ve elektronik posta adresini doğru olarak iletmelidir. Ayrıca, bu bilgilerin teyidi için Nominet tarafından bir talepte bulunulması halinde talep hızlı bir şekilde yerine getirilmelidir. Talebin yerine getirilmemesi halinde Alan Adı Kaydı Hüküm ve Koşullar kapsamında alan adı iptal edilebilmekte veya özel statüye alınabilmektedir (Nominet, 2020, s.7):

> *“10.1 Aşağıdaki durumlarda size bildirimde bulunarak bir alan adını iptal edebilir veya özel bir statüye alabiliriz:*
> *10.1.1 Tamamen kendi takdirimize bağlı olarak, sizin veya kayıt kuruluşunuzun ciddi ölçüde hatalı, şüpheli veya yanlış iletişim bilgileri (isimler dahil) verdiğini, iletişim bilgilerini güncel tutmadığını veya bu bilgileri hiç vermediğini düşündüğümüz durumda, ...”*

“.uk” uzantılı alan adlarında kayıt bilgileri kontrolü Mitek[24] aracılığıyla yapılmaktadır. Yapılacak kontroller, alan adı sahibinin Nominet çevrimiçi hizmetler kullanıcı bilgilerini kaybetmesi durumunda talep üzerine yapılabileceği gibi, doğrudan Nominet tarafından da yapılabilmektedir (Nominet, 2024d).

Kontrol süreci Nominet tarafından iletilen elektronik posta ile başlamaktadır. Elektronik postada, ilgili belgelerin yüklenebileceği ve erişim sağlamak için SMS doğrulama kodu alınabilen Mitek platformuna ait bir bağlantı yer almaktadır. Belirtilen elektronik posta Mitek tarafından da iletilebilmektedir (Nominet, 2024d).

Kontrol sürecinin yedi gün içerisinde tamamlanması gerekmektedir. Sürenin dolmasından üç gün önce bir hatırlatma e-postası iletilmektedir. Süreç halen tamamlanmaz ise sürenin dolmasından yirmi dört saat önce ikinci bir hatırlatma e-postası daha iletilmektedir (Nominet, 2024d).

Süreç kapsamında hangi belgelerin iletilmesi gerektiği koşullara göre değişebilmektedir. Genel olarak, fotoğraflı bir kimlik belgesi veya sürücü belgesi, fatura veya banka özeti gibi belgelerin yüklenmesi gerekmektedir. Bazı durumlarda ek belgelerin yüklenmesi istenebilmektedir (Nominet, 2024d).

4.7. Kanada

Kanada’nın ccTLD’si “.ca”dır ve kar amacı gütmeyen bir kuruluş olan Canadian Internet Registration Authority *(CIRA)* tarafından yönetilmektedir (CIRA, 2023b).

[24] Mitek, finansal kurumlar, ödeme şirketleri ve yüksek düzeyde denetimli sektörlerde faaliyet gösteren diğer işletmeler tarafından tercih edilen bir kimlik doğrulama sağlayıcısıdır. Mitek, dijital ayak izleri, kimlik belgeleri ve biyometrik yüz tanıma aracılığıyla insanları hızlı ve güvenli bir şekilde doğrulamaktadır.

“.ca” uzantılı alan adları sadece, “Kanada'da Bulunma Koşulları[25]”nı sağlayan kişiler tarafından tahsis edilebilmektedir (CIRA, 2023c). Tahsis işlemlerinde ilk gelen ilk alır kuralı işletilmektedir (CIRA, 2019).

CIRA, auDA’nın “Rezerve Adlar *(Reserved Names)*”ına benzer bir şekilde “Rezerve/Yasak Adlar (Reserved/Restricted Names)” ile bazı adların “.ca” altında tahsisine izin vermemekte, bazı adların tahsisini ise belirli kişilere yapmaktadır. Bu listelerin hangi adları içereceği, “.ca”’ya ilişkin “Genel Kayıt Kuralları (*General Registration Rules)*”’nda belirtilmiş ve bunlarla sınırlı olmadığı ifade edilmiştir (CIRA, 2019).

Alan adı sahiplik bilgilerinin doğruluğuna ilişkin olarak CIRA, Punktum dk’nın uyguladığı sürece benzer olarak Kayıt Sahibi Bilgi Doğrulaması *(Registrant Information Validation - RIV)* sürecini gerçekleştirmektedir. RIV sürecinde alan adı sahibinin bilgileri Kanada Mevcudiyet Gerekliliği Politikasına[26] uygunluğu kapsamında kontrol edilmektedir. CIRA, “.ca” uzantılı alan adlarına ilişkin “Alan Adı Sahibi Sözleşmesi *(Registrant Agreement)*”ne göre; alan adı sahibinin ilettiği bilgilerinin kontrolünü sağlamak için belge talep edebilmektedir (CIRA, 2022; CIRA, 2023ç).

RIV süreci, alan adı sahibi ve/veya idari irtibat kişisine; Kanada Mevcudiyet Gerekliliği politikasına uygunluğunu gösteren belgelerin iletilmesi gerektiğine dair yapılan bildirimle başlamaktadır. Sürecin başlamasıyla birlikte alan adının başka bir

---

[25] Kanada'da Bulunma Koşulları; “Alan adı sahipleri için Kanada'da Bulunma Koşulları”nda tanımlanan ve Kanada vatandaşı veya daimi ikamet eden olma, Kanada yasalarına veya Kanada’nın herhangi bir eyaletine veya bölgesine tabi bir şirket olma ve Aborijin Halkları gibi farklı durumları içeren terimdir. Daha fazla bilgi için bkz. (https://www.cira.ca/en/resources/documents/domains/canadian-presence-requirements-registrants/), (21.12.2023)

[26] “Kanada'da Bulunma Koşulları”nı sağlayan alan adı sahipleri ile CIRA öncesi “.ca” uzantılı alan adı sahibi olan kişileri de kapsayan daha geniş bir topluluğa ilişkin politikadır. Daha fazla bilgi için bkz. (https://www.cira.ca/en/resources/documents/domains/canadian-presence-requirements-registrants/,) (21.12.2023)

kayıt kuruluşu veya kişiye transferi ile iletişim bilgilerinin değiştirilmesi CIRA tarafından engellenmektedir (CIRA, 2023ç).

İlk bildirim tarihinden itibaren on iş günü içerisinde Kanada Mevcudiyet Gerekliliği politikasına uygunluğu kanıtlayan belge iletilmezse, CIRA tarafından hatırlatma amacıyla ikinci bir bildirim yapılmakta ve beş iş günü içerisinde belge iletilmediği takdirde alan adının durdurulacağı belirtilmektedir. Bu süre zarfında belge iletilmediği durumda, alan adının otuz günlüğüne durdurulduğu ve bu süre içerisinde kanıtlayıcı belge iletilmediği takdirde alan adının iptal edileceğine dair "durdurma bildirimi" yapılmaktadır. Otuz günlük süre zarfında da kanıtlayıcı belge iletilmemesi halinde, alan adının iptal edildiğine dair son bir bildirim yapılmaktadır (CIRA, 2023ç).

RIV süreci kapsamında iletilen belgelerin CIRA tarafından uygun bulunduğu durumda[27] alan adı sahibi ve/veya idari irtibat kişisine, iletilen belgelerin uygun bulunduğuna ilişkin elektronik posta gönderilecek ve alan adı üzerindeki transfer ve bilgi değişikliğine ilişkin kısıtlamalar kaldırılacaktır. İletilen belgeler CIRA tarafından uygun bulunmadığı takdirde ise alan adı sahibi ve/veya idari irtibat kişisine, iletilen belgelerin uygun bulunmadığı ve alan adının iptal edilerek yeniden tahsise açılacağına ilişkin elektronik posta gönderilecektir (CIRA, 2023ç).

CIRA, alan adı kilidi kapsamında "Kayıt Otoritesi Kilidi *(Registry Lock)*" hizmetini sunmaktadır. Bu hizmet sayesinde, kilitli bir adına dair bilgiler değiştirilememekte, alan adı transfer edilememekte ve alan adından feragat edilememektedir. Kayıt otoritesi kilidi hizmeti, ".ca" uzantılı alan adı hizmeti veren kayıt kuruluşları aracılığıyla yıllık olarak alınabilmekte ve tahsis süresi boyunca otomatik olarak yenilenmektedir (CIRA, 2023a). Kayıt kuruluşlarının kayıt otoritesi hizmeti için alan adı başına ödediği ücret yıllık 240$'dır (CIRA, 2023d).

---

[27] CIRA, kabul edilebilir belgelerine ilişkin olarak kurumsal internet sitesinde bilgi vermektedir. Daha fazla bilgi için bkz. (https://www.cira.ca/en/legal-policy-and-compliance/registrant-information-validation/), (21.12.2023)

CIRA, DNS Abuse ile mücadelede doğrudan aksiyon alabilmektedir. ".ca"ya ilişkin "Genel Kayıt Kuralları (*General Registration Rules)*"nda DNS Abuse türleri ayrıntılı olarak tanımlanmış ve CIRA'ya belirtilen durumlarda alan adını durdurma veya iptal etme yetkisi verilmiştir:

> *"...CIRA ayrıca, doğrudan veya dolaylı olarak, kasıtlı veya kasıtsız olarak, aşağıdaki faaliyetlerden herhangi birine dahil olan veya olabilecek herhangi bir alan adı kaydını durdurabilir ve/veya iptal edebilir:*
>
> 1. ***Yasa dışı veya hileli eylemler (Illegal or fraudulent actions)****;*
> 2. ***İstenmeyen Elektronik Posta (Spam):*** *Elektronik mesajlaşma sistemlerinin istenmeyen toplu mesajlar göndermek için kullanılmasıdır. Bu terim, elektronik posta spam'ı ve anlık mesajlaşma spam'ı, mobil mesajlaşma spam'ı ve internet siteleri ile internet forumlarının spam'ı gibi benzer suistimaller için geçerlidir. Örnek olarak, hizmet engelleme saldırılarında elektronik postaların kullanılması;*
> 3. ***Kimlik avı/oltalama (Phishing):*** *Kullanıcı adları, şifreler veya finansal veriler gibi hassas verileri ifşa etmeleri için kişileri kandırmak üzere tasarlanmış sahte internet sayfalarının kullanılması;*
> 4. ***Site Trafiği Yönlendirme (Pharming):*** *Kullanıcıların, genellikle yetkili ad sunucunun ele geçirilmesi veya yinelemeli çözümleyicinin zehirlenmesi yoluyla farkında olmadan sahte internet sitelerine veya hizmetlere yönlendirilmesi;*
> 5. ***Kötü amaçlı yazılım yayılımı (Distribution of malware):*** *Bir bilgisayar sistemine sızmak veya zarar vermek için tasarlanmış yazılımların, sahibinin onayı olmadan yayılmasıdır. Bunlarla sınırlı olmamak üzere bilgisayar virüsleri, solucanlar, keylogger'lar ve truva atları örnek olarak verilebilir;*
> 6. ***Hızlı akış barındırma (Fast flux hosting):*** *İnternet sitelerinin veya diğer internet hizmetlerinin konumunu gizlemek veya tespit ve etkisini azaltma çabalarından kaçınmak ya da yasa dışı faaliyetlere ev sahipliği*

yapmak için hızlı akış tekniklerinin kullanılmasıdır. Hızlı akış teknikleri, bir internet ana bilgisayarının veya yetkili ad sunucusunun, alan adının çözümlendiği internet üzerindeki konumu sık sık değiştirmek için DNS'i kullanmasıdır. Hızlı akış barındırma yalnızca CIRA'nın önceden izni ile kullanılabilir;

7. ***Köle bilgisayar ağları komuta ve kontrolü (Botnet command and control):*** *Güvenliği ihlal edilmiş bilgisayarlar veya "zombiler" topluluğunu kontrol etmek veya hizmet engelleme saldırılarını (DDoS saldırıları) yönlendirmek için alan adı üzerinde çalışan hizmetlerdir;*
8. ***Çocukların cinsel istismarı materyallerinin dağıtımı (Distribution of child sexual abuse material)****;*
9. ***Diğer Bilgisayarlara veya Ağlara Yasa Dışı Erişim (Illegal Access to Other Computers or Networks):*** *Başka bir tarafa ait bilgisayarlara, hesaplara veya ağlara yasa dışı olarak erişmek veya başka bir kişiye ait sisteminin güvenlik önlemlerine sızmaya çalışmaktır (genellikle "bilgisayar korsanlığı" olarak bilinir). Ayrıca, sisteme sızma girişiminin öncüsü olarak kullanılabilecek her türlü faaliyettir (örn. port taraması, gizli tarama veya diğer bilgi toplama faaliyetleri)"* (CIRA, 2019).

CIRA tarafından herhangi bir nedenle alan adının durdurulması veya iptal edilmesi durumunda, alan adı sahibi ve kayıt kuruluşuna alan adı durdurulma veya iptal edilme nedeni elektronik posta yoluyla iletilmektedir (CIRA, 2019).

Ayrıca, ".ca" uzantılı alan adlarına ilişkin "Alan Adı Sahibi Sözleşmesi"nde CIRA'ya, başvuru sahibi özelinde alan adı başvurusunu reddetme yetkisi verilmiştir. Buna göre, daha önce CIRA ile yaptığı "Alan Adı Sahibi Sözleşmesi" CIRA tarafından feshedilen kişilerin alan adı başvuruları reddedilebilmektedir (CIRA, 2022). Sözleşme fesih

nedenleri arasında, Kayıt Otoritesi PRP *(Registry PRP)*[28]sinin herhangi bir şartının ihlal edilmesi ve bu ihlalin CIRA'dan bildirim alındıktan sonra on gün içinde giderilmemesi yer almaktadır (CIRA, 2022).

CIRA, farkındalık çalışmaları kapsamında belirli bir ücret karşılığında kuruluşlara siber güvenlik eğitimleri vermektedir. Bu eğitimler beş ile elli kişi arasında çalışanı olan kuruluşlara verildiği gibi, daha büyük organizasyonlara da verilebilmektedir. Eğitim alan kuruluşlarda kimlik avı/oltalama elektronik postasına tıklayan personel sayısında ortalama üç katlık bir düşüş olduğu CIRA tarafından belirtilmektedir (CIRA, 2024a; CIRA, 2024b).

".ca" uzantılı alan adları DNSSEC teknolojisinin uygulandığı alan adları arasında yer almaktadır. CIRA, DNSSEC çerçevesinde kurumsal internet sitesinde sıkça sorulan sorular formatında bilgiler ve ".CA için CIRA DNSSEC Uygulama Beyanı *(CIRA DNSSEC Practice Statement for .CA)*" dokümanını paylaşmıştır (CIRA, 2024c; CIRA, 2024ç).

[28] CIRA'nın internet sitesinde yer alan ve CIRA tarafından zaman zaman değiştirilebilecek veya kabul edilebilecek olan; alan adı sahipleri, kayıt kuruluşları ve alan adı tahsislerine ilişkin CIRA politikaları, kuralları ve prosedürleridir. Daha fazla bilgi için bkz. (https://www.cira.ca/en/resources/documents/about/registrant-agreement/), (28.12.2023)

5. ".TR" UZANTILI ALAN ADLARINDA ALAN ADI SİSTEMİNİN KÖTÜYE KULLANIMI (DNS ABUSE) İLE MÜCADELE UYGULAMALARI

Türkiye'nin ccTLD'si ".tr"dir ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yönetilmektedir. ".tr" uzantılı alan adları 1991 yılından 2022 yılına kadar Orta Doğu Teknik Üniversitesi tarafından yönetilmiştir. 14 Eylül 2022 tarihinde .tr Ağ Bilgi Sistemi *(TRABİS)*[1]'nin faaliyete geçmesiyle birlikte internet alan adları yönetimi BTK'ya geçmiştir.

5809 sayılı Elektronik Haberleşme Kanununun (Kanun) "Kurumun[2] görev ve yetkileri başlıklı" 6 ncı maddesinin birinci fıkrasının (v) bendinde;

> *"Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri yerine getirmek*"

görevi yer almaktadır.

Kanun'un "İnternet Alan Adları" başlıklı 35'inci maddesinde yer alan *"(1) İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık[3] tarafından belirlenir."* hükmü kapsamında hazırlanan ve 07.11.2010 tarihli ve 27752 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren İnternet Alan Adları Yönetmeliği'nin (Yönetmelik) "Kurumun Görevleri" başlıklı 14'üncü maddesinin birinci fıkrasının (a) bendi ile TRABİS'i kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde TRABİS'in üçüncü bir tarafça kurulması ve işletilmesini sağlamak görevi BTK'ya verilmiştir. Bu görev uyarınca gerekli hazırlıklar tamamlanmış ve TRABİS 14 Eylül 2022 tarihinde faaliyete geçmiştir.

---

[1] .tr ağ bilgi sistemi *(TRABİS)*, ".tr" uzantılı internet alan adı sisteminin ve buna ait merkezi veri tabanının işletilmesine, rehberin oluşturulmasına, güncellenmesine ve rehberlik hizmetinin sunulmasına ve alan adı başvuru işlemlerinin gerçek zamanlı olarak yapılmasına imkân veren, tüm bu faaliyetlerin güvenli ve iş sürekliliğini sağlayacak şekilde gerçekleştirildiği sistemdir.

[2] Bilgi Teknolojileri ve İletişim Kurumu

[3] Ulaştırma ve Altyapı Bakanlığı

Yönetmelik'te alan adları yapısı; "a.tr" ve "a.b.tr" şeklinde düzenlenmiştir. "a.b.tr" yapısındaki alan adlarında ".com, .net, .gov, .dr vb." alt alan adları altında tahsis mümkünken, "a.tr" yapısındaki alan adlarında doğrudan ".tr" altında tahsis yapılabilmektedir.

".tr" uzantılı alan adları, belgeli ve belgesiz tahsis modellerinin birlikte uygulandığı karma bir model ile tahsis edilmektedir. Yönetmelik'te belgeli ve belgesiz ayrımı alt alan adları bazında yapılmıştır. ".av, .bel, .dr, .edu, .gov, .pol, .k12, .tsk, .kep" alt alan adlarını içeren alan adları belgeli olarak tahsis edilirken, ".bbs, .biz, .com, .gen, .info, .name, .net, .org, .tel, .tv, .web" alt alan adları içeren alan adları belgesiz olarak ve ilk gelen ilk alır kuralına göre tahsis edilmektedir (Gürel, s.36).

"a.tr" yapısındaki alan adları tahsis süreci 14 Eylül 2023 tarihinde başlamış ve ilk tahsis sürecinde mevcut alan adı sahiplerine öncelik tanınmıştır. Sürecin tamamlanması ile birlikte "a.tr" yapısındaki alan adları belgesiz olarak ve ilk gelen ilk alır kuralına göre tahsis edilecektir (BTK, 2024).

Belgeli olarak tahsis edilen ".tr" uzantılı alan adlarının kimler tarafından tahsis edilebileceği, BTK tarafından 15.12.2020 tarihli ve 2020/DK-BTD/346 sayılı Kurul Kararı ile yayımlanan "Belgeli Tahsis Edilecek İnternet Alan Adlarına İlişkin Usul ve Esaslar"da düzenlenmiştir. Belgesiz olarak tahsis edilen alan adlarının kimler tarafından tahsis edilebileceğine dair koşullar bulunmamaktadır ancak 21.08.2013 tarihli ve 28742 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren İnternet Alan Adları Tebliği *(Tebliğ)* "İnternet alan adı başvurusu" başlıklı 14'üncü madde uyarınca başvuru sahibinin; gerçek kişi ise Türkiye Cumhuriyeti Kimlik Kartı numarası veya yabancı kimlik numarasını[4], tüzel kişi ise vergi kimlik numarasını alan adı

[4] 5490 Sayılı Nüfus Hizmetleri Kanunu gereğince, Türkiye'de herhangi bir amaçla en az altı ay süreli ikamet tezkeresi (oturma izni belgesi) alan yabancılara Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünce "Yabancılara Mahsus Kimlik Numarası" tahsis edilmektedir. Bu numara yabancının resmî kurumlardaki iş ve işlemlerini yürütebilmesi amacıyla kullanılmaktadır.

başvurusunda iletmesi gerekmektedir. Bu kapsamda, alan adı tahsisi yapabilecek kişilere bir sınırlama getirildiği söylenebilmektedir.

Belgesiz tahsis işlemlerinde ise, bazı adların kötüye kullanılmasını engellemek için Tahsisi Kapalı Alan Adları Listesi *(TAKAL)* ve Tahsisi Kısıtlı Alan Adları Listesi *(TAKIL)* oluşturulmuştur. Bunlar; Yönetmelik, Tebliğ ve 15.12.2020 tarihli ve 2020/DK-BTD/345 sayılı Kurul Kararı ile yayımlanan "Tahsisi Kısıtlı Alan Adlarına İlişkin Usul ve Esaslar"da düzenlenmiştir.

Tebliğ'de TAKIL ve TAKAL'ın hangi adlardan oluşacağı genel olarak ifade edilmiş, bu adların BTK tarafından güncelleneceği belirtilmiştir:

> "***Tahsise kapalı ve tahsise kısıtlı adlar listesi***
> ***MADDE 34*** *– (1)* ***(Değişik:RG-17/10/2020-31277)*** *Mevzuata, kamu düzenine, ülke güvenliğine, genel ahlaka, sağlığa ve emniyete aykırı olma gibi sebeplerle tahsisine izin verilmeyen adlar Tahsise Kapalı Adlar Listesine alınır.*
> *(2) Tahsise Kısıtlı Adlar Listesi;*
> *a)Tarihi ve kültürel değerler bakımından halka mal olmuş adlardan,*
> *b)Şehir isimlerinden,*
> *c) İnternet kullanıcılarını aldatmaya yönelik olarak hazırlanabilecek finans kuruluşları ve devlet kurumları adlarını içeren sahte İAA'ların tahsisini zorlaştırmak için bank, banka, finans, bakanlık gibi adlardan,*
> *oluşur.*
> *(3)* ***(Ek:RG-17/10/2020-31277)*** *Tahsise Kapalı Adlar Listesi ve Tahsisi Kısıtlı Adlar Listesi gerektiğinde Kurum tarafından güncellenir*."

Ayrıca, TAKIL'da yer alabilecek adlar, tahsisin gerçekleşebilmesi için gönderilebilecek belgeler, başvuru değerlendirme süreci ve diğer ilgili şeyler "Tahsisi Kısıtlı Alan Adlarına İlişkin Usul ve Esaslar"da düzenlenmiştir.

TAKAL'da bulunan adları içeren alan adlarının tahsisine izin verilmemektedir. Diğer bir değişle, "a.b.tr" ve "a.tr" yapısındaki alan adlarında "a" kısmındaki adın TAKAL'da bulunması halinde başvurular otomatik olarak reddedilmektedir. Tahsisli bir alan adının "a" kısmındaki adın sonradan TAKAL'a alınması durumunda ise alan adı iptal edilmektedir.

TAKIL'da bulunan adları içeren alan adlarının tahsisi, alan adı tahsis amacının belgelendirilmesi ve ilgili belgelerin iletilmesi durumunda gerçekleştirilmektedir. Başvurulara ilişkin değerlendirme BTK tarafından yapılmaktadır. Başvurunun reddedilmesi durumunda uygun bulunmama nedenleri ile tespit edilen eksikliklere ilişkin bilgilendirme TRABİS üzerinden kayıt kuruluşuna yapılmaktadır. Kayıt kuruluşu da başvuru sahibini bilgilendirmektedir.

".tr" uzantılı alan adlarına ilişkin mevzuatta, DNS Abuse ile ilişkili olabilecek "kötü niyetli alan adı tahsisi" ifadesi yer almaktadır. Bu ifade tanımlanmamış olup, sadece Tebliğ'in "Diğer yükümlülükler" başlıklı 13'üncü maddenin (e) bendinde geçmektedir:

> *"**Diğer yükümlülükler***
> ***MADDE 13** – (1) KK; ...*
> *e) Kötü niyetli İAA tahsisine karşı tedbir almakla,*
> *... yükümlüdür."*

".tr" uzantılı alan adları kapsamında DNS Abuse ile mücadele, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile birlikte yürütülen süreçler, kritik alan adları ve DNSSEC'le gerçekleştirilmektedir. Belirtilen uygulamalar sırasıyla açıklanacaktır.

- **USOM ile Birlikte Yürütülen Süreçler**

USOM, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı gereğince 2013 yılında kurulmuştur. Ülke çapında siber güvenlik bilincini artırmak ve siber tehditlere

karşı koruma sağlamak amacıyla alarm, uyarı ve duyuru faaliyetlerini yöneten USOM, kritik durumlarda yerinde müdahale ekipleriyle olayların kontrolünü ele almak ve siber olaylara karşı ulusal düzeyde koordinasyonu sağlamak üzere faaliyetlerini sürdürmektedir (USOM, 2024a; Yılmaz, 2023, s.80) USOM faaliyetlerinin hukuki dayanağını, Kanunun "Kurumun yetkisi ve idarî yaptırımlar" başlıklı 60 ıncı maddenin on birinci fıkrası oluşturmaktadır:

> *"(11)* ***(Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.)*** *Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır."*

".tr" uzantılı alan adları kapsamında DNS Abuse ile mücadelede USOM ile birlikte iki farklı süreç yürütülmektedir Bu süreçler;

- USOM tarafından tespit edilen alan adlarına ilişkin süreç ile
- DNS Abuse kapsamında gelen şikayetlerin USOM'a iletilmesi ile ilgili süreçtir.

USOM, yapay zekâ teknolojileri kullanılarak AZAD yazılımı geliştirilmiştir. Bu yazılımda, doğal dil işleme[5] ve makine öğrenimi teknikleri kullanılarak kimlik avı/oltalama yapılması muhtemel alan adlarına ilişkin tarama yapılmaktadır (USOM, 2024b). Yapılan tarama sonrası alan adlarına 0-100 arası bir puan verilmekte, belirli bir puanın üzerinde olanlar USOM tarafından değerlendirilmek üzere bir arayüze aktarılmaktadır. USOM tarafından alan adının sakıncalı olduğunun değerlendirilmesi halinde TRABİS ilgili personele; alan adının alınacak önlemler açısından değerlendirilmesi ve gerekli işlemlerin yapılması konusunda bildirim yapılmaktadır.

[5] Doğal dil işleme (*Natural Language Processing - NLP*), bilgisayarlara insan dilini yorumlama, işleme ve anlama yeteneği veren bir makine öğrenimi teknolojisidir.

Ayrıca, USOM'un farklı araçlar ile tespit ettiği ".tr" uzantılı alan adları da bildirime konu olmaktadır.

USOM'dan gelen bildirim sonrasında, alan adı sahibi kimlik bilgilerinin doğrulanması süreci başlatılmaktadır. Bu süreçte, alan adı tedbir amaçlı durdurulmakta ve hizmet alınan kayıt kuruluşu aracılığıyla alan adı sahibinden kimlik bilgilerini kanıtlaması istenmektedir. Alan adı sahibinin, kimlik bilgilerinin doğruluğunu kanıtlayamaması halinde alan adı, Yönetmelik'in "İptal" başlıklı 11 inci maddesi gereğince iptal edilmektedir:

> *"**İptal***
> ***MADDE 11** – (1) Alan adı tahsisi aşağıda belirtilen durumlarda alan adı sahibi ve ilgili KK bilgilendirilerek TRABİS vasıtasıyla iptal edilir:*
> *a) Alan adı sahibinin verdiği bilgilerin tam ve/veya doğru olmadığının tespit edilmesi,*
> *b) Alan adının tahsise kapalı adlar listesine alınması,*
> *c) Alan adı tahsisinin iptali ile ilgili UÇHS tarafından Kuruma iletilen hakem ya da hakem heyeti kararının bulunması ve kararın uygulanması için Kurum tarafından belirlenen gerekli şartların mevcut olması,*
> *ç) Alan adı tahsisinin iptaline yönelik bir mahkeme kararının bulunması.*
> *(2) **(Ek:RG-20/4/2021-31460)** Belgeli tahsis edilen alt alan adları için başvuru esnasında sunulan bilgi ve/veya belgelerin geçerliliğini yitirdiğinin tespit edilmesi durumunda Kurum ilgili alan adı tahsisini iptal edebilir."*

DNS Abuse ile mücadele kapsamında yürütülen diğer süreçte, DNS Abuse'a ilişkin TRABİS ekibine gelen şikayetler USOM'a iletilmektedir. USOM tarafından şikayete konu alan adının sakıncalı bulunması durumunda alan adı tedbir amaçlı durdurulmakta ve alan adı sahibinin kimlik bilgilerinin doğrulanmasına ilişkin süreç başlatılmaktadır. Alan adı sahibinin kimlik bilgilerini kanıtlayamaması durumunda Yönetmelik "İptal" başlıklı 11 inci madde kapsamında alan adı iptal edilmektedir.

- **Kritik Alan Adları**

“.tr” uzantılı alan adlarında alan adı kilidi hizmeti, “kritik alan adları” listesinde yer alanlar için sunulmaktadır. Bu listede; bazı kamu kurum ve kuruluşları, bankalar vb. kuruluşlara ait alan adları yer almaktadır. Yapılan değerlendirmeye göre liste güncellenmektedir.

Kritik alan adları listesinde olanlar için yapılan ilgili işlemler gerçekleştirilmeden önce bir arayüze aktarılmaktadır. TRABİS ilgili personel tarafından bu alan adların ilgili kişileriyle mail üzerinden iletişime geçilmektedir. Elektronik posta ile teyit alındıktan sonra işleme onay verilmektedir.

Kritik alan adları kapsamındaki hizmet ücretsiz olarak sunulmaktadır. Bu hizmet herkese açık olmayıp BTK tarafından belirlenen alan adları için gerçekleştirilmektedir.

- **DNSSEC**

DNSSEC teknolojisi “.tr”de 2023 yılında kullanılmaya başlanmıştır. DNSSEC ile imzalanan ilk alan adı “dnssec.gov.tr”dir. Bu alan adı, BTK’ya tahsislidir ve DNSSEC ile ilgili bilgileri paylaşmak için kullanılmaktadır. Bu kapsamda, sıkça sorular formatında bilgi verilmiş ve “.TR Alan Adları için DNSSEC Uygulama Bildirimi (.TR DPS)” yayınlanmıştır. İnternet sitesinde ayrıca, BTK’nın çevrimiçi eğitim platformu olan “BTK Akademi” üzerinden DNSSEC eğitiminin verileceği bilgisi paylaşılmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2023; Bilgi Teknolojileri ve İletişim Kurumu, 2024).

Ayrıca, “.tr” uzantılı alan adları için hizmet veren kayıt kuruluşlarına yönelik olarak Şubat 2024'te BTK merkezinde ICANN ile iş birliği içerisinde teorik ve uygulamalı bir eğitim verilmiştir.

SONUÇ

Bu çalışmada, DNS Abuse kavramı, DNS Abuse tespit yöntemleri ve uygulanan eylemler incelenmiş; DNS Abuse ile mücadelede ccTLD uygulamaları kapsamında Almanya, Avustralya, Belçika, Danimarka, Hollanda, İngiltere, Kanada ve Türkiye'de kullanılan yöntemler ve düzenlemeler araştırılmış, gTLD uygulamaları kapsamında ICANN çalışma ve düzenlemeleri incelenmiş; Avrupa Birliği nezdinde yapılan NIS 2 Direktifi tetkik edilmiş ve hazırlanan DNS Abuse raporu hakkında bilgi verilmiştir. Bu kapsamda, ülkemizde uygulanabilecek düzenlemeler ve yöntemler tespit edilmeye çalışılmıştır.

Yapılan literatür incelemesinde DNS Abuse kavramının tanımı ve kapsamı üzerinde bir uzlaşı olmadığı görülmüştür. Bunun temel sebebi, pornografi, çocuk istismarı materyali, nefret söylemi ve fikri mülkiyet hakları ihlali gibi yasa dışı internet içeriklerinin DNS Abuse kapsamına girip girmeyeceği konusundaki anlaşmazlıktır. ICANN nezdinde kabul görmüş bir tanım olmamasına rağmen "Kayıt Otoritesi Yetki Sözleşmesi (*Registry Agreements - RA*)" ile "Kayıt Kuruluşu Akreditasyon Sözleşmesi (*Registrar Accreditation Agreement - RAA*)"nde DNS Abuse; kötü amaçlı yazılım, köle bilgisayar ağları, kimlik avı/oltalama, site trafiği yönlendirme ve diğer türler için dağıtım mekanizması olarak kullanıldığında istenmeyen elektronik posta olarak tanımlanmış, yasa dışı internet içerikleri tanım kapsamına dahil edilmemiştir.

Tüm gTLD uzantılı alan adlarının yönetimi RA ve RAA yoluyla yapılmasına karşın ccTLD uzantılı alan adlarının yönetimi farklılık göstermektedir. DNS Abuse da bu farklılıktan etkilenmektedir. ccTLD'ler bazında yapılan incelemeler neticesinde;

- ".au" düzenlemelerinde DNS Abuse ifadesinin yer aldığı ve tanımın ICANN'e atıfla yapıldığı,
- ".be" düzenlemelerinde "alan adı kötüye kullanımı (*domain name abuse*)" ifadesinin yer aldığı ancak bir tanımın yapılmadığı,

- ".ca" düzenlemelerinde DNS Abuse'a ilişkin herhangi bir ifadenin yer almadığı ancak alan adı üzerinden yapılması halinde durdurma ve iptal eylemlerinin uygulanabileceği türlerin tanımlandığı,
- ".dk" düzenlemelerinde "Alan Adının Yasa dışı Kullanımı (*Unlawful use of a Domain Name*)" ifadesinin yer aldığı ve tanımın örnekler üzerinden yapıldığı,
- ".nl" düzenlemelerinde bir tanımın yapılmadığı ancak yasa dışı veya suç teşkil eden ifadesi ile çok geniş bir kapsamda eylemde bulunabileceğinin belirtildiği,
- ".de" düzenlemelerinde DNS Abuse'la ilişkili olabilecek "yasa dışı" ifadesinin yer aldığı ancak herhangi bir tanımın yapılmadığı
- ".uk" düzenlemelerinde DNS Abuse ifadesinin doğrudan değil bazı türleri itibariyle yer aldığı ve uygulanabilecek eylemlerin belirtildiği ve
- ".tr" düzenlemelerinde DNS Abuse'la ilişkili olabilecek "kötü niyetli alan adı tahsisi" ifadesine yer verildiği ancak tanımın yapılmadığı görülmüştür.

Sonuç olarak, ccTLD'ler düzeyinde DNS Abuse kavramı kullanımının yaygın olmadığı ve bazı kayıt otoritelerinin yasa dışı internet içeriklerine müdahalede bulunduğu anlaşılmıştır.

DNS Abuse faaliyeti yürütülen alan adlarının tespiti; kayıt otoriteleri, ticari şirketler, kamu kurumları ve kar amacı gütmeyen kuruluşlar gibi farklı aktörler tarafından yapılmaktadır. Bu tezin odağını oluşturan kayıt otoriteleri tarafından yapılan tespitler ise farklı yöntemler ile gerçekleşmektedir. Bunlar; resen yapılan tespitler, bildirimlere bağlı yapılan tespitler, hizmet alınan kuruluşlar aracılığıyla yapılan tespitler ve "Reputation Block List - RBL" aracılığıyla yapılan tespitler olarak sınıflandırılabilir.

DNS Abuse tespiti yapılan alan adlarına karşı kayıt otoriteleri tarafından "Kilitle *(Lock)*, Durdur *(Hold/Suspension)*, Yönlendir *(Redirect)*, Aktar *(Transfer)*, İptal *(Delete)* ve Oluştur *(Create)*" gibi farklı eylemler uygulanabilmektedir. Seçilecek eylemin tespiti DNS Abuse'un türü ve mevcut koşullara göre değişebilmektedir ancak yapılan araştırmalarda kayıt otoritelerinin en fazla durdur eylemini kullandığı tespit edilmiştir.

DNS Abuse ile mücadelede farklı yöntemler kullanılabilmektedir. Yapılan araştırmalar neticesinde bu yöntemlerin; alan adı kayıt bilgilerinin kontrolü, alan adı kilidi, hesap güvenliği, makine öğrenimi, DNSSEC teknolojisi, farkındalık çalışmaları ve kurum ve kuruluşlar ile iş birliği başlıkları altında toplanabileceği değerlendirilmiştir. DNS Abuse'e karşı yürütülecek çalışmalarda farklı yöntemlerin uyum içerisinde kullanılmasının faydalı olacağı değerlendirilmektedir.

Avrupa Birliği tarafından DNS Abuse ile ilgili olarak yapılan çalışmalar kapsamında NIS 2 Direktifi ve DNS Abuse raporu incelenmiştir. NIS 2 Direktif'inde kayıt otorite ve kayıt kuruluşlarının DNS Abuse ile mücadele kapsamında eylemde bulunması gerekmemekte ancak alan adı kayıt bilgilerinin doğruluğu ve tamlığının sağlanması ile bu bilgilerin ilgili kişilere verilmesi hususlarını yerine getirmesi istenmektedir.

Avrupa Komisyonu tarafından yayımlanan DNS Abuse raporunda da alan adı kayıt bilgilerinin doğruluğu ve tamlığı konusuna önem verilmiştir. Bu bilgilerin teyidi için de ilgili prosedür ve kimlik tanıma yöntemlerinin kullanılması tavsiye edilmiştir. Ayrıca, kötüye kullanım amaçlı alan adı tahsislerini önlemek için tahmine dayalı algoritmalar veya diğer yöntemlerin kullanılması, ilan edilen kötüye kullanım oranlarını belirli bir süre boyunca aşan kayıt otoritesi ve kayıt kuruluşlarının yetkilendirmelerinin iptal edilmesi, DNSSEC imzalı alan adları için indirimler yapılması, yinelemeli çözümleyicileri işleten internet servis sağlayıcılarının DNSSEC doğrulamalarını yapılandırması ve DNS Abuse kapsamında farkındalık çalışmalarının yürütülmesi tavsiye edilmiştir.

DNS Abuse ile mücadelede kapsamında ccTLD uzantılı alan adlarında kayıt otoritelerinin, gTLD uzantılı alan adlarında ise kayıt kuruluşlarının daha aktif rol aldığı görülmüştür. Bu durumun RA, RAA ve ccTLD düzenlemeleri ile ilgisi bulunmaktadır. İlgili düzenlemeler incelendiğinde; ccTLD'lerde kayıt otoritelerinin daha yetkili olduğu görülürken, gTLD'lerde ise paydaşlar arası bir yetki dağılımının olduğu görülmüştür. ccTLD'ler arasında ".uk" gibi gTLD yapısına daha yakın örnekler de bulunmaktadır.

gTLD uzantılı alan adları DNS Abuse politikası ICANN tarafından belirlenmektedir. ICANN, DNS Abuse ile mücadelede RA ve RAA ile kayıt otoritesi ve kayıt kuruluşlarına bazı sorumluluklar yüklemiştir. Bu sorumluluklar kapsamında kayıt otoritesi ve kayıt kuruluşları DNS Abuse ile mücadelede aktif olarak rol almaktadır.

RA hükümleri uyarınca kayıt otoriteleri;

- DNS Abuse da dahil olmak üzere TLD'deki kötü niyetli davranışlarla ilgili bildirimleri değerlendirecek sorumlu irtibat noktasını ICANN'e bildirmeli ve internet sitesinde yayınlamalı,
- TLD'de kayıtlı bir alan adının DNS Abuse için kullanıldığını tespit etmesi halinde eylemde bulunmalı veya konuyu kayıt kuruluşuna yönlendirmeli,
- Sahipsiz birleştirici kayıtlarının kötü amaçlı kullanımını engellemeli,
- Kötü amaçlı yazılım, kimlik avı/oltalama, korsanlık, ticari marka veya telif hakkı ihlali gibi faaliyetleri yasaklayan ve bunların yapılması halinde durdurma dahil eylemlerin uygulanacağını belirten hükümleri kayıt kuruluşu ile alan adı sahibi arasında yapılan sözleşmeye eklenmesini sağlamalı ve
- TLD'deki alan adlarının DNS Abuse için kullanılıp kullanılmadığını tespit etmek adına periyodik teknik analizler gerçekleştirmeli, bu analizler sonucunda tespit edilen DNS Abuse kayıtları ve alınan önlemler çerçevesinde istatistiksel rapor tutmalıdır.

RAA'da belirtilen yükümlülükler çerçevesinde kayıt kuruluşları;

- DNS Abuse ve yasa dışı faaliyet bildirimleri de dahil olmak üzere, hizmet verilen alan adlarıyla ilgili kötüye kullanım bildirimlerini almak için kötüye kullanım irtibat noktası oluşturmalı,
- Bu tür bildirimler için internet sitesinin ana sayfasında veya ICANN tarafından belirlenebilecek başka bir yerde görünür ve kolayca erişilebilen bir elektronik posta adresi veya web formu yayınlamalı,

- Hizmet verdiği alan adının DNS Abuse için kullanıldığını tespit ettiğinde uygun eylemi derhal gerçekleştirmeli,
- Kurulduğu veya fiziksel bir ofisinin bulunduğu bölgenin ulusal veya bölgesel hükümeti tarafından yetkilendirilmiş kolluk kuvvetleri, tüketici koruma makamı, yarı hükümet veya diğer benzer yetkililer tarafından yasa dışı faaliyet bildirimlerini almak için, sürekli takip edilen elektronik posta adresi ve telefon numarası da dahil olmak üzere özel bir kötüye kullanım irtibat noktası oluşturmalı,
- Kötüye kullanım bildirimlerinin alınması, işlenmesi ve izlenmesine ilişkin prosedürlerinin açıklamasını internet sitesinde yayınlamalı ve
- Bu tür tüm bildirimleri aldığını ve bunlara yanıt verdiğini belgelemelidir.

gTLD kayıt otoritesi ve kayıt kuruluşlarının RA ve RAA'da belirtilen yükümlülükleri yerine getirmemesi halinde ICANN tarafından soruşturma başlatılabilmektedir. Soruşturma sürecinde ihlal düzeltilmezse ICANN tarafından kamuya açık bir ihlal bildirimi yayınlanmaktadır. İhlal bildiriminde belirtilen tarihe kadar ilgili yükümlülükler yerine getirilmediği durumda, kayıt otoritesi ve kayıt kuruluşlarının sözleşmeleri feshedilebilmektedir.

ICANN, DNS Abuse ile mücadele kapsamında "Alan Adı Kötüye Kullanım Faaliyeti Raporlama *(Domain Abuse Activity Reporting - DAAR)* ve "Alan Adı Güvenliği Tehdidi Bilgi Toplama ve Raporlama *(The Domain Name Security Threat Information Collection and Reporting -DNSTICR)"* projelerini yürütmektedir. DAAR projesinde, RBL'ler aracılığıyla tespit edilen kimlik avı/oltalama, kötü amaçlı yazılım, köle bilgisayar ağları komuta ve kontrol ve istenmeyen elektronik posta verileri kayıt otoritelerine raporlanmaktadır. Kayıt otoriteleri hem kendi verilerini hem de anonimleştirilmiş toplu istatistikleri bu raporlarda görebilmektedir. Projeye gTLD kayıt otoritelerinin yanı sıra ccTLD kayıt otoriteleri de katılabilmektedir. DNSTICR ise, kimlik avı/oltalama veya kötü amaçlı yazılım faaliyetlerinde kullanılan ve belirli isimleri içeren alan adlarını raporlayan bir projedir. Raporları oluşturmak için mevcut gTLD bölge dosyalarında belirli anahtar kelimeleri içeren alan adları taranmakta ve

tarama sonucu tespit edilen alan adları tehdit istihbarat kaynakları ile karşılaştırılmaktadır. ICANN tarafından yapılan inceleme ve değerlendirmeler sonucunda raporlanmaya karar verilen alan adları ilgili kayıt otoritesi ve kayıt kuruluşlarına gönderilmektedir.

DNS Abuse politikası gTLD uzantılı alan adlarında genel olarak ICANN tarafından belirlenirken ccTLD uzantılı alan adlarında kayıt otoriteleri tarafından belirlenmektedir. ccTLD kayıt otoriteleri arasında uygulanan politikalarda ve kullanılan yöntemlerde farklılıklar bulunmaktadır.

DNS Abuse ile mücadelede ccTLD uygulamaları kapsamında Almanya, Avustralya, Belçika, Danimarka, Hollanda, İngiltere, Kanada ve Türkiye incelenmiştir. Yapılan incelemeler sonucunda;

- DNSSEC teknolojisinin incelenen tüm ccTLD'lerde kullanıldığı,
- Alan adı kayıt bilgileri kontrolü çerçevesinde;
    - ".au" uzantılı alan adlarında hem tahsis esnasında hem de tahsis sonrasında kontrollerin belge üzerinden yapıldığı,
    - ".dk" uzantılı alan adlarında, Danimarka'da yerleşik olan başvuru sahipleri için tahsis esnasında kontrolün yapıldığı, yerleşik olmayan başvuru sahipleri için ise bu kontrolün gerçekleştirilmediği; tahsis sonrasında Danimarka'da yerleşik olanlar için doğrulama sürecinin devam ettiği, yerleşik olmayanlar için doğrulamanın bazı durumlarda yapıldığı,
    - ".be" uzantılı alan adlarında yeni tahsis edilen tüm alan adlarının kontrol edildiği, mevcut olanlar için ise bazı durumlarda kontrolün gerçekleştirildiği,
    - ".ca", ".nl", ".tr" ve ".uk" uzantılı alan adlarında kontrolün mevcut alan adları için bazı durumlarda yapıldığı,
    - ".de" uzantılı alan adlarında ise tahsis esnasında ve tahsis sonrasında kontrollerin yapılmadığı,

- Alan adı kilidi hizmetinin “.be”, “.ca”, “.de”, “.dk”, “.nl” ve “.uk” uzantılı tüm alan adlarında sunulduğu, “.tr” uzantılı alan adlarında ise bunun bazı alan adları ile sınırlı tutulduğu,
- Kayıt kuruluşlarındaki müşteri hesaplarının güvenliği çerçevesinde sadece “.au” uzantılı alan adlarında düzenleme yapıldığı,
- “.be”, “.dk”, “.nl”, “.tr” ve “.uk” uzantılı alan adlarında makine öğrenimi teknolojisinin kullanıldığı,
- “.au”, “.be”, “.nl” ve “.uk” uzantılı alan adları kapsamında ilgili kurum ve kuruluşlar ile iş birliği yapıldığı ve
- “.au, “.be”, “.ca”, “.de”, “.dk” ve “.nl” kayıt otoriteleri tarafından farkındalık çalışmaları yürütüldüğü görülmüştür.

ÖNERİLER

DNS Abuse ile Mücadele Politikasının Değiştirilmesi: Tez kapsamında da belirtildiği üzere ".tr" uzantılı alan adları mevzuatında DNS Abuse tanımı bulunmamaktadır. Nitekim, Tebliğ'de "kötü niyetli internet alan adı tahsisi" ifadesi geçmesine rağmen tanımın yapılmamış olması sebebiyle kapsamın belirsiz kaldığı değerlendirilmektedir. Kötü niyetli internet alan adı tahsisinin DNS Abuse'u da içine alan çok daha geniş bir ifade olduğu düşünülmektedir. Mevzuatta DNS Abuse tanımının yanısıra, DNS Abuse'a karşı uygulanacak yaptırımlar da belirlenmemiştir. Tanımın ve uygulanacak yaptırımların belirlenmemiş olması, mevcut DNS Abuse politikasının geliştirilmesinin önünde bir engel oluşturmaktadır.

Uygulanan politika, USOM'un bildirimine binaen alan adının tedbir amaçlı durdurulması ve alan adı sahibi kimlik bilgilerinin kontrol edilmesi şeklindedir. Alan adı sahibi, kimlik bilgilerini kanıtlayamadığı takdirde ilgili madde kapsamında alan adı iptal işlemi gerçekleştirilmektedir. Söz konusu politika genel olarak başarılı olmakla birlikte, eksiklikleri de bulunmaktadır. Bu eksiklikler; politikanın DNS Abuse türlerine göre farklı yaptırımlar uygulanmasına imkan sağlamaması ve iptal edilen alan adının iki ay sonra yeniden başvuruya açılacak olması sebebiyle kötüye kullanımın bu sürenin sonunda tekrar edebilecek olması olarak ifade edilebilir. Alan adının durdurulması yaptırımının kullanılması halinde daha uzun olabilecek bu süre iptal kapsamında iki ay ile sınırlıdır.

Bu çerçevede, ".tr" uzantılı alan adları kapsamında DNS Abuse ile mücadelede etkin bir politikanın oluşturulabilmesi için DNS Abuse'a ilişkin tanımın ve uygulanabilecek yaptırımların alan adları mevzuatında yer alması gerektiği değerlendirilmektedir.

Bu doğrultuda, DNS Abuse kavramına karşılık olarak "alan adı sistemi kötüye kullanımı" ifadesinin, İnternet Alan Adları Yönetmeliği'nin "Tanımlar ve kısaltmalar" başlıklı 3'üncü maddesi 1'inci fıkrasında; "*ö) Alan adı sistemi kötüye kullanımı: Alan adı sistemi ile ilişkili olduğu ölçüde kimlik avı/oltalama, kötü amaçlı yazılım, köle*

bilgisayar ağları komuta kontrol, site trafiği yönlendirme ve diğer türleri yaymak için kullanıldığında istenmeyen elektronik posta gibi kötü amaçlı faaliyetler," olarak tanımlanmasının uygun olacağı değerlendirilmektedir. Uygulanacak yaptırımlar konusunda da kötüye kullanımın niteliğine ve türüne göre farklılaştırmaya gidilerek durdurma, iptal ve internet alan adı dondurma yaptırımlarının mevzuatta belirtilmesinin uygun olacağı değerlendirilmektedir. Nitekim, İnternet Alan Adları Uyuşmazlık Çözüm Mekanizması Tebliğinde internet alan adı dondurma, internet alan adı kaydında yer alan bilgilerin değiştirilmesine, internet alan adının satışına, devrine, feragatine ve kayıt kuruluşu transferine izin verilmeyip yenilenmesine izin verilmesi hali olarak tanımlanmıştır.

DNS Abuse kapsamında eylemde bulunulduğu zaman bunun ilgili taraflara kısa sürede bildirilmesi önemlidir. Bu kapsamda, alan adı sahibine ve hizmet veren kayıt kuruluşuna eylemin gerçekleştirilmesi sonrasında otomatik olarak bilgilendirici bir elektronik posta iletilmesinin uygun olacağı değerlendirilmektedir. Bu elektronik postada, uygulanan eylem ve itiraz kapsamında yapılabileceklere ilişkin bilgilerin yer almasının faydalı olacağı değerlendirilmektedir.

DNS Abuse Türlerinin Alan Adı Mevzuatında Tanımlanması: DNS Abuse politika değişikliği önerisinde; DNS Abuse'a karşılık olarak "alan adı sistemi kötüye kullanımı" ifadesinin belirtilen türler kapsamında tanımlanmasın uygun olacağı belirtilmiştir. Ancak, yapılan incelemelerde belirtilen türlerin alan adları mevzuatında tanımlanmadığı görülmüştür. Bu kapsamda, kimlik avı/oltalama, kötü amaçlı yazılım, köle bilgisayar ağları, site trafiği yönlendirme ve istenmeyen elektronik posta kavramlarının alan adları mevzuatında tanımlanmasının uygun olacağı değerlendirilmektedir.

Kayıt Kuruluşları ile İletişimin Artırılması: DNS Abuse kapsamında otomatik gönderilen elektronik postanın yanında, kayıt kuruluşunun hizmet verdiği alan adlarından DNS Abuse ile ilgili işlem yapılanların bilgisine ulaşmasını sağlayan bir

arayüz oluşturulmasının veya TRABİS geliştirmesi yapılmasının uygun olacağı değerlendirilmektedir.

Ayrıca, kayıt kuruluşlarına yönettikleri tüm alan adlarına oranla DNS Abuse faaliyeti gerçekleşen alan adları için bir puan verilmesi ve bu puana göre aylık olarak bir sıralama yapılmasının faydalı olacağı değerlendirilmektedir. Bu sıralamada kayıt kuruluşunun sadece puanını ve sıralamadaki yerini görmesinin uygun olacağı değerlendirilmektedir.

Kayıt Kuruluşu Müşteri Hesap Güvenliğinin Sağlanması: Tezin ilgili bölümlerinde, müşterinin kayıt kuruluşundaki hesabının saldırganlar tarafından ele geçirilmesi halinde, alan adı sahibinin bilgisi dışında DNS Abuse faaliyeti gerçekleştirilebileceği belirtilmiştir. Bu faaliyetler, yetkili ad sunucu bilgilerinin değiştirilmesi yoluyla yapılabileceği gibi, saldırganlar tarafından alan adı sahibi adına tahsis edilen alan adları üzerinden de yapılabilecektir. Ayrıca, alan adının devri, feragat ve transfer işlemleri ile de alan adı sahibi mağdur edilebilecektir. Bu sorunların önüne geçebilmek için müşteri hesaplarına girişte iki faktörlü kimlik doğrulama yöntemlerinin kullanılması önerilmektedir. Bu kapsamda, hesap sahibi tarafından talep edilmesi halinde bu doğrulamanın kayıt kuruluşu tarafından sağlanmasına ilişkin bir hükmün alan adları mevzuatına eklenmesinin uygun olacağı değerlendirilmektedir.

Alan Adı Kilidi Hizmetinin Tüm ".tr" Uzantılı Alan Adlarını İçerecek Şekilde Düzenlenmesi: Kayıt kuruluşu müşteri hesabının ele geçirilmesi dışında alan adı sahibinin bilgisi olmadan, kayıt kuruluşu sistemlerinin kısmen veya tamamen saldırganlar tarafından ele geçirilmesi sebebiyle de DNS Abuse faaliyeti gerçekleşebilmektedir. Ayrıca, yetkisiz bir şekilde yapılacak devir, feragat ve transfer işlemleriyle alan adı sahibi mağdur edilebilmektedir. Hem müşteri hesabının hem de kayıt kuruluşu sistemlerinin ele geçirilmesi halinde ortaya çıkabilecek sorunların önüne geçebilmek adına birçok ccTLD kayıt otoritesi tarafından alan adı kilidi hizmeti sunulmaktadır. Bu hizmet ile alan adı kayıt bilgileri değişikliği, devir, feragat ve

transfer işlemleri daha önceden belirlenen yetkili kişinin onayına sunulmakta, oluşabilecek kötüye kullanım ve mağduriyetlerin önüne geçilmektedir.

“.tr” uzantılı alan adlarında alan adı kilidi hizmeti, “kritik alan adları” kapsamında seçilen bazı alan adlarıyla sınırlı tutulmuş, genele yönelik olarak sunulmamıştır. Tercih edilen yöntem sebebiyle tüm alan adı sahipleri bu hizmetten yararlanamamaktadır. Bu eksikliğin giderilebilmesi için, alan adı kilidi hizmetinin tüm “.tr” uzantılı alan adlarını kapsayacak şekilde alan adları mevzuatında düzenlenmesinin uygun olacağı değerlendirilmektedir.

Alan adı kilidi kapsamında belirlenecek yetkili kişinin alan adı sahibi veya üçüncü bir kişi olabileceği değerlendirilmektedir. Alan adı kilidi başvurusuna ilişkin kontrolün, iki faktörlü doğrulama yapılan hesaplardan yapılması şeklinde olması ve bunun mevzuata eklenen hüküm ile sağlanmasının uygun olacağı düşünülmektedir. Bu hesaplardan elektronik başvuru formları ile yapılan başvurular kayıt kuruluşu aracılığıyla TRABİS’e iletilecek ve yapılan kontroller sonucunda onaylanabilecektir. Ayrıca, alan adı işlemleri, yetkili kişi değişikliği ve alan adı kilidi hizmetinden feragat işlemleri için de benzer süreçlerin yürütülmesinin uygun olduğu değerlendirilmektedir.

Alan adı kilidi hizmeti başvurusu, feragati ve yetkili kişi değişikliğine ilişkin süreçlerin aşağıda yer aldığı şekliyle yapılmasının uygun olacağı değerlendirilmektedir:

1. İki faktörlü doğrulama yapılan müşteri hesabından elektronik form ile ilgili talebinin yapılması
2. Kayıt kuruluşunun işlem talebini TRABİS’e iletmesi
3. TRABİS’in alan adı sahibi cep telefonu numarasına SMS ile tek kullanımlık bir kod, elektronik posta adresine bu kodun girileceği bir bağlantı iletmesi
4. Alan adı sahibi tarafından tek kullanımlık kodun iletilen bağlantıya girilmesi
5. TRABİS tarafından işlemin gerçekleştirilmesi

Alan adı kilidi hizmeti sunulan alan adları için feragat, devir, transfer ve kayıt bilgileri değişikliği işlemlerinin gerçekleştirilmesi sürecinin aşağıda yer aldığı şekliyle yapılmasının uygun olacağı değerlendirilmektedir:

1. İki faktörlü doğrulama yapılan müşteri hesabından elektronik form ile işlem talebinin yapılması
2. Kayıt kuruluşunun işlem talebini TRABİS'e iletmesi
3. TRABİS'in yetkili kişi cep telefonu numarasına SMS ile tek kullanımlık bir kod, elektronik posta adresine bu kodun girileceği bir bağlantı iletmesi
4. Yetkili kişi tarafından tek kullanımlık kodu iletilen bağlantıya girilmesi
5. TRABİS tarafından işlemin gerçekleştirilmesi

Alan adı kilidi hizmeti kapsamında elektronik başvuru formuyla yapılan işlemler için SMS ile alınan tek kullanımlık kod ve maile gelen bağlantı üzerinden yapılan doğrulama esas olmakla birlikte, alan adı sahibi tarafından BTK'ya sunulan yazılı taleplerin teyit sürecinde değerlendirmeye alınabileceği düşünülmektedir. Bu yöntem ile üçüncü kişi tarafından yönetilen veya kayıt bilgilerinde sabit telefon numarası olan alan adlarında oluşabilecek sorunların önüne geçilebileceği değerlendirilmektedir. Ayrıca, uygulamada esneklik sağlamak amacıyla, BTK'nın gerekli gördüğü hallerde farklı onay mekanizmaları oluşturabileceğine dair bir hükmün mevzuata dahil edilmesinin uygun olacağı değerlendirilmektedir.

Bunların yanı sıra, alan adı kilidi hizmetinin belirli bir ücret karşılığında sunulması ve bu ücretin, diğer ccTLD kayıt otoritesi tarifeleri, ülke piyasa koşulları ve hizmet verimliliği gözetilerek belirlenmesinin uygun olacağı değerlendirilmektedir.

Alan Adı Kayıt Bilgileri Kontrol Sürecinin Değiştirilmesi: ".tr" uzantılı alan adı kayıt bilgileri tahsis esnasında kontrol edilmemektedir. Tahsis sonrası yapılan kontroller ise çoğunlukla DNS Abuse tespiti yapılan alan adlarıyla sınırlıdır. Tez kapsamında önerilen DNS Abuse politikası değişikliğinde alan adı kayıt bilgileri kontrol yöntemi yer almamaktadır. Ancak, bu yöntemin belirli aralıklarla rastgele

seçilen alan adları kapsamında devam ettirilmesinin yararlı olacağı düşünülmektedir. Bu sayede DNS Abuse ile mücadeleye katkı sağlanacağı ve alan adı kayıt bilgilerinin TRABİS'e iletilirken daha dikkatli olunacağı düşünülmektedir.

DNSSEC Kullanımının Yaygınlaştırılması: DNSSEC'in işlevsel olabilmesi; yinelemeli çözümleyici, kök sunucu, TLD sunucu ve yetkili ad sunucunun bu teknoloji ile uyumlu olmasına bağlıdır. Kök sunucu ve ".tr" sunucusu bu teknolojiyle uyumludur ancak ülkemizdeki internet servis sağlayıcıları ile yetkili ad sunucu hizmeti veren yer sağlayıcılar için aynı durum geçerli değildir. İşlevsel olmayan bir teknoloji de kişiler tarafından tercih edilmeyecektir. Bu sebeple, internet servis sağlayıcıları ile yer sağlayıcılarının DNSSEC teknolojisi ile uyumlu olmasını zorunlu kılacak hükümlere ilgili mevzuatta yer verilmesinin uygun olacağı değerlendirilmektedir.

DNSSEC'in işlevsel olabilmesi için yapılacak geliştirmeler ne kadar önemliyse, kullanıcılar tarafından tercih edilmesi de o kadar önemlidir. Eğer kullanıcılar DNSSEC'i tercih etmezse yapılan geliştirmeler anlamını yitirecektir. Bu nedenle, kullanıcıların DNSSEC'i tercih etmelerini teşvik etmek için DNSSEC imzalı alan adlarına daha düşük ücret uygulanmasının DNSSEC kullanımının yaygınlaşması açısından yararlı olacağı düşünülmektedir.

Bunların yanı sıra, DNSSEC teknolojisi konusunda kamuoyu oluşturmak, bilgi paylaşımına imkân sağlamak ve ilgili taraflar arasında iş birliğini teşvik etmek amacıyla BTK tarafından belirli aralıklarla; internet servis sağlayıcıları, yer sağlayıcıları, kayıt kuruluşları ve ilgili akademisyen ve sivil toplum kuruluşlarının da dahil olacağı çalıştaylar düzenlenmesinin uygun olacağı değerlendirilmektedir.

DNS Abuse'a Karşı Kayıt Kuruluşlarının Aldığı Tedbirlerin İzlenmesi: DNS Abuse sonrasında uygulanan eylemlerle mağduriyetin azaltılması önemli olduğu gibi, DNS Abuse'un oluşmasını engelleyecek tedbirlerin alınması da önemlidir. Tez kapsamında yer alan öneriler arasında bulunan alan adı kilidi hizmeti, kayıt

kuruluşundaki müşteri hesabı güvenliğinin sağlanması ve DNSSEC teknolojisi bu tedbirler arasında yer almaktadır.

Tebliğ'in "Diğer yükümlülükler" başlıklı 13'üncü maddesinin (e) bendinde; kötü niyetli internet alan adı tahsisine karşı kayıt kuruluşunun tedbir alma yükümlülüğü bulunmaktadır. Kötü niyetli internet alan adı tahsisinin genel bir ifade olmasına ve mevzuatta tanımlanmamış olmasına rağmen DNS Abuse faaliyetini kapsayacağı düşünülmektedir. Bu kapsamda, DNS Abuse'a karşı önleyici tedbirler çerçevesinde kayıt kuruluşlarına sorumluluk yüklendiği düşünülmektedir.

Bu sorumluluk kapsamında, kayıt kuruluşlarının her yıl BTK'ya sundukları faaliyet raporlarında, alınan tedbirleri bildirmelerinin uygun olacağı değerlendirilmektedir. Bunun yanı sıra, belirli bir dönemde gerçekleşen DNS Abuse faaliyetlerinde hizmet verdiği alan adı sayısı yüksek olan kayıt kuruluşlarına, ilgili madde kapsamında alınan tedbirlerin yetersiz olduğunun ve bu sayıyı azaltmak için yeni tedbirler almaları gerektiğinin BTK tarafından bildirilmesinin uygun olacağı değerlendirilmektedir. Kayıt kuruluşu ile yapılan yazışmalar sonucunda mevcut durumun anlamlı bir şekilde değişmemesi halinde, ilgili mevzuat hükümleri uyarınca idari yaptırım sürecinin başlatılabileceği değerlendirilmektedir.

ICANN'in "Alan Adı Kötüye Kullanım Faaliyeti Raporlama *(Domain Abuse Activity Reporting - DAAR)* Projesine Dahil Olunması: DAAR projesinde, RBL'ler aracılığıyla tespit edilen kimlik avı/oltalama, kötü amaçlı yazılım, köle bilgisayar ağları komuta ve kontrol ve istenmeyen elektronik posta verileri kayıt otoritelerine raporlanmaktadır. Bu raporlarda, yönetilen TLD bazında yapılan analizler ile diğer gTLD ve ccTLD'lerle ilgili anonim veriler yer almaktadır. Ayrıca, DAAR sistemindeki istatistikler ve anonimleştirilmiş veriler, kayıt otoritesinin kayıt verilerini veya kötüye kullanım faaliyetlerini incelemesi, günlük veya tarihsel olarak raporlanması için bir platform görevi görebilmektedir.

Bu çerçevede, USOM tarafından tespit edilen alan adı verileri ile DAAR verilerinin karşılaştırılması, projeye dahil olan TLD'lere göre ".tr"nin hangi seviyede olduğunun anlaşılması ve raporlarda sunulan analizlerin konu hakkında uzmanlığa katkı sağlayacak olması sebebiyle DAAR projesine dahil olunmasının uygun olacağı değerlendirilmektedir.

trabis.gov.tr'de DNS Abuse ile İlgili İçeriklerinin Oluşturulması: BTK'nın ".tr" uzantılı alan adları özelinde hizmet veren internet sitesi trabis.gov.tr üzerinden DNS Abuse kapsamında farkındalık çalışmaları yapılmasının ve uygulanan politika hakkında bilgi verilmesinin uygun olacağı değerlendirilmektedir. Yapılacak çalışmada asgari olarak aşağıdaki unsurların yer almasının faydalı olacağı düşünülmektedir:

- DNS Abuse tanımı
- Yasa dışı içeriklerin kapsamı ve DNS Abuse'tan farkı
- DNS Abuse faaliyetine karşı alınabilecek önlemler
- DNS Abuse ve yasa dışı içerik şikayet mercileri
- ".tr" uzantılı alan adlarında uygulanan DNS Abuse politikası

".tr" ile İlgili Mevzuatta Terim Birliğinin Sağlanması: DNS Abuse ile mücadele kapsamına girmemekle birlikte ".tr" ile ilgili mevzuat içerisindeki "alan adı" ve "internet alan adı" karışıklığına son verilmesinin uygun olacağı değerlendirilmektedir. Yönetmelik'in "Tanımlar ve kısaltmalar" başlıklı 3 üncü maddesinde alan adı, ".tr" uzantılı internet alan adı; "internet alan adı ise okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokol adresini bulan ve kullanıcıya veren sistem" olarak tanımlanmıştır. Tebliğ'de ise internet alan adı, ".tr" uzantılı internet alan adı olarak tanımlanmıştır. Bu karışıklık BTK tarafından yayımlanan Usul ve Esaslar kapsamında da devam etmiştir. Bu çerçevede, Kanun gereği strateji ve politika belirleyicisi olan Ulaştırma ve Altyapı Bakanlığı tarafından belirlenecek terim üzerinden mevzuat değişikliklerinin yapılmasının uygun olacağı değerlendirilmektedir.

KAYNAKLAR

ALTINOK Arda, 2019, Markanın İnternet Alan Adı Olarak Kullanılması, Yüksek Lisans Tezi, İstanbul

Amazon, 2023, What is DNS?, https://aws.amazon.com/tr/route53/what-is-dns/ (04.09.2023)

auDA, 2020, auDA Registrar Agreement, https://assets.auda.org.au/a/2020-11/auDA-Registrar-Agreement-20200625.pdf?VersionId=jphjRHOyDr9_iM8q01PhhQ3Kxk_Tb3Fj, (23.05.2024)

auDA, 2023a, About .au Domain Administration, https://www.auda.org.au/about-auda/about-au-domain-administration, (25.11.2023)

auDA, 2023b, .au Domain Administration Rules: Licensing, https://www.auda.org.au/policy/au-domain-administration-rules-licensing#2-11, (25.11.2023)

auDA, 2023c, Combatting DNS abuse in .au - fact sheet, https://www.auda.org.au/au-domain-names/domain-name-help/combatting-dns-abuse-au-fact-sheet, (25.11.2023)

auDA, 2023ç, Fact sheet – Keep your website secure from DNS abuse, https://www.auda.org.au/au-domain-names/domain-name-help/fact-sheet-keep-your-website-secure-dns-abuse, (28.11.2023)

auDA, 2024, Domain Name System Security Extensions (DNSSEC), https://www.auda.org.au/industry/information-registrars/domain-name-system-security-extensions-dnssec, (26.04.2024)

BELLON Lorraine, 2020, What is the difference between authoritative and recursive DNS nameservers?, https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers (03.09.2023)

Bilgi Teknolojileri ve İletişim Kurulu, a.tr Tahsisleri Başlıyor, https://www.trabis.gov.tr/content/atr, (09.01.2024)

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 15.12.2020 tarih ve 2020/DK-BTD/345 sayılı "Tahsisi Kısıtlı Alan Adlarına İlişkin Usul ve Esaslar" konulu karar

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 15.12.2020 tarih ve 2020/DK-BTD/346 sayılı "Belgeli Tahsis Edilecek İnternet Alan Adlarına İlişkin Usul ve Esaslar" konulu karar

Bilgi Teknolojileri ve İletişim Kurumu, 2023, TR Alan Adları için DNSSEC Uygulama Bildirimi (.TR DPS), https://www.trabis.gov.tr/medya/docs/eP381oDF8oXJZICzD5tw3lx3TggphUtvZ6AVBr9e.pdf, (28.04.2024)

Bilgi Teknolojileri ve İletişim Kurumu, 2024, DNSSEC, https://www.dnssec.gov.tr/, (28.04.2024)

Britannica Online Encyclopedia, 2024, Internet, https://www.britannica.com/technology/Internet/Foundation-of-the-Internet, (03.05.2024)

Campbell-Kelly Martin, Garcia-Swartz Daniel D, 2013, The history of the internet: the missing narratives, Journal of Information Technology, Sayı 28, s.18-33

CENTR, 2021, Registration data accuracy in European national domain registries: existing practices and challenges, https://centr.org/library/library/download/10478/7435/41.html, (17.02.2024)

CENTR, 2022, Domain name registries and online content, https://centr.org/library/library/policy-document.html, (01.02.2024)
CHANDRAMOULI Ramaswamy, ROSE Scott, 2013, Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication 800-81-2

CIRA, 2019, General Registration Rules, https://www.cira.ca/en/resources/documents/domains/general-registration-rules/, (22.12.2023)

CIRA, 2022, Registrant Agreement, https://www.cira.ca/en/resources/documents/about/registrant-agreement/, (21.12.2023)

CIRA, 2023a, Registry Lock, https://www.cira.ca/en/ca-domains/optimize-your-ca/registry-lock/, (24.12.2023)

CIRA, 2023b, We are Canada's internet, https://www.cira.ca/en/about-cira/, (21.12.2023)

CIRA, 2023c, Canadian Presence Requirements for Registrants, https://www.cira.ca/en/resources/documents/domains/canadian-presence-requirements-registrants/, (21.12.2023)

CIRA, 2023ç, Registrant Information Validation, https://www.cira.ca/en/legal-policy-and-compliance/registrant-information-validation/, (21.12.2023)

CIRA, 2023d, Registrar Fees List, https://www.cira.ca/en/resources/documents/domains/registrar-fees-list/#registry-lock-fees, (22.12.2023)

CIRA, 2024a, Cybersecurity Awareness Training, https://www.cira.ca/en/cybersecurity/cybersecurity-awareness-training/, (22.05.2024)

CIRA, 2024b, Cybersecurity Awareness Training for Small Teams, https://www.cira.ca/en/small-teams-training/, (22.05.2024)

CIRA, 2024c, DNSSEC Securing the domain name system, https://www.cira.ca/en/dnssec-securing-domain-name-system/, (27.04.2024)

CIRA, 2024ç, CIRA DNSSEC Practice Statement for .CA, https://www.cira.ca/en/resources/documents/domains/cira-dnssec-practice-statement-for-ca/, (27.04.2024)

CleanDNS, Inc., 2024a, How CleanDNS Works, https://cleandns.com/, (09.02.2024)

CleanDNS, Inc., 2024b, Protective Holds and Their Crucial Role in Combating DNS Abuse, https://cleandns.com/protective-holds-and-their-crucial-role-in-combating-dns-abuse/, (10.02.2024)

Cloudflare, 2023, What is a DNS root server?, https://www.cloudflare.com/learning/dns/glossary/dns-root-server/ (03.09.2023)

Cloudflare, 2024, What is the Internet Protocol?, https://www.cloudflare.com/learning/network-layer/internet-protocol/, (05.05.2024)

DENIC, 2023a, .de Registry Lock, https://www.denic.de/en/service/de-registry-lock, (30.12.2023)

DENIC, 2023b, About DENIC, https://www.denic.de/en/about-denic, (29.12.2023)

DENIC, 2023c, Domain Terms and Conditions, https://www.denic.de/en/domains/de-domains/domain-terms-and-conditions, (29.12.2023)

DENIC, 2023ç, Legal Information, https://www.denic.de/en/know-how/legal-issues, (29.12.2023)

DENIC, 2023d, How to Update the Lock Contact, https://www.denic.de/en/service/de-registry-lock/update-lock-contact/, (30.12.2023)

DENIC, 2024a, Rechtswidrige Inhalte – die Grauzone im Internet, https://www.denic.de/wissen/rechtswidrige-inhalte, (24.04.2024)

DENIC, 2024b, Informationen Zu Fake Shops, https://www.denic.de/aktuelles/informationen-zu-fake-shops, (24.04.2024)

DENIC, 2024c, DNSSEC – Domain Name System Security Extensions, https://www.denic.de/wissen/dnssec, (26.04.2024)

DENIC, 2024ç, DENIC-Domainrichtlinien und Datenschutzhinweise, https://www.denic.de/domains/de-domains/domainrichtlinien, (17.05.2024)

DENNİS Michael Aaron, KAHN Robert, Internet, Encyclopaedia Britannica, https://www.britannica.com/technology/Internet, (31.08.2023)

DNS Abuse Framework, 2020, https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf, (15.11.2023)

DNS Abuse Institute, 2023, A Holistic Approach to Tackling DNS Abuse for Registries and Registrars, https://dnsabuseinstitute.org/tackling-dns-abuse/, (09.02.2024)

DNS Belgium, 2018, Fraudulent websites offline within 24 hours, https://www.dnsbelgium.be/en/news/fraudulent-websites-offline, (02.04.2024)

DNS Belgium, 2023a, Terms and conditions for.be domain name registrations, https://www.dnsbelgium.be/en/terms-and-conditions-be-domain-names, (28.04.2024)

DNS Belgium, 2023b, AI project aimed at detecting fraudulent domain name registrations, https://www.dnsbelgium.be/en/news/ai-project-aimed-detecting-fraudulent-domain-name-registrations, (02.04.2024)

DNS Belgium, 2024a Registrant verification, https://docs.dnsbelgium.be/be/general/, (01.02.2024)

DNS Belgium, 2024b, Prevention and control, https://www.dnsbelgium.be/en/secure/prevention-and-control#we-inspect-registrant-data-before-activation, (27.03.2024)

DNS Belgium, 2024c, About DNS Belgium, https://www.dnsbelgium.be/en/about-dns-belgium, (25.03.2024)

DNS Belgium, 2024ç, Documentary evidence for registrant verification, https://www.dnsbelgium.be/en/documentary-evidence-registrant-verification, (27.03.2024)

DNS Belgium, 2024d, Contact, https://www.dnsbelgium.be/en/contact, (01.04.2024)

DNS Belgium, 2024e, .be Registrant verification now also with Machine Learning, https://www.dnsbelgium.be/en/news/registrant-verification-with-machine-learning?utm_source=newsletter_186&utm_medium=email&utm_campaign=weekly-news-20240327, (02.04.2024)

DNS Belgium, 2024f, Domain Guard, https://www.dnsbelgium.be/en/secure/domain-guard, (02.04.2024)

DNS Belgium, 2024g, Domain Shield, https://www.dnsbelgium.be/en/secure/domain-shield, (02.04.2024)

DNS Belgium, 2024ğ, Request for Domain Guard, https://assets.dnsbelgium.be/attachment/Request-DomainGuard-en_1.pdf, (03.04.2024)

DNS Belgium, 2024h, Change authorised person for Domain Guard, https://assets.dnsbelgium.be/attachment/Change-auth-DomainGuard-en_0.pdf, (03.04.2024)

DNS Belgium, 2024ı, Cancellation Domain Guard, https://assets.dnsbelgium.be/attachment/Cancellation-DomainGuard-en_1.pdf, (03.04.2024)

DNS Belgium, 2024i, Safebrowsing, https://www.dnsbelgium.be/en/secure/safebrowsing, (19.04.2024)

DNS Belgium, 2024j, Safe on the internet, https://www.dnsbelgium.be/en/smart-online, (19.04.2024)

DNS Belgium, 2024k, DNSSEC, https://www.dnsbelgium.be/en/secure/dnssec, (17.04.2024)

DOĞAN İsmail Can, 2014, Propaganda Aracı Olarak İnternet: "Kayseri İli Merkez Seçmeni Üzerine Bir Alan Araştırması", Yüksek Lisans Tezi, Konya

ECO, 2022, Comment on the Study on Domain Name System (DNS) Abuse, https://www.eco.de/wp-content/uploads/2022/04/20220427_comments_ec_dns_abuse_study.pdf (12.11.2023)

Elektronik Haberleşme Kanunu, 2008, Resmi Gazete, 27050, 10 Kasım 2008

ENİSA, 2023, DNS Identity, https://www.enisa.europa.eu/publications/dns-identity, (16.02.2024)

European Commission, 2022, Study on Domain Name System (DNS) Abuse, https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1, (12.11.2023)

EURid, 2020, 1st AI-driven proactive suspension system for domain names, https://eurid.eu/en/news/1st-ai-suspension-system-for-ds/, (01.02.2024)

European Parliamentary Research Service, 2023, The NIS2 Directive: A high common level of cybersecurity in the EU, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333, (03.11.2023)

FRANKEL Tamar, 2004, Governing by Negotiation: The Internet Naming System, 12 Cardozo Journal of International and Comparative Law 449, s.449-492 https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1908&context=faculty_scholarship (06.05.2024)

GÜL, Abdülkadir, 2015, İnternet Alan Adları Uyuşmazlıkları Alternatif Çözüm Mekanizmasında Dünya Uygulamalarının İncelenmesi ve Türkiye İçin Öneriler, Bilgi Teknolojileri ve İletişim Kurumu, Uzmanlık Tezi, Ankara

GÜLDÜZ GÜREL Elif, 2022, İnternet Alan Adlari İhtilaf Türleri Ve Alternatif Çözüm Mekanizmasi: Icann Tahkim Usulü Ve ".Tr" Mevzuat İncelemesi, Ülkemiz İçin Düzenleme Önerileri, Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi, Ankara

IANA, 2023, .ARPA Zone Management, https://www.iana.org/domains/arpa, (31.08.2023)

IANA, 2024, Root Zone Database, https://www.iana.org/domains/root/db, (06.05.2024)

IBM, What is machine learning (ML)?, https://www.ibm.com/topics/machine-learning, (19.04.2024)

ICANN, 2005, Status Report on the sTLD Evaluation Process, https://archive.icann.org/en/tlds/stld-apps-19mar04/stld-status-report.pdf, (31.08.2023)

ICANN ccNSO Delegation and Redelegation Working Group, Report on the Delegation of ccTLDs, 2011, http://ccnso.icann.org/workinggroups/drd-wg-final-report-07mar11-en.pdf, (16.09.2023)

ICANN, 2012, General Questions - Complaints and Disputes, https://www.icann.org/resources/pages/faqs-84-2012-02-25-en#38, (08.03.2024)

ICANN, 2017a, Reputation Block Lists: Protecting Users Everywhere, https://www.icann.org/en/blogs/details/reputation-block-lists-protecting-users-everywhere-1-11-2017-en, (12.02.2024)

ICANN, 2017b, Advisory, New gTLD Registry Agreement Specification 11 (3)(b) , https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en, (07.03.2024)

ICANN, 2018, Notice Of Breach Of Registry Agreement, https://www.icann.org/uploads/compliance_notice/attachment/1049/serad-to-allain-11jul18.pdf, (11.04.2024)

ICANN, 2019a, How is ICANN organized?, https://atlarge.icann.org/about/how-is-icann-organized, (07.10.2023)

ICANN, 2019b, DNSSEC – What Is It and Why Is It Important?, https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en, (29.01.2024)

ICANN, 2020, Reporting Potential Pandemic-Related Domains, https://www.icann.org/en/blogs/details/reporting-potential-pandemic-related-domains-1-5-2020-en, (28.02.2024)

ICANN, 2021a, ICANN Organization Enforcement of Registration Data Accuracy Obligations Before and After GDPR, https://www.icann.org/resources/pages/registration-data-accuracy-obligations-gdpr-2021-06-14-en, (19.02.2024)

ICANN, 2021b, Second Security, Stability, and Resiliency (SSR2) Review Team Final Report, https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf, (13.11.2023)

ICANN, 2021c, SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS, https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf, (22.02.2024)

ICANN, 2021ç, Country Code Top Level Domains in DAAR, https://www.icann.org/resources/pages/daar-cctld-2021-05-11-en, (27.02.2024)

ICANN, 2022a, Bylaws For Internet Corporation For Assigned Names And Numbers, https://www.icann.org/resources/pages/governance/bylaws-en, (07.10.2023)

ICANN, 2022b, ccTLD Agreements, https://www.icann.org/resources/pages/cctlds/cctlds-en, (23.09.2023)

ICANN, 2022c, DNS Abuse Measurement Technology, https://community.icann.org/display/SIFT/DNS+Abuse+Measurement+Technology, (26.02.2024)

ICANN, 2022ç, Notice Of Breach Of Registrar Accreditation Agreement, https://www.icann.org/uploads/compliance_notice/attachment/1169/hedlund-to-miranda-10jan22.pdf, (08.03.2024)

ICANN, 2022d, Notice Of Termination Of Registrar Accreditation Agreement, https://www.icann.org/uploads/compliance_notice/attachment/1175/hedlund-to-miranda-7feb22.pdf, (08.03.2024)

ICANN, 2023a, Top-Level Domains, https://archive.icann.org/en/tlds/, (31.08.2023)

ICANN, 2023b, New General Top-Level Domains, https://newgtlds.icann.org/en/about/program, (31.08.2023)

ICANN, 2023c, About Domain Names, https://www.icann.org/resources/pages/about-domain-names-2018-08-30-en, (31.08.2023)

ICANN, 2023ç, Acronyms and Terms, https://www.icann.org/en/icann-acronyms-and-terms?page=1&search=dns%20abuse, (12.11.2023)

ICANN, 2023d, Information for Registrars, https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en (27.09.2023)

ICANN, 2023e, ICANN, 2023, ICANN's Multistakeholder Model, https://www.icann.org/community#org-structure, (07.10.2023)

ICANN, 2023f, DNS Security Threat Mitigation Program, https://www.icann.org/dns-security-threat, (12.11.2023)

ICANN, 2024a, Registry Agreement, https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-21-01-2024-en.html, (21.02.2024)

ICANN, Registrar Accreditation Agreement, 2024b, https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-21jan24-en.html#rdds-accuracy, (21.02.2024)

ICANN, 2024c, Notices of Breach, Suspension, Termination and Non-Renewal, https://www.icann.org/compliance/notices, (23.02.2024)

ICANN, 2024ç, Domain Abuse Activity Reporting, https://www.icann.org/octo-ssr/daar, (27.02.2024)

ICANN, 2024d, Frequently Asked Questions: ICANN's Domain Abuse Activity Reporting (DAAR) Project, https://www.icann.org/octo-ssr/daar-faqs/#purpose, (27.02.2024)

ICANN, 2024e, Domain Name Security Threat Information Collection & Reporting (DNSTICR), https://www.icann.org/dnsticr-en, (28.02.2024)

ICANN, 2024f, Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement, https://www.icann.org/resources/pages/advisory-compliance-dns-abuse-obligations-raa-ra-2024-02-05-en, (29.02.2024)

ICANN, 2024g, Notices of Breach, Suspension, Termination and Non-Renewal, https://www.icann.org/compliance/notices, (08.03.2024)

Internet Society, Why should I care about DNSSEC?, https://www.internetsociety.org/deploy360/dnssec/basics/, 29.01.2024

IŞIKLI Hasibe, 2001, İnternet Alan İsimleri Sistemi Markalar ve Alan İsimleri Arasındaki İlişki, Devlet Planlama Teşkilatı, Ankara

İnternet Alan Adları Yönetmeliği, 2010, Resmi Gazete, 27752 , 7 Aralık 2010

İnternet Alan Adları Tebliği, 2013, Resmi Gazete, 28742, 21 Ağustos 2013

iQ Global AS, 2024, Introducing iQ Abuse Scan, https://iq.global/iq-abuse-scan, (09.01.2024)

HASNA A., 2023, What Is DNS and How Does It Work – A Comprehensive Guide, https://www.hostinger.com/tutorials/what-is-dns

KARAKOÇ Zehra, 2022, Alan Adı Sistemi (Domain Name System – DNS) Protokollerine İlişkin Gizlilik İle Güvenlik Tehditleri ve Çözümlerinin İncelenmesi: Diğer Ülke Uygulamalarının İncelenmesi ve Ülkemiz için Öneriler, Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi, Ankara

KERNER Sean Michael, 2023, Internet Protocol, TechTarget, https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol, (31.08.2023)

LEINER Barry M. vd., 1997, Brief History of the Internet, The Internet Society, https://www.internetsociety.org/internet/history-internet/brief-history-internet/, (31.08.2023)

mambo +, 2024, https://mambo.plus/features, (09.02.2024)

Messaging, Malware and Mobile Anti-Abuse Working Group, 2023, https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries_bod_approved_jan_2024.docx_.pdf, (17.02.2024)

NetBeacon, 2024, MAP Abuse Analytics, https://netbeacon.org/map-analytics/, (14.10.2024)

Nominet, 2018, Rules, https://nominet.uk/wp-content/uploads/2018/05/22141819/dotUK-Rules-of-Registration.pdf, (30.11.2023)

Nominet, 2020, Terms And Conditions Of Domain Name Registration, https://nominet.uk/wp-content/uploads/2020/04/Terms-and-Conditions-of-Domain-Name-Registration-24-04-2020-v1.pdf, (27.05.2024)

Nominet, 2021, Criminal Practices Policy, https://nominet.uk/wp-content/uploads/2021/02/Criminal-Practices-Policy-26-11-2021.pdf, (07.12.2023)

Nominet, 2023a, Domain Lock, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-lock/, (04.12.2023)

Nominet, 2023b, Domain Watch, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-watch/, (02.12.2023)

Nominet, 2023c, Discover Nominet, https://www.nominet.uk/about/, (28.11.2023)

Nominet, 2023ç, Domain Health, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-health/, (30.11.2023)

Nominet, 2023d, Domain Health REST API, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-health/domain-health-rest-api/, (30.11.2023)

Nominet, 2023e, Domain Watch FAQs, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-watch/domain-watch-faqs/, (02.12.2023)

Nominet, 2023f, Domain Lock User Guide, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/domain-lock/domain-lock-user-guide-from-4-july-2017/, (04.12.2023)

Nominet, 2023g, Investigation Lock, https://registrars.nominet.uk/uk-namespace/security-tools-and-protection/investigation-lock/, (06.12.2023)

Nominet, 2023ğ, Acceptable Use Policies, https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/acceptable-use-policy/#Delete-and-lock, (07.12.2023)

Nominet, 2024a, DNSSEC, https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/dnssec/, (27.04.2024)

Nominet, 2024b, Managing DNSSEC with EPP, https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/dnssec/managing-dnssec-with-epp/, (27.04.2024)

Nominet, 2024c, Managing DS records for DNSSEC, https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/dnssec/dnssec-and-our-registrar-systems/, (27.04.2024)

Nominet, 2024ç, Using DNSSEC with EPP and WDM, https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/dnssec/dnssec-for-registrars/, (27.04.2024)

Nominet, 2024d, ID Verification using Mitek, https://www.nominet.uk/mitek-id-verification/, (27.05.2024)

OECD, 2006, Evolution In The Management Of Country Code Top-Level Domain Names (ccTLDs), Working Party on Telecommunication and Information Services Policies, 2006, https://www.oecd.org/sti/ieconomy/37730629.pdf, (31.08.2023)

Online Library Learning Center, 2023, A Brief History of the Internet, https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml, (31.08.2023)

Punktum dk, 2023a, Procedure for checking contact information and identity of an existing registrant resident outside Denmark, https://punktum.dk/en/articles/procedure-for-checking-contact-information-and-identity-of-an-existing-registrant-0, (19.12.2023)

Punktum dk, 2023b, https://punktum.dk/en/articles/organisation, (09.12.2023)

Punktum dk, 2023c,Terms and conditions for the right of use to a .dk domain name, https://punktum.dk/en/articles/terms-and-conditions-for-the-right-of-use-to-a-dk-domain-name, (19.12.2023)

Punktum dk, 2023ç, Terms and procedures https://punktum.dk/en/articles/terms-and-procedures, (19.12.2023)

Punktum dk, 2023d, What does it mean that my domain name is validated?, https://punktum.dk/en/faq/what-does-it-mean-that-my-domain-name-is-validated, (19.12.2023)

Punktum dk, 2023e, Procedure for checking contact information and identity of a new registrant resident in Denmark, https://punktum.dk/en/articles/procedure-for-checking-contact-information-and-identity-of-a-new-registrant-resident-in, (19.12.2023)

Punktum dk, 2023f, Procedure for checking contact information and identity of an existing registrant resident in Denmark, https://punktum.dk/en/articles/procedure-for-checking-contact-information-and-identity-of-an-existing-registrant-resident, (19.12.2023)

Punktum dk, 2023g, Procedure for checking contact information and identity of a new registrant resident outside Denmark, https://punktum.dk/en/articles/procedure-for-checking-contact-information-and-identity-of-a-new-registrant-resident, (19.12.2023)

Punktum dk, 2023ğ, Vilkår for VID-service, https://punktum.dk/artikler/vilkaar-for-vidservice, (23.05.2024)

Punktum dk, 2023h, Markant stigning i DNSSEC-signerede .dk-domænenavne, https://punktum.dk/nyheder/markant-stigning-i-dnssecsignerede-dkdomaenenavne, (26.04.2024)

Punktum dk, 2024a, Prices and fees, https://punktum.dk/en/articles/prices-and-fees, (23.05.2024)

Punktum dk, 2024b, Sikker e-handel, https://punktum.dk/artikler/sikker-ehandel, (24.04.2024)

Punktum dk, 2024c, DNSSEC - ekstra beskyttelse på dit domæne, https://punktum.dk/artikler/dnssec-ekstra-beskyttelse-paa-dit-domaene, (14.05.2024)

SIDN, 2019, Fake webshops taken off line much sooner, https://www.sidn.nl/en/news-and-blogs/fake-webshops-taken-off-line-much-sooner, (02.01.2023)

SIDN, 2023a, Assessing the risk of new .nl registrations using RegCheck, https://www.sidnlabs.nl/nieuws-en-blogs/risicobeoordeling-van-nieuwe-nl-registraties-met-behulp-van-regcheck, (03.01.2024)

SIDN, 2023b, Onze organisatie, https://www.sidn.nl/over-sidn/onze-organisatie, (30.12.2023)

SIDN, 2023c, General Terms and Conditions for .nl Registrants ,https://www.sidn.nl/downloads/5sWqyY0sTKHoWlCTm9RmZt/ef98ec32612ff200cfa94efe64b7341c/General_Terms_and_Conditions_for_nl_Registrants_20231001.pdf, (30.12.2023)

SIDN, 2023ç, Appeal and Complaint Fees, https://cvkb.nl/downloads/2SDwlMOdqSyHlzGQ3RqiTg/745fb920db130b66ab0d59db42197f1b/CvKB-regeling.pdf, (07.01.2023)

SIDN, 2024a, .nl Control, https://www.sidn.nl/en/product/nl-control, (01.01.2024)

SIDN, 2024b, Abuse prevention, https://www.sidn.nl/en/cybersecurity/abuse-prevention, (04.01.2024)

SIDN, 2024c, Complaining about the content of a website, https://www.sidn.nl/en/nl-domain-name/complaining-about-the-content-of-a-website, (02.01.2024)

SIDN, 2024ç, Notice-and-Take-Down-procedure voor .nl-domeinnamen, https://www.sidn.nl/downloads/Sfk1T4mVSaiwoO5_-T8vNg/124a9edaf6597b5b1145f0a2ff768d19/Notice_and_Take_Down_procedure_voor_nl_domeinnamen.pdf, (02.01.2024)

SIDN, 2024d, Verification of registration data, https://www.sidn.nl/en/nl-domain-name/verification-of-registration-data, (03.01.2024)

SIDN, 2024e, Voorwaarden .nl Control voor domeinnaamhouders, https://www.sidn.nl/downloads/1TyMUPWaH5mRYgLkZeQK2E/e4dded05e5f37aa08fa88f6ae0baae44/Voorwaarden_nl_Control_voor_domeinnaamhouders.pdf, (01.01.2024)

SIDN, 2024f, SIDN BrandGuard, https://www.sidn.nl/en/product/sidn-brandguard, (01.01.2024)

SIDN, 2024g, Legal follow-up, https://www.sidn.nl/en/legal-follow-up-for-sidn-brandguard-users, (02.01.2024)

SIDN, Protecting yourself against internet abuse in the Netherlands and in gTLDs 2024ğ, https://www.sidn.nl/en/cybersecurity/protecting-yourself-against-internet-abuse-in-the-netherlands-and-in-gtlds, (07.01.2024)

SIDN, 2024h, Abuse of the internet, https://www.sidn.nl/en/cybersecurity/abuse-of-the-internet, (24.04.2024)

SIDN, 2024ı, DNSSEC, https://www.sidn.nl/en/modern-internet-standards/dnssec, (26.04.2024)

SWITCH, 2021, Committed to a secure DNS in Switzerland, https://www.switch.ch/en/insights/committed-secure-dns-switzerland, (01.02.2024)

SOYSAL, Tamer, 2014, İnternet Alan Adları Hukuku, Adalet Yayınevi, Ankara

The Domain Name Industry Brief, 2024, https://dnib.com/articles/the-domain-name-industry-brief-q4-2023, (06.05.2024)

The Internet & Jurisdiction Policy Network, 2019, Domains & Jurisdiction Program, Operational Approaches Norms, Criteria, Mechanisms, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf, (19.11.2023)

The Internet & Jurisdiction Policy Network, 2021, Toolkit: Dns Level Action To Address Abuses, https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-105-Toolkit-DNS-Level-Action-to-Address-Abuses-2021.pdf, (11.02.2024)

USOM, 2024a, USOM Hakkında, https://www.usom.gov.tr/hakkimizda, (12.01.2024)

USOM, 2024b, USOM AR-GE Çalışmaları, https://www.usom.gov.tr/arge, (12.01.2024)

YASAMAN F. Zeynep, 2019, Infringement Of Trademark Rights On The Internet In The European Union And Turkish Law, Doktora Tezi, İstanbul

YEŞİL, Sezen, 2013, National Sovereignty In Internet Governance: The Case Of The Turkish ccTLD, (Unpublished LLM dissertation), University Of Essex, 2013

YILMAZ, Hasan, 2023, Nesnelerin İnterneti Cihazlarinin Güvenlik Boyutuyla İncelenmesi Ve Ülkemiz İçin Düzenleme Önerileri, Bilgi Teknolojileri ve İletişim Kurumu, Uzmanlık Tezi, Ankara

YU Peter K., 2004, The Origins of ccTLD Policymaking,nTexas A&M Law Scholarship, s.387-408, https://core.ac.uk/download/pdf/217217749.pdf (26.09.2023)

WEITZENBOECK Emily M., 2014,Hybrid net: the regulatory framework of ICANN and the DNS, International Journal of Law and Information Technology, Volume 22, Issue 1, s. 49–73, https://academic.oup.com/ijlit/article/22/1/49/697798, (10.10.2023)

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

02.07.2024

Burak EREN

ÖZGEÇMİŞ

1994 yılında Bursa'da doğdu. 2015 yılında Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi İktisat bölümünden mezun oldu. 2018 yılında askerlik görevini tamamladı. 2020 yılında göreve başladığı Bilgi Teknolojileri ve İletişim Kurumunun Bilgi Teknolojileri Dairesi Başkanlığında Bilişim Uzman Yardımcısı olarak çalışma hayatını sürdürmektedir.