T.C.
BİLGİ TEKNOLOJİLER VE İLETİŞİM KURUMU
Basın İle İlişkiler Müdürlüğü

28.04.2017

Konu: Ulusal Siber Olaylara Müdahale Merkezi (USOM)'dan Lokibotnet İsimli Zararlı Yazılıma Karşı Operasyon

Basın Açıklaması

SİBER ORDU BOTNETİ VURDU

BTK'dan Botnete Ağır Darbe

Bilgi Teknolojileri ve İletişim Kurumu bünyesinde çalışan Ulusal Siber Olaylara Müdahale Merkezi (USOM) özellikle Türkiye'deki akıllı telefon kullanıcılarını hedef alan LokiBotnet isimli zararlı yazılımın komuta kontrol sunucularına yönelik operasyon gerçekleştirdi. Komuta sunucularında tespit edilen vatandaşların telefon bilgilerini alan siber güvenlik uzmanları LokiBotnet'e ait komuta merkezlerini çökertti.

Android tabanlı cihazlara gönderilen SMS'lerde yer alan linkler üzerinden akıllı telefonlara yüklenen zararlı uygulama; kendisini bankacılık uygulaması veya çekilişle hediye kazandıran bir yazılım gibi gösteriyor. Zararlı yazılım farklı görünüm ve isimlerde vatandaşlara gönderilebiliyor. Zararlı yazılım, akıllı telefonlara bir defa bulaştıktan sonra, telefondaki rehberleri, SMS'leri saldırganların komuta sunucusuna gönderebiliyor, kullanıcının karşısına istediği anda herhangi bir bankanın internet bankacılığı sayfasının benzerini çıkarabiliyor.

Komuta Sunucuları Çökertildi

Bir banka ve söz konusu bankaya hizmet veren güvenlik firması tarafından iletilen ihbarlardan yola çıkan BTK siber güvenlik uzmanları, LokiBotnet siber saldırganlarının komuta kontrol sunucularında tespit ettikleri zafiyetten faydalanarak operasyonu genişletti. BTK uzmanları sistemlere sızdı ve şu ana kadar zararlı yazılım bulaştırılan cihazların listesini ele geçirdi. Operasyon sırasında ilk olarak zararlı uygulamanın bulaştırıldığı cihazlarla komuta sunucusu arasındaki iletişimi kesen BTK Türkiye'de bot haline getirilen cihazların komuta merkezinden emir almasının önüne geçti. Filmleri andıran operasyonda, sisteme sızıldığını fark eden saldırganlar erişimleri kapatmaya çalıştı. Zamana karşı yarışan USOM

uzmanları saldırganların sistemlerindeki gerekli bilgileri ele geçirdikten sonra, komuta sunucusundaki tüm bilgileri temizleyerek, komuta merkezini tamamen devre dışı bıraktı.

BTK Operasyon Sonuçlarını BDDK, Emniyet ve İlgili Kurumlara Gönderdi

Saldırganların kişilerin rehberlerinden yola çıkarak 27 binden fazla telefon numarasını ele geçirdiği tespit edildi. Ağırlıklı olarak Türkiye (%54) ve İran (%27) müşterilerine olmak üzere zararlı yazılımın toplamda 4116 adet cihaza bulaştırıldığını tespit eden BTK, bu verilerden yola çıkarak toplam 2512 standarda uygun IMEI üzerinden yaptığı incelemede zararlı yazılıma maruz kalan 1441 kişiye ulaştı. BTK, LokiBotnet'ten etkilenen cihazlar ve kişilerle birlikte, saldırganlarla ilgili bilgileri BDDK, Emniyet Genel Müdürlüğü ve ilgili kurumlarla paylaştı.

Bankalar Gerekli Önlemleri Aldı

Bankalar bu kapsamda gerekli önlemlerini aldı ve müşterilerine uyarılarını gerçekleştirdi. Alınan hızlı önlemler sayesinde şu ana kadar bazı EFT girişimleri engellenmiş ve bu çerçevede maddi zarara uğrayan bir vaka tespit edilmediği raporlanmıştır. Bu kapsamda bankaların izleyeceği ve önereceği tedbirlere uyması gereken müşterilerin sahte SMS ve dolandırıcılığa yönelik kendilerine gelen aramalara karşı da dikkatli olması gerekiyor.

Vatandaşların ne yapması gerekiyor?

- Bankanızdan aranıp bu konuda bilgilendirildiyseniz, size iletilen ve önerilen tedbirlere uymanız gerekmektedir, ancak dolandırıcıların sahte aramalarına dikkat edin,
- Bilinmeyen sitelerden uygulama indirmeyin,
- Eğer güvenilir olmayan yerlerden uygulama indirdiniz ve telefonunuzda zararlı uygulama varsa cihazınızı sıfırlayıp tüm kredi kartı ve parola bilgilerinizi güncelleyin
- Güvenilir uygulama marketlerinden İndirdiğiniz uygulamaların yetkilerine sınırlama getirin
- Kredi kartı parolası gibi kişisel hassas verilerinizi cihaz içerisinde (not olarak dahi) kayıtlı olarak tutmayın
    - Uygulama verileri, parola bilgileri ve diğer ayarların Google servislerinde depolanmasını kapatarak bilgilerininiz başka servisler ile paylaşılmasını engelleyin, (Ayarlar – Hesaplar – Yedekleme)
- Mobil cihazınızdaki tarayıcılarda parola bilgilerinizi kaydetmeyin ("Beni hatırla" seçili olduğu zaman kaldırın)

- Reklam önerilerini kapatın. Cihazınızda ‘ilgi alanına dayalı reklamcılık’ gibi önemli bir ayar vardır. Böylece uygulamalar lokasyon, cinsiyet, yaş gibi genel kişisel bilgilerinizi veya ziyaret ettiğiniz siteleri kullanabilirler. (Kapatmak için; Ayarlar – Google –Reklamlar)
- VPN yöntemleri kullanarak internete bağlanmayın. BTK zararlı bağlantıları ve komuta kontrol sunucularını engellemektedir, VPN kullanırsanız isteğiniz dışında zararlı bağlantılara erişebilirsiniz.