NETAS | Bilişim Teknolojileri

Siber Güvenlik Hizmetleri Direktörlüğü

TA505 Oltalama Kampanuası Vaka Analiz Önizlemesi

Sürüm 1.0

23/07/2019

Gizli Başlangıç Tarihi: 23 Temmuz 2019
Bitiş Tarihi: Devam Ediyor
Güvenlik Vakası: TA505 Türkiye Odaklı Oltalama Kampanyası Aktiviteleri
Vaka Tipi: Phishing

Netaş Bilişim Teknolojileri A.Ş.
Orhanlı Mah. İrfan Cad. No: 28
Tuzla / İstanbul

T: +90 216 522 58 74
F: +90 216 329 08 14
E: info@netasbilisim.com.tr

www.netasbilisim.com.tr

VAKA ÖNİZLEMESİ

Oltalama kampanyası, kişilere ait bilgilerin saldırganlar tarafından çalınabilmesi için tasarlanmış aldatmaca e-posta serisidir. Saldırganlar kampanya süresince hedef aldıkları kitleye, yaptıkları işlemlerin ve kimliklerinin güvenilir olduğunu hissettirerek kişilere ait kredi kartı ya da kişisel hassas bilgileri edinmeye çalışırlar.

Oltalama kampanyalarındaki ana yöntem güvenilir süsü verilen, saldırganlardan gelmekte olan güvenilir e-postalar olsa dahi, verilerin çalınması ve saldırganlar tarafından cihazların enfekte edilmesi aşamalarındaki yöntemler çeşitlilik göstermektedir. Vakaya konu olan zararlı Excel Office dökümanı ve Trojan.Jacard türü zararlı yazılımının kullanılması ise bu yöntemlerden ve saldırı vektörlerinden birkaç tanesine örnek olarak ortaya çıkmıştır.

Trojan zararlı yazılımları; enfekte ettikleri sistem üzerinde, saldırgana her türlü işlemi gerçekleştirme hakkı tanır. Özellikle sistem üzerinde bilgi toplama, klavye komutlarını takip etme ve kaydetme, cihazı ayrıca farklı zararlılarla da enfekte etme ve saldırgana uzaktan erişim sağlama işlemlerini gerçekleştirirler.

TA505 olarak adlandırılan tehdit aktörü, en az 4 yıldır dünya genelinde zararlı aktiviteler gerçekleştirdiği bilinen bir gruptur. Özellikle de meşhur Dridex bankacılık zararlı yazılımı ve Locky fidye yazılımı operasyonlarının ardında oldukları bilinmektedir. Saldırılarını Necurs olarak adlandırılan Bot ağı aracılığıyla gerçekleştirdikleri, yapılan araştırmalarda tespit edilmiştir. Sürekli değişen ve gelişen taktikleri sayesinde, güvenlik ürünlerinin radarına yakalanmadan aktivitelerini sürdürebilmektedirler.

Netaş Bilişim Teknolojileri A.Ş.
Orhanlı Mah. İrfan Cad. No: 28
Tuzla / İstanbul
T: +90 216 522 58 74
F: +90 216 329 08 14
E: info@netasbilisim.com.tr
www.netasbilisim.com.tr