Siber Tehditler 2019: Geçmiş Yıla Bir Bakış

Mart 2020

Tedarik zincirleri üzerinden saldırı:

Sürekli hedef odağı olanlar

Nitelikli saldırganlar için kurum ortaklıklarını ve üçüncü taraf tedarik zincirlerini sömürmek, belirgin bir eğilimdi:

- **Arka kapıları gizlemek** için dijital sertifikaları çalmak;
- Üçüncü taraf tedarikçi şirketler aracılığıyla **kötü niyetli trafiği yönlendirmek** (komuta ve kontrol sunucuları olarak kullanarak); ayrıca,
- Hedeflere erişim elde etmek ve tespit edilmekten kaçınmak amacıyla **zararlı yazılım yaymak** için üçüncü taraf tedarikçi ağlarına sızmak.

Özellikle Çin merkezli saldırganlar, üçüncü taraflara (kurum ortaklıkları, meşru tedarik zincirleri vs.) sağlanan güvenin ve ayrıcalıklı erişimin istismar edilmesine daha fazla odaklandı.

Olay incelemeleri

Olay incelemesi 1: Ele geçirilmiş uygulama güncellemeleri

2019'da keşfedilen bir olay; 2018'de birkaç ay boyunca ASUS'a sızılması, ele geçirilen servisler üzerinden kullanıcılara zararlı yazılım içeren güncellemelerinin iletilmesi ile sonuçlandı.

Olay incelemesi 2: Sertifikalı!

Kuzey Kore merkezli "Black Artemis" lakaplı saldırgan, zararlı yazılımlarını imzalamak ve anti-virus kontrollerini atlatmak amacıyla gerekli sertifikaları çalmak için İngiltere bazlı meşru şirketlerin kılığına girdi.

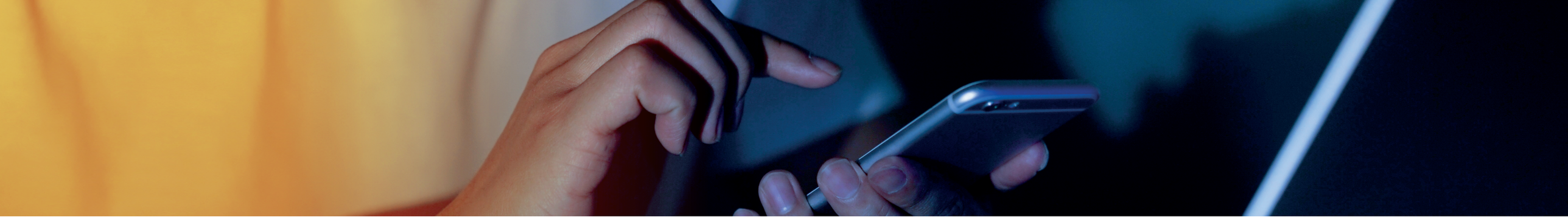
Olay incelemesi 3: Winnti topluluğu

Winnti arka kapısına erişimi olan Çin merkezli saldırganlar birden fazla tedarik zinciri saldırısıyla ilişkilendirildi.

2019 Mayıs itibariyle, telekomünikasyon servis sağlayıcılarından hava yollarına kadar çeşitli sektörlerden 23 ülke üzerinde 150 ele geçirilmiş yapı tespit ettik.

Bu grafik, siber saldırgan Winnti topluluğu tarafından hedeflenen sektörleri en çok hedeflenen sırada görüntülemektedir.

- Teknoloji ve Telekomünikasyon
- Dini / Muhalif Organizasyonlar
- İmalat Sektörü
- Devlet ve Halka Açık Sektörler
- Ulaşım ve Lojistik
- Eğlence ve Medya
- Eğitim



Mobil tehditler:

2019'un en popüler trendi: **hem suç hem de casusluk** amacı güden saldırganlar, dikkatlerini mobil platformlardaki zararlı yazılımların ve truva atlı mobil uygulamaların yanı sıra telekomünikasyon ağlarının geniş çapta sömürülmesine yöneltti.

Bütün mesajlarınızı okumayı umuyorum

2019'da, casusluk amacı güden bir saldırgan, telekomünikasyon sağlayıcılarını ele geçirdi ve bu sistemlere SMS mesajlarını gerçek zamanlı olarak izleyebilmek için zararlı yazılım yükledi. Bu olay, hedefler üzerinde kitlesel ölçekte bilgi edinme gücü sağladı.

2FA Tehlikeleri

Şubat 2019'da, siber saldırganlar Metro Bankasını hedefleyen bir saldırıda çevrimiçi bankacılık ve e-ticaret sistemleri için kullanılan SMS bazlı 2FA çözümlerini hedefleyen teknikler geliştirdiklerini göstermiş oldular.

Siber suç sahnesi: fidye yazılımı

Siber saldırganlar gelir çeşitliliği aradılar; POS cihazlarını hedefleyen zararlı yazılımlar yazmakla bilinen saldırganlar bu sefer e-ticaret platformlarına saldırmaya başlarken, diğerleri fidye yazılımlarına yönelmeyi tercih etti.

Fidye yazılımı tehditleri 2019'da yoğunlaşıyor

Son 12 ayda çeşitli kurbanları ve sektörleri etkileyen başarılı ve üst düzey fidye yazılımı saldırıları gözlemlendi.

Hedef odaklı saldırılara önem veren fidye yazılımı saldırılarının büyük ölçekli yaygınlaşmasının **şiddetinde ve sıklığında** kayda değer bir artış oldu.

> DDOS hizmetleri için saldrganların fiyatlandırması, saldırı süresine göre değişir ve "etkili saldırılar" sunan hizmetler saatte 10 ABD doları saldırganlar tarafından sunulmaktadır.

Büyüme gözlemleniyor

- DDoS saldırıları, diğer siber operasyonların arka planında paralel bir eğimde yaşanmaya devam etti.
- Saldırganlar saldırıları güçlendirmek ve DDoS önlemlerini aşmak için yeni teknikler geliştirdi.
- İnternete bağlı cihazların yaygınlaşmasının kolaylaşmasıyla daha geniş çapta botnet yapılarının oluşturulması da basitleşti.
- Siber suç ekosistemi de botnet oluşturma işlemlerinden para kazanmak için DDoS saldırı hizmetleri sunmaya yöneldi.

2020-0054