**BASIN BÜLTENİ**

**Siber saldırganlar yakalanmamak için atlatma ve anti analiz tekniklerine yöneliyor**

**Fortinet Tehdit Görünümü Endeksi’ne göre artarak devam eden siber saldırı teşebbüsleri bugüne kadarki en yüksek seviyeye ulaştı.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), çeyrekten çeyreğe yayınladığı Global Tehdit Görünümü Raporu’nun son bulgularını duyurdu.

* Araştırma, siber suçluların dijital saldırı yüzeyi boyunca yeni saldırı fırsatları aramaya devam ettiklerini ve saldırılarını daha sofistike hale getirdikçe atlatma ve anti-analiz tekniklerinden faydalandıklarını ortaya koyuyor.
* Tehdit Görünümü Endeksi, bu çeyrekte bir dönüm noktası yaşadı. Endeks, yıldan yıla orijinal başlangıç seviyesinin neredeyse yüzde 4 üzerine çıktı. Yıllık zaman dilimindeki yükseliş zirve yaptı ve 2019 takvim yılı ikinci çeyreğinin kapanış noktasına ulaştı. Bu ani ve hızlı artışta artan zararlı yazılım ve istismar vakaları etkili oldu.

Fortinet Tehdit Görünümü Raporu’nun öne çıkan bulguları ise şöyle:

**Siber saldırganlar atlatma taktiklerinde eli yükseltiyor**

Pek çok modern zararlı yazılım araçları, halihazırda virüs koruma programından kaçan virüsleri veya diğer tehdit tespit uygulamalarını içeriyor; ancak, siber saldırganlar, gizlenme ve tespit edilmeden kaçınma için uyguladıkları anti-analiz pratiklerinde giderek daha sofistike hale geliyor.

Örneğin, bir spam [kampan](https://www.fortinet.com/blog/threat-research/excel-variable-targeting-japanese-users.html)yası siber saldırganların bu teknikleri savunma sistemlerine karşı nasıl kullandıklarını ve kendilerine göre nasıl uyarladıklarını gösteriyor. Saldırı kampanyası zararlı bir makroya dönüşerek silah haline gelen bir Excel dokümanıyla ekli olarak gelen bir oltalama (phishing) e-postasının kullanımını içeriyor. Excel’deki makro yapısının güvenlik araçlarını devreden çıkaracak, talimatları gelişigüzel yerine getirecek, bellek sorunlarına yol açacak özelliklerle tasarlandı ve yalnızca Japon sistemleri üzerinde çalışması sağlandı. Saldırının bilhassa aradığı bir özellik olan bir xlDate değişkeni ise belgelenmemiş gibi görünüyor.

Diğer bir örnek olan Dridex bankacılık truva atının varyantı ise, saldırının kurbanı her oturum açtığında dosyaların adını değiştirerek ve bozarak virüsün bulaştığı ana sistem üzerinde zararlı yazılımın tespit edilmesini zorlaştırıyor.

Anti-analiz ve gelişmiş atlatma taktiklerinin artan kullanımı çok katmanlı savunma ve davranış temelli tehdit tespitine yönelik ihtiyacı bir kez daha hatırlatıyor.

**Çok iyi gizlenen saldırılar uzun vadeli olmayı amaçlıyor**

Bilgi çalan Zegost zararlı yazılımı, [kişiye özel oltalama kampanyalarında](https://www.fortinet.com/blog/threat-research/zegost-campaign-targets-internal-interests.html) bir dönüm noktası teşkil ediyor ve karmaşık yapıda teknikler kullanıyor. Tıpkı bilgi çalmayı amaçlayan diğer zararlı yazılımlar gibi Zegost’un da asıl amacı kurbanın cihazına ait bilgi toplamak ve bunları ele geçirmek. Ancak, bilgi çalmayı hedefleyen diğer yazılımlarla karşılaştırıldığında, Zegost, benzersiz bir şekilde fark edilmemek üzere yapılandırıldı. Örneğin, Zegost olay kayıtlarını temizlemek için tasarlanan bir işlevselliğe sahip. Tipik zararlı yazılımlarda, bu türden bir temizleme özelliği görülmüyor. Zegost’un atlatma yeteneklerindeki ilginç gelişmelerden biri de bulaşma rutinini başlatmasının ardından 14 Şubat 2019’a kadar bilgi çalma özelliğini “hareketsiz” tutan bir komuta sahip olmasıydı.

Zegost’un ardındaki tehdit aktörleri, onu benzerlerine kıyasla daha uzun süreli bir tehdit haline getirerek, hedeflenen kurbanlarla bir bağlantı kurduğunu ve sürdürdüğünü garantilemek için bir dizi istismardan faydalanıyor.

**Fidye yazılımlar daha hedef odaklı saldırı eğilimini sürdürüyor**

Çeşitli şehirlere, yerel yönetimlere ve eğitim sistemlerine yönelik saldırılar, fidye yazılımların ortadan kaybolmadığına, aksine büyüyen pek çok kuruma yönelik ciddi bir tehdit oluşturmaya devam ettiğine dair bir hatırlatma görevi görüyor. Fidye yazılım saldırıları, kitlesel, rastgele saldırılardan, fidye ödemeye eğilimli ya da fidye ödeyebilecek durumda olduğu düşünülen kurumlara yönelik daha hedef odaklı saldırılar haline geliyor. Bazı vakalarda, siber suçlular, fırsattan en iyi şekilde istifade etmek için dikkatlice belirledikleri sistemlere fidye yazılım kurulumunu yapmadan önce ciddi bir ön araştırma yürütüyor.

Örneğin, kurumun ağ altyapısına saldırmak için tasarlanan RobbinHood fidye yazılımı, veri şifrelemeyi engelleyen Windows hizmetlerini devre dışı bırakabiliyor, paylaşımlı sürücülerle olan bağlantıları koparabiliyor.

Sodinokibi adlı bir başka fidye yazılım da kurumlar için ciddi bir tehdit oluşturabiliyor. İşleyiş anlamında, kullanımda olan fidye yazılımların büyük bir kısmından farklılaşmıyor. Sodinokibi, gelişigüzel kod işletimine imkân tanıyan yeni bir zafiyeti istismar eden ve oltalama e-postasıyla kullanıcıya iletilen diğer fidye yazılımların aksine herhangi bir kullanıcı etkileşimi gerektirmeyen bir saldırı vektörü nedeniyle sorun yaratıyor.

Vektörden bağımsız olarak, fidye yazılımlar gelişen kurumlar için ciddi bir tehdit oluşturmaya devam etmesi, yamalamanın önceliklendirilmesi ve bilgi güvenliği farkındalık eğitiminin önemine dair bir hatırlatma görevi görüyor. Bunun yanı sıra, [BlueKeep](https://www.fortinet.com/blog/threat-research/cve-20190708-remote-desktop-protocol-and-code-execution-bluekeep.html) gibi uzaktan Masaüstü Protokolü (Remote Desktop Protocol-RDP) zafiyetleri, uzaktan erişim hizmetlerinin siber saldırganlar için bir fırsat teşkil ettiğini ve fidye yazılımları yaymak için bir saldırı vektörü olarak da kullanılabileceklerine dair bir uyarı niteliği taşıyor.

**Dijital saldırı yüzeyinde yeni fırsatlar**

Evdeki yazıcılar ve kritik altyapılar arasındaki grafik, evde ya da küçük ölçekli işletmelerde kullanılan kontrol sistemleri konusunda artan bir seyir gösteriyor. Bu akıllı sistemler, endüstriyel versiyonlarına kıyasla siber saldırganların daha az dikkatini çekse de bu durum çevresel kontrol, güvenlik kameraları ve emniyet sistemleri gibi kontrol cihazlarını hedef alan saldırı aktivitelerindeki artışa bağlı olarak değişebilir. Yönetim çözümleri geliştirmeye yönelik bir bulgunun kurumların yalnızca yüzde 1’inde görüldüğü tespit ediliyor. Bu, her ne kadar küçük bir oran gibi görünse de ICS ve SCADA ürünlerinde olağan olarak değerlendirilen rakamın üzerinde kalıyor.

Siber suçlular ev ve işyerlerindeki kontrol cihazlarını ele geçirmenin yeni yollarını arıyor. Bazen bu cihazlar, diğerleri kadar önceliklendirilmiyor ya da geleneksel BT yönetimi kapsamının dışında tutuluyor. Evlerde kullanılan akıllı cihazlar ve küçük işletmelerin sistemlerinin güvenliğine, bu cihazlara erişimin ciddi güvenlik sonuçları yaratabileceği sebebiyle, bilhassa özen gösterilmesi gerekiyor. Bu, güvenli erişimin çok önemli olduğu uzaktan çalışma ortamları için de geçerlidir.

**Kurumunuzu siber saldırılara karşı korumanın yolu kapsamlı, entegre ve otomatik güvenlikten geçiyor**

Dinamik, proaktif ve gerçek zamanlı tehdit analizi dijital saldırı yüzeyini hedef alan saldırı yöntemlerinin evrimleşmesini gösteren trendlerin tespit edilmesine ve siber hijyen önceliklerinin belirlenmesine yardımcı olabilir. Tehdit istihbaratı her bir güvenlik cihazında gerçek zamanlı olarak uygulanmazsa tehdit istihbaratına göre aksiyon alabilme becerisi ve önemi ciddi oranda azalıyor. Yalnızca kapsamlı, entegre ve otomatik bir yapıda olan “security fabric” mimarisi nesnelerin internetinden uca, ağ çekirdeğine ve çoklu bulutlara kadar ağa bağlantılı tüm ortamda hızlı ve ölçeklenebilir koruma sağlayabiliyor.

**Rapor ve endekse dair genel bilgi**

Fortinet Küresel Tehdit Raporu her çeyrekte yayınlanan ve FortiGuard Laboratuvarlarının Fortinet'in geniş çaplı global sensörlerinden elde ettiği 2019 yılının 2. Çeyreğine ait kolektif istihbarat bilgilerini yansıtan bir raporudur. Araştırma verileri küresel ve bölgesel perspektifleri kapsar. Raporda bu görünümün merkezi ve tamamlayıcı yönleri olan istismarlar, zararlı yazılımlar, botnetlerin bu çeyrekteki yaygınlığını ve hacmini gösteren Fortinet Tehdit Görünümü Endeksi (TLI) de yer alır.

**Ek kaynaklar**

* Bu araştırma hakkında daha fazla bilgi almak ve raporun tamamına erişmek için [blog](https://www.fortinet.com/blog/threat-research/fortinet-q2-2019-threat-landscape-report.html) sayfamızı inceleyebilirsiniz.
* 2019'un ikinci çeyreğiyle ilgili botnet, zararlı yazılımlar ve saldırılara yönelik Fortinet Tehdit Görünüm Endeksini [inceleyebilirsiniz.](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta)
* Değişen tehditler ve her hafta Fortinet Tehdit Görünümü Endeksi’ne dahil olan eylemler için Haftalık [FortiGuard Tehdit İstihbaratı Özetleri'ne](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta) göz atabilirsiniz.
* [FortiGuard Laboratuvarları](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta) ve FortiGuard Güvenlik Hizmetleri [portföyü](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services) hakkında bilgi almak için tıklayın.
* Güvenlik denetimleri ve en iyi uygulamaların görebileceğiniz [FortiGuard Security Rating Service](https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/security-rating.html?utm_source=blog&utm_campaign=2018-blog-security-rating-service) bağlantısına tıklayabilirsiniz.
* [Network Security Expert program](https://www.fortinet.com/support-and-training/training/network-security-expert-program/nse-1.html?utm_source=blog&utm_campaign=2018-q2-nse-training), [Network Security Academy program](https://www.fortinet.com/support-and-training/training/fortinet-network-security-academy.html?utm_source=blog&utm_campaign=2018-fnsa-program) ve [FortiVets program](https://www.fortinet.com/corporate/careers/vets.html?utm_source=blog&utm_campaign=2018-q2-fortivet) hakkında bilgi almak için bağlantılara tıklayabilirsiniz.
* [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric) hakkında ayrıntılı bilgi için bağlantıya tıklayabilirsiniz.
* Fortinet’i [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet%22%20%5Ct%20%22_blank), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/fortinet) ve [Instagram](https://www.instagram.com/behindthefirewall/)’dan takip edebilirsiniz.

**İlgili Kişi:**
Eray Çoşan Akkuş
Marjinal Porter Novelli
0 533 927 23 97
erayc@marjinal.com.tr

**Fortinet Hakkında**
Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet'in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 415 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: [http://www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://fortiguard.com/).