**Siber Saldırganlar Kurumları Hazırlıksız Yakalamak için Eski Yöntemleri Kullanıyor**

*Fortinet Tehdit Görünümü Raporu, Siber Suçluların Halka Açık Hizmetlere Kod Eklemek ve Çalıştırmak için Popüler Oltalama Yönteminden Uzaklaştığını Gösteriyor.*

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), çeyreklik olarak hazırlanan en yeni  [Tehdit Görünümü Raporu](https://www.fortinet.com/resources/resources-campaign.html?utm_source=direct&utm_medium=asset-video&campaign=power-of&utm_term=q3fy19tlr#ufh-i-503778344-quarterly-threat-landscape-report)’na ait bulgularını duyurdu.

* Araştırma, siber suçluların dijital saldırı zemininde yeni saldırı fırsatları aramaya devam ettiğini açığa çıkarıyor. Siber suçlular, aynı zamanda halka açık sınır hizmetlerini hedef almak gibi saldırı vektörlerini de şirketlerin oltalama gibi popüler yöntemlere karşı geliştirdiği alıştırma ve eğitim fırsatlarını baltalamak gibi yeni yaklaşımlarla değiştiriyor.
* Tehdit Görünüm Endeksi çeyrek boyunca nispeten sabit kaldı. Bazı dalgalanmalar olsa da önemli artışlar yaşanmadı. Yine de kurumların kalkanlarını indirmemesi gerekiyor. Çünkü endeks göstergeleri aynı zamanda tutarlı ve devam eden bir siber saldırı aktivitesine işaret ediyor.
* Tehdit Görünümü Endeksi ve açıklar, kötü amaçlı yazılımlar ve botnet altdizinlerinin yanı sıra bazı önemli konu başlıkları [blogda](https://www.fortinet.com/blog/threat-research/fortinet-q3-threat-landscape-report.html) yer alıyor.

**Fortinet Tehtid Görünümü raporunda öne çıkan bulgular şöyle:**

**Kurumları Hazırlıksız Yakalamak için Yöntem Değiştiriyorlar:** Kötü amaçlı yazılımların büyük çoğunluğu e-posta ile gönderiliyor. Bu yüzden birçok kurum oltalama saldırılarına karşı kendilerini son kullanıcı eğitimleri ve gelişmiş e-posta güvenlik çözümleriyle hazırlıyor. Siber suçlular da bu yüzden kötü amaçlı yazılımlarını aktarabilmek için başka yöntemlere başvuruyor. Geleneksel oltalama yöntemlerini kullanmadan yeni saldırı alanları açacak bu yöntemler arasında web altyapısı, ağ iletişim protokolü reklam engelleyici araçları atlayarak yeni saldırı vektörleriyle halka açık sınır hizmetleri hedef almak yer alıyor. Örnekle açıklamak gerekirse bu çeyrekte FortiGuard Laboratuvarları, tüm bölgelerde sınır hizmetleri hedefleyen bir kodun uzaktan çalıştırılmasına izin veren bir zafiyetin kullanıldığı saldırılarla karşılaştı. Bu yöntem yeni olmasa da sistem yöneticilerinin yakından takip etmediği bir alandan saldırmak, kurumları hazırlıksız yakalayıp, saldırının başarılı olma ihtimalini artırabilir. Bu durum özellikle online hizmet aktivitesinin artmasının beklendiği online alışveriş dönemlerinin öncesinde sorun yaratabilir.

**Gelir Potansiyelini En Yükseğe Çıkartıyorlar:** Dark web’de Hizmet olarak Fidye Yazılımı (RaaS) çözümü olarak erişime açılan [GandCrab fidye yazılımını](https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html) kullanan siber suç kurumları, gelir potansiyelini artırmak için yeni hizmetleri erişime açıyor. Siber suçlular, bağlı iş ortaklarından bir ağ oluşturarak fidye yazılımlarını daha geniş kitlelere iletebiliyor ve bu süreçte gelirlerini gözle görülür derecede artırabiliyor. FortiGuard Labs, RaaS çözümü olarak hizmete alınan Sodinokibi ve Nemty isimli iki önemli fidye yazılımı ailesini gözlemliyor. Bu yazılımlar, gelecekte benzer hizmetlerin geliştirilmesine zemin hazırlayabilir.

**Başarı için Fidye Yazılımını Geliştiriyorlar:** Tespit edilmekten kaçınmak için, daha sofistike ve kötü amaçlı yazılımlarını geliştiren siber suçlu sayısı giderek artıyor. Emotet kötü amaçlı yazılımının evrimi bunun bir örneği. Siber suçluların sızdıkları sistemlere veri yükü bindirmek ve finansal gelirlerini artırmak için kötü amaçlı yazılımları daha sık kullanmaya başlaması, kurumlar için endişe verici bir durum. Yakın zamanda saldırganlar, Emotet’i fidye yazılımları, bilgi hırsızları ve TrickBot, IcedID ve Zeus Panda gibi banka trojanları için veri yükü ulaştırma mekanizması olarak kullanmaya başladı. Tüm bunlara ek olarak, saldırganlar e-posta dizisini güvenli kaynaklardan ele geçirerek ve o e-posta dizinine kötü amaçlı yazılımı yerleştirerek zararlı eklentilerin açılma ihtimalini gözle görülür derecede artırıyor.

**Eski Zafiyetlerle ve Botnetlerle Fırsatlar Artırılıyor:** Doğru şekilde emniyete alınmamış eski ve korunmasız sistemleri hedef almak hala etkili saldırı stratejileri arasında yer alıyor. FortiGuard Labs, siber suçluların yeni saldırılara kıyasla 12 yıldır veya daha uzun süredir var olan zafiyetleri daha sık hedef aldığını açığa çıkardı. Aslına bakılırsa, her sene bir önceki yılın zayıf ve savunmasız noktalarına saldırma oranları, yeni açıklara saldırma oranlarıyla aynı.

Benzer şekilde mevcut fırsatı artırma trendi botnetlerle de görülüyor. Diğer tehdit türleriyle kıyaslandığında daha sık görülen botnetlerin en tehlikelileri, dünya çapında her çeyrekte ve her bölgede ufak farklılıklarla popülerliğini koruyor. Bu da kontrol altyapısının belli araçlar ve yeteneklerle karşılaştırıldığında daha kalıcı bir çözüm olduğunu gösteriyor. Siber suçlular sadece yeni fırsatları değil, aynı zamanda yasal işletmeler gibi verimliliği artırmak ve işletim yükünü hafifletmek için mümkün olan her fırsatta [mevcut altyapılarını](https://www.fortinet.com/blog/threat-research/cyber-adversaries-flock-to-apps-where-the-users-are-and-when-use.html) geliştiriyorlar.

**Beklenmeyeni Korumak: Geniş, Entegre ve Otomatikleştirilmiş Koruma**

Siber suçluların genişleyen saldırı zemini ve dönüşüme uğrayan saldırı stratejileri, kurumların en ufak tehdit dizisini görmezden gelemeyeceği anlamına geliyor. Kurumların ayrık ve ağ tabanlı ortamlarını korumak için bütüncül bir yaklaşım benimsemesi çok önemli. Bu da geniş, entegre ve otomatikleştirilmiş bir [güvenlik yapısının](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric) hizmete alınmasını gerektiriyor. Bu yaklaşım, kurumların entegre cihazlarda geniş görünürlükle genişleyen saldırı zeminini küçültmelerini ve yönetmelerini, yapay zekadan güç alan ihlal engellemeyle gelişmiş tehditleri durdurmalarını ve otomatikleştirilmiş operasyon ve orkestrasyon ile karmaşıklığı azaltmalarını sağlıyor. Ek olarak dinamik, proaktif ve gerçek zamanda erişilebilir tehdit istihbaratı, dijital saldırı zeminini hedef alan saldırı yöntemlerinin dönüşümünü takip ederek trendlerin ve siber hijyen önceliklerinin belirlenmesinde kilit role sahip.

**Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz raporun bulgularını şöyle değerlendirdi:**

“Siber suçlular, siber güvenlik profesyonellerinin bir adım önünde olmak için çalışmaya devam ediyor. Yeni kötü amaçlı yazılım ve sıfırıncı gün saldırıları geliştiren siber saldırganlar, saldırı zemini üzerindeki fırsatları artırmak için daha önce başarılı olmuş yöntemleri yeniden kullanıyor. Kurumların yamalama, bölme ve eğitim gibi temel stratejilerin yanı sıra tehdit istihbaratıyla ilişkilendirme ve tehditlere gerçek zamanlı karşılık verme gibi yeteneklerini iyileştirmek için otomasyon ve yapay zekayı da benimsemesi gerekiyor. Ancak bu strateji, yalnızca kurumlar bütün güvenlik kaynaklarını hızlıca genişleyen ağı görebilen ve ayak uydurabilen güvenlik yapısına entegre ederse başarılı olabilir.”

**Rapor ve endekse dair genel bilgi**

Fortinet Küresel Tehdit Raporu her çeyrekte yayınlanan ve [FortiGuars Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta)’in Fortinet'in geniş çaplı global sensörlerinden elde ettiği 2019 yılının 3. Çeyreğe 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 düşüşünü 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 sayfamızı inceleyebilirsiniz.
* 2019'un üçüncü çeyreğiyle ilgili botnet, zararlı yazılımlar ve saldırılara yönelik Fortinet Tehdit Görünüm Endeksini [inceleyebilirsiniz](https://www.fortinet.com/resources/resources-campaign.html?utm_source=direct&utm_medium=asset-video&campaign=power-of&utm_term=q3fy19tlr#ufh-i-503778344-quarterly-threat-landscape-report) veya raporun tamamına [erişebilirsiniz](https://www.fortinet.com/resources/resources-campaign.html?utm_source=direct&utm_medium=asset-video&campaign=power-of&utm_term=q3fy19tlr#ufh-i-503778344-quarterly-threat-landscape-report).
* FortiGuard Laboratuvarları ekibinin oluşturduğu en yeni Adversary Playbook – Emotent’i buradan [görüntüleyebilir ve okuyabilirsiniz](https://www.fortinet.com/blog/threat-research/emotet-playbook-banking-trojan.html).
* Değişen tehditler ve her hafta Fortinet Tehdit Görünümü Endeksi’ne dahil olan eylemler için Haftalık FortiGuard [Tehdit İstihbaratı Özetleri](https://fortiguard.com/resources/threat-brief)'ne 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-and-training/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-and-training/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/training/network-security-expert-program.html?utm_source=blog&utm_campaign=2019-q2-nse-landing), [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), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/fortinet) ve [Instagram](https://www.instagram.com/behindthefirewall/)’dan takip edebilirsiniz.

**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 425 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: <http://www.fortinet.com/>, [Fortinet Blog sayfası](https://blog.fortinet.com/) veya [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta).