**Fortinet, Fidye Yazılımlarında 10 Kat Artış Gözlemliyor**

*Kamu ve özel sektör, attığı adımlarla siber suçluların tedarik zincirlerini bozmaya devam ediyor.*

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet®, yılda iki kere paylaştığı [FortiGuard Labs Küresel Tehdit Zemini Raporu](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2021-threat%20landscape.pdf)’nun en yeni bulgularını paylaştı. 2021'in ilk yarısında elde edilen tehdit istihbaratı, bireyleri, kuruluşları ve giderek daha kritik hale gelen altyapıyı hedef alan saldırıların hacminde ve gelişiminde önemli bir artış olduğunu gösteriyor. Geleneksel ağın içinde ve dışında hibrit çalışanların ve öğrencilerin genişleyen saldırı yüzeyi hedef olmaya devam ediyor. Kolluk kuvvetlerinin yanı sıra kamu ve özel sektör arasında zamanında gerçekleştirilen işbirliği ve ortaklıklar, 2021'in ikinci yarısına girerken siber suç ekosistemini bozmak için önemli bir fırsat sunuyor. Raporun ayrıntılı bir görünümü ve bazı önemli bulgular [blog](https://www.fortinet.com/blog/industry-trends/fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware?utm_source=pr&utm_campaign=fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware)da yer alırken 2021’in birinci yarısındaki verilerden oluşturulan raporunun öne çıkan başlıkları da aşağıda bulunuyor:

**1) Fidye Yazılımı Paradan Daha Fazlasını Kaybettiriyor:** FortiGuard Labs verileri, fidye yazılımlarının Haziran 2021'deki haftalık ortalama etkinliğinin önceki yıla kıyasla on kattan fazla olduğunu gösteriyor. Bu veri aynı zamanda bir yıl boyunca tutarlı ve genel olarak istikrarlı bir artış olduğunu da gözler önüne seriyor. Saldırılar, özellikle kritik öneme sahip sektörler olmak üzere birçok kuruluşun tedarik zincirlerini işlemeyecek hale getirdi ve günlük yaşamı, verimliliği ve ticareti her zamankinden daha fazla etkiledi. En çok hedef alınan şirketler telekomünikasyon sektöründe yer alırken, telekomünikasyon sektörünü de kamu, yönetilen güvenlik hizmeti sağlayıcıları, otomotiv ve imalat sektörleri takip ediyor. Buna ek olarak, bazı fidye yazılımı operatörleri, stratejilerini e-postadan bulaşan dosyalar yerine kurumsal ağlara ilk erişimi elde etme ve satma üzerine oluşturmaya başladı. Bu değişim, siber suçları güçlendiren Hizmet olarak Fidye Yazılımı (RaaS) ürünlerinin gelişmeye devam ettiğini gösteriyor. [Fidye yazılımları](https://www.fortinet.com/blog/ciso-collective/ciso-guide-your-checklist-to-follow-in-the-mist-of-ransomware-attack?utm_source=pr&utm_campaign=ciso-guide-your-checklist-to-follow-in-the-mist-of-ransomware-attack) bulunduğu sektörden veya büyüklüğünden bağımsız olarak tüm şirketler için gerçek bir tehlike olmaya devam ediyor. Şirketlerin [sıfır güven erişim](https://www.fortinet.com/solutions/enterprise-midsize-business/network-access?utm_source=pr&utm_campaign=network-access) yaklaşımının, ağ segmentasyonunun ve şifrelemenin yanı sıra güvenli ortamlara yönelik gerçek zamanlı uç nokta koruması, tespit etme ve otomatik yanıt çözümleriyle proaktif bir yaklaşım benimsemesi gerekiyor.

**2) Dört Şirketten Birisi Kötü Amaçlı Reklam Tespit Etti:** En çok görülen fidye yazılımlarına bakıldığında aldatıcı sosyal mühendislik ile geliştirilen kötü amaçlı reklamcılık ve kullanıcıyı korkutan yazılımlarda bir artış olduğu görülüyor. Şirketlerin yüzde 25’inden fazlası, kötü amaçlı reklam veya korkutma denemeleri tespit etti. Bu da Cryxos'u dikkat edilmesi gereken bir kötü amaçlı yazılım ailesi yapıyor. Bununla birlikte verilerin büyük bir kısmı, büyük olasılıkla kötü amaçlı reklamcılık olarak değerlendirilebilecek diğer benzer JavaScript çalışmalarıyla destekleniyor. Korkutmaya ek olarak gasp etmeyi de hedefleyen siber suçlular, hibrit çalışma yöntemlerinden yararlanabileceği yollar aradığı için şirketlerin bu yöndeki tercihi, siber saldırganların taktiklerdeki bu trende net bir şekilde güç veriyor. Siber güvenlik bilincinin artması, korkutma ve kötü amaçlı reklam taktiklerinin başarılı olmasını engellediği için zamanında eğitim imkanı sağlamak, her zaman olduğu gibi çok önemli.

**3) Botnet Trendleri Saldırganların Sınıra Yöneldiğini Gösteriyor:** Tespit edilen botnetlerin yaygınlığına bakıldığında bu cihazların aktivitelerinde artış yaşandığı görülüyor. Yılın başında botnet etkinliği tespit eden şirketlerin oranı yüzde 35 olurken, altı ay sonra bu oran yüzde 51’e yükseldi. Haziran ayında botnet etkinliğindeki genel artışın arkasında TrickBot’un etkinliğindeki büyük artış yer alıyor. TrickBot başlangıçta siber suç sahnesinde bir bankacılık truva atı olarak ortaya çıktı ancak o zamandan beri birçok yasa dışı faaliyeti destekleyen karmaşık ve çok aşamalı bir araç setine dönüştürüldü. Genel olarak en yaygını olan Mirai ise 2020'nin başlarında Gh0st'ı geride bıraktı ve 2021'e kadar hüküm sürdü. Zaman içinde Mirai’ye siber saldırganlara güç verecek yeni özellikler eklenmeye devam etti. Mirai'nin hakimiyetinin bir kısmında evden çalışan veya eğitimine evden devam eden kişiler tarafından kullanılan Nesnelerin İnterneti (IoT) cihazlarından yararlanmaya çalışan siber suçlular büyük rol oynamış olabilir. Saldırganların virüslü sistemin kontrolünü tam olarak ele geçirmesine, canlı web kamerası görüntülerini ve mikrofondan çıkan sesleri kaydetmesine veya dosya indirmesine izin veren bir uzaktan erişim botneti olan Gh0st da gözle görülür derecede aktif. Uzaktan çalışma ve öğrenme alanlarındaki değişimlerinin üzerinden geçen bir yıldan uzun süre boyunca siber saldırganlar, fırsatlardan yararlanmak için kullanıcıların günlük alışkanlıkları hedeflemeye devam ediyor. Ağları ve uygulamaları korumak için şirketler, IoT uç noktasına ve ağa giren cihazlara karşı en düşük erişim imkanını sağlamak için sıfır güven erişim yaklaşımlarına ihtiyaç duyuyor.

**4) Siber Suçların Engellenmesi, Tehdit Hacimlerinin Düşmesini Sağlıyor:** Siber güvenlikte her eylem anında veya kalıcı bir etkisi sunmuyor ancak 2021'deki bazı olaylar özellikle sistemi savunanlar için olumlu gelişmeler sağlıyor. TrickBot'un orijinal geliştiricisi, haziran ayında birden fazla suçlamayla yargılandı. Ayrıca yakın tarihin en verimli kötü amaçlı yazılım operasyonlarından biri olan Emotet'in koordineli olarak kaldırılması ve Egregor, NetWalker ve Cl0p fidye yazılımı operasyonlarını bozmaya yönelik atılan adımlar, siber suçları engellemek için devletlerin küresel çalışmalarını ve kolluk kuvvetleri de dahil olmak üzere siber saldırganlara karşı mücadele veren ekiplerin başarısını gösteriyor. Ek olarak bazı operasyonların yarattığı etki, birçok fidye yazılımı operatörünün operasyonlarını durdurmasını sağladı. FortiGuard Labs'ın verileri, Emotet'in kaldırılmasının ardından tehdit etkinliğinin azaldığını gösterdi. Emotet botnet, çevrimdışı olduktan sonra TrickBot ve Ryuk varyantlarının etkinliği devam etti ancak hacmi azaldı. Siber tehditleri veya siber saldırganların tedarik zincirlerini hemen ortadan kaldırmak zor olsa da bu operasyonlar son derece büyük başarılarla sonuçlandı.

**5) Sistem Yöneticilerinden Savunma Amaçlı Kaçınma ve Sistem İçinde Sahip Olunan Ayrıcalıkları Artırma Teknikleri Siber Suçlular Tarafından Tercih Ediliyor:** Daha kapsamlı tehdit istihbaratı incelendiğinde saldırı tekniklerinin şu anda nasıl geliştiğine dair değerli bulgular ortaya çıkıyor. FortiGuard Labs, siber saldırganların neyi amaçladığını gözlemlemek için örnekleri inceleyerek tespit edilen kötü amaçlı yazılıma özgü belirli özellikleri [analiz etti](https://www.fortinet.com/blog/industry-trends/fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware?utm_source=pr&utm_campaign=fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware). Ortaya da saldırıda kullanılan dosyalar hedef ortamlarda çalıştırılsaydı kötü amaçlı yazılımın başarabileceği olumsuz sonuçların listesi çıktı. Bu liste, siber saldırganların diğer tekniklerin yanı sıra sahip olduğu ayrıcalıkları artırmaya, savunmalardan kaçınmaya, dahili sistemler arasında hareket etmeye ve güvenliği ihlal edilmiş verileri sızdırmaya çalıştığını gösteriyor. Örneğin, gözlemlenen ayrıcalık yükseltme çalışmalarının yüzde 55'inde yönlendirme (hooking) yöntemi, yüzde 40'ında da işlem enjeksiyonu (process injection) yöntemi kullanıldı. Bu veriler, yüksek ölçüde savunmadan kaçınma ve ayrıcalık yükseltme yaklaşımlarına odaklanıldığını öne çıkarıyor. Bu teknikler yeni olmasa da sistemleri savunan ekipler bu güncel bilgi sayesinde gelecekteki saldırılara karşı daha iyi hazırlıklı olabiliyor. Eyleme geçirilebilir tehdit istihbaratıyla desteklenen entegre ve yapay zekadan (AI) güç alan [platform yaklaşımları](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=pr&utm_campaign=security-fabric), tüm uçlarda savunma yapmak ve şirketlerin bugün gerçek zamanlı olarak karşı karşıya kaldıkları değişen tehditleri belirlemek ve düzeltmek için gerekiyor.

**İş Ortaklıkları, Eğitim, Yapay Zekadan Güç Alan Önleme, Tespit Etme ve Yanıt Teknolojiler Hayati Öneme Sahip**

Hükümet ve kolluk kuvvetleri geçmişte siber suçlarla ilgili önlemler almış olsa da 2021'in ilk yarısı, değişimlerin yaşandığı bir dönem olabilir. Sektördeki sağlayıcılar, siber saldırganlara karşı doğrudan harekete geçmek için kaynakları ve gerçek zamanlı tehdit istihbaratını birleştirmek amacıyla tehdit istihbarat şirketleriyle ve diğer küresel iş ortaklığı kurumlarıyla birlikte çalışıyor. Otomatik tehdit tespit etme ve yapay zeka, şirketlerin saldırıları gerçek zamanlı olarak ele almalarını sağlamak ve saldırıları tüm uçlarda hızla ve istenen ölçekte azaltmak için hala gerekli olmaya devam ediyor. Ayrıca siber saldırıların hedefi olan herkes için siber güvenlik [kullanıcı farkındalığı eğitimi](https://www.fortinet.com/blog/business-and-technology/fortinet-training-advancement-agenda-taa-improves-cyber-awareness-globally?utm_source=blog&utm_campaign=TAA) her zamankinden daha önemli. Çalışanları ve organizasyonu güvende tutmak için herkesin en iyi uygulamalar hakkında düzenli eğitime ihtiyacı var.

**FortiGuard Labs Güvenlik Yaklaşımları ve Global Tehdit Ortaklığı Başkanı Derek Manky**, konuyla ilgili şunları söyledi:

“Binlerce kuruluşu etkileyen etkili ve yıkıcı siber saldırıların arttığını ve siber suçlara karşı verilen savaşta önemli bir dönüm noktası oluşturduğunu görüyoruz. Artık herkesin siber saldırıyı engelleme süreçlerini güçlendirmede her zamankinden daha önemli bir rolü var. Siber suçluların tedarik zincirlerini bozmak için güçleri işbirliğiyle birleştirmeye öncelik vermek gerekiyor. Paylaşılan veriler ve iş ortaklıkları, daha etkili yanıtların ortaya çıkmasını ve saldırganların çabalarını boşa çıkartmak için gelecekte kullanılabilecek teknikleri daha iyi tahmin edilmesini sağlayabiliyor. Siber güvenlik farkındalığı eğitimini ara vermeden sunmanın yanı sıra uç noktalar, ağlar ve bulut arasında entegre edilen yapay zeka destekli önleme, tespit etme ve yanıt teknolojileri, siber saldırganlara karşı koymak için hayati önem taşıyor.”

**Raporun Özeti**

Küresel Tehdit Raporu, [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs)’ın Fortinet'in geniş çaplı sensörlerinden elde ettiği 2021'in birinci yarısına ait kolektif istihbarat bilgilerini yansıtan bir raporudur. MITRE ATT&CK yapısının saldırganların yöntemlerini ve tekniklerini [keşif](https://attack.mitre.org/tactics/TA0043), [kaynak geliştirme](https://attack.mitre.org/tactics/TA0042) ve [ilk erişim](https://attack.mitre.org/tactics/TA0001) olacak şekilde üç başlıkta sınıflandırmasına benzer olarak FortiGuard Labs Küresel Tehdit Raporu da tehdit aktörlerinin zafiyet bulma, kötü amaçlı yazılım altyapısı geliştirme ve hedeflerini istismar etme süreçlerini tanımlamak için bu modelden faydalanıyor. Raporda aynı zamanda küresel ve bölgesel bakış açıları da yer alıyor.

**Ek Kaynaklar**

* Raporun önemli başlıkları için [blog](https://www.fortinet.com/blog/industry-trends/fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware?utm_source=pr&utm_campaign=fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware) içeriğini okuyabilir ya da [raporun tamamına](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2021-threat%20landscape.pdf) erişebilirsiniz.
* [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs) tehdit istihbaratı ve araştırma veya yıkıcı siber saldırıların etkisini azaltmak için zamanında atılması gereken adımları sunan [Outbreak Alerts](https://www.fortinet.com/fortiguard/outbreak-alert?utm_source=pr&utm_campaign=outbreak-alert) hakkında daha fazla bilgi için bağlantılara tıklayabilirsiniz.
* Fortinet’in FortiGuard güvenlik hizmetleri [portföyü](https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions?utm_source=pr&utm_campaign=fortiguard-subscriptions) hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* Fortinet’in her zaman güvenilir bir dijital dünyayı nasıl mümkün kıldığını görmek için [videoyu](https://youtu.be/C5PuGKKNzpU) izleyebilir, [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=pr&utm_campaign=security-fabric)’in kurumların tüm dijital saldırı zemininde kapsamlı, entegre ve otomatik korumayı nasıl sağladığını öğrenmek için [bağlantıya](https://www.youtube.com/watch?v=x8US5w7D5Mc) tıklayabilirsiniz.
* [Fortinet müşterilerinin](https://www.fortinet.com/customers.html?utm_source=pr&utm_campaign=customers) kurumlarını nasıl koruduğu hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* Fortinet’in Training Advancement Agenda (TAA) inisiyatifi kapsamında [ücretsiz siber güvenlik eğitimi](https://www.fortinet.com/blog/business-and-technology/fortinet-training-advancement-agenda-taa-improves-cyber-awareness-globally?utm_source=blog&utm_campaign=TAA), [Network Security Expert programı](https://training.fortinet.com/?utm_source=pr&utm_campaign=nse-institute), [Security Academy programı](https://training.fortinet.com/local/staticpage/view.php?page=fnsa&utm_source=pr&utm_campaign=fnsa) ve [Veterans programı](https://www.fortinet.com/corporate/careers/vets.html?utm_source=pr&utm_campaign=fortivet) hakkında ayrıntılı bilgi için bağlantılara tıklayabilirsiniz.
* [Fortinet Kullanıcı Topluluğu’nda (Fuse)](https://fusecommunity.fortinet.com/home?utm_source=blog&utm_medium=campaign&utm_campaign=2020-fusecommunity) fikirlerinizi ve geribildirimlerinizi paylaşmak, ürünler ve teknolojiler hakkında daha fazla bilgi almak veya benzer iş kollarındaki kişilerle iletişime geçebilmek için bağlantıya tıklayabilirsiniz.
* Fortinet’i [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/) ve [Instagram](https://www.instagram.com/behindthefirewall/)’dan takip edebilirsiniz. Fortinet’e YouTube’dan [abone olabilirsiniz](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1).

**İlgili Kişiler:**Ceren Moral Aru – Marjinal Porter Novelli
0533 921 43 53
cerenm@marjinal.com.tr
Beril Pelesen – Marjinal Porter Novelli
0537 220 49 39
berilp@marjinal.com.tr

**Fortinet Hakkında**

İnsanları, cihazları ve verileri her yerde koruma misyonuyla faaliyet gösteren Fortinet, güvenilir bir dijital dünya yaratmayı mümkün kılmaktadır. Bu yüzden dünyanın en büyük şirketleri, hizmet sağlayıcıları ve kamu kurumları dijital dönüşümlerini güvenle hızlandırmak için Fortinet’i tercih etmektedir. Fortinet Security Fabric, tüm dijital saldırı zemininde kapsamlı, entegre ve otomatik koruma sunarak kritik cihazları, verileri, uygulamaları ve veri merkezi, bulut ve home ofis arasındaki bağlantıyı korumaktadır. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 530 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Fortinet’in Training Advancement Agenda (TAA) inisiyatifinin bir parçası olan Fortinet NSE Eğitim Enstitüsü, herkesin siber eğitimlere erişebilmesi ve yeni kariyer fırsatlarını değerlendirebilmesi için sektördeki en büyük ve kapsamlı siber güvenlik eğitim programlarından birini sunmaktadır. Daha fazla bilgi için: https://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.