**BASIN BÜLTENİ**

**FortiGuard Labs’in raporuna göre siber suçlular**

**uzayı da hedefliyor**

**FortiGuard Labs gelişen siber suç yöntemleri konusunda uyarıyor. Gelişmiş kalıcı siber suç teknikleri, daha yıkıcı fidye yazılımları ve tedarik zinciri saldırıları anlamına geliyor.**

[Geniş, entegre ve otomatik siber güvenlik çözümlerinde küresel bir lider olan Fortinet](http://ctt.marketwire.com/?release=11G067974-001&id=7377526&type=0&url=http%3a%2f%2fwww.fortinet.com)® (NASDAQ: FTNT), bugün [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs) küresel tehdit istihbaratı ve araştırma ekibinin 2022 ve sonrası için siber tehdit ortamı hakkındaki tahminlerini açıkladı. Siber saldırganlar, özellikle her yerden çalışma devam ederken, tüm saldırı yüzeyini kapsayan yeni kullanım alanlarını hedeflemek için saldırı yöntemlerini geliştiriyor ve genişletiyor. 5G-etkin sınırdan çekirdek ağa, eve ve hatta uzaydaki uydu internete kadar en üst düzeye çıkarma fırsatı arıyorlar. İleriye dönük trendlere bakıldığında, FortiGuard Labs'in siber rakiplerin ileriye dönük avantajlardan yararlanacağını ve savunma hatlarındakilerin yaklaşan bu saldırılara karşı korunmaya hazırlanmalarına yardımcı olacak önerileri ortaya koyuyor.

**Fidye Yazılımlar gibi saldırıları En Üst Düzeye Çıkarabilmek için Saldırı öncesi Keşifler Artıyor**

Saldırılar genellikle MITRE [ATT&CK çerçevesi](https://www.fortinet.com/blog/industry-trends/smarter-security-starts-with-understanding-how-cybercriminals-wo) gibi bir saldırı zinciri üzerinden bakıldığında sol taraf ve sağ taraf tehditleri olarak inceleniyor. Saldırı zincirinin sol tarafında planlama, geliştirme ve silahlanma stratejilerini içeren ve saldırı öncesi harcanan çabalar yer alıyor. Sağ tarafta ise saldırıların daha tanıdık icra aşamaları var. FortiGuard Labs, keşif ve yeni teknolojilerden yararlanmak ve daha başarılı saldırılar sağlamak isteyen siber suçluların sıfır gün yeteneklerini keşfetmek için daha fazla zaman ve çaba harcayacağını öngörüyor. Ne yazık ki, genişleyen “Hizmet Olarak Suç” pazarı nedeniyle sağ tarafta yeni saldırıların başlama oranında da bir artış olacağı tahmin ediliyor.

* ***Ransomware Daha Yıkıcı Olacak:*** Suç yazılımları yayılmayı sürdürüyor ve fidye yazılımları önümüzdeki dönemde de odak olmaya devam edecek. Fidye yazılımı saldırganları, fidye yazılımlarını DdoS ile birleştirerek zaten bu trende eklendi ve BT ekiplerini bunaltıp saldırı hasarını azaltmak için son saniye eylemlerini yapamayacak hale getirmeyi umuyor. Sadece verileri mahvetmekle kalmayıp aynı zamanda sistemleri ve donanımı yok eden bir saatli bomba" yapmak, şirketlerin ek önlemler almasını gerektiriyor. Örneğin, wiper yani silici isimli kötü amaçlı yazılım, [Tokyo'daki Olimpiyat Oyunları](https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games)'nı hedef alarak çarpıcı bir dönüş yaptı. Siber suçlu saldırı yöntemleri ve gelişmiş kalıcı tehditler (ATS) arasında görülen yakınsama seviyesi göz önüne alındığında, fidye yazılımı araç setlerine kötü amaçlı silici yazılımları gibi yapılandırıcı yeteneklerin eklenmesi an meselesi. Bu, gelişmekte olan sınır ortamları, kritik altyapı ve tedarik zincirleri için de bir endişe kaynağı olabilir.
* ***Siber Suçlular Derin Sahtecilikte Ustalaşmak İçin Yapay Zekayı Kullanıyor***: Yapay Zeka (AI), genellikle botnet'ler tarafından bir saldırıya işaret edebilecek olağandışı davranışları tespit etmek gibi birçok yönden savunma amaçlı olarak zaten kullanılıyor. Siber suçlular, anormal etkinliklerini tespit etmek için kullanılan karmaşık algoritmaları engellemek için yapay zekadan da yararlanıyor. İleriye dönük olarak, derin sahtekarlıklar giderek artan bir endişe haline geldikçe bu durum da evrilecek, çünkü insan faaliyetlerini taklit etmek için AI'dan yararlanıyorlar ve onu sosyal mühendislik saldırılarını geliştirmek için kullanabilirler. Ayrıca, gelişmiş uygulamaların sürekli ticarileştirilmesi nedeniyle derin sahtekarlıklar oluşturulan yerlerin de çıtası düşürülecektir. Bunlar, biyometrik analizleri geçebilen ses ve video uygulamaları üzerinde gerçek zamanlı kimlik sahteciliğine yol açarak, nihayetinde ses izleri veya yüz tanıma gibi güvenli kimlik doğrulama biçimleri için zorluklar oluşturabilir.
* ***Tedarik Zincirinde Önceden Daha Az Hedeflenmiş Sistemlere Karşı Daha Fazla Saldırı***: Birçok ağda, arka uç bilgi işlem sistemlerinin çoğunu Linux çalıştırıyor ve burası yakın zamana kadar siber suçlu topluluğunun birincil hedefi olmamıştı. Son zamanlarda, Windows 10, Windows 11 ve Windows Server 2019'da Linux binary dosyalarını yerel olarak çalıştırmak için bir uyumluluk katmanı olan Microsoft'un WSL'sini (Linux için Windows Alt Sistemi) hedef alan yeni kötü amaçlı binary dosyalar tespit edildi. Ayrıca, Linux platformları için botnet kötü amaçlı yazılımları zaten yazılıyor. Bu, saldırı yüzeyini ağın çekirdeğine doğru genişletiyor ve genel olarak savunulması gereken tehditleri artırıyor. Bunların, operasyonel teknoloji (OT) cihazları ve genel olarak Linux platformlarında çalışan tedarik zincirleri için olumsuz sonuçları olacaktır.

**FortiGuard Labs Güvenlik Öngörüleri ve Küresel Tehdit İttifakları Yöneticisi Derek Manky,** “Siber suçlular gelişiyor ve geleneksel APT gruplarına daha çok benzemeye başlıyor. Saldırganlar artık sıfır gün donanımlı, yıkıcı ve hedeflerine ulaşmak için tekniklerini gerektiği gibi genişletebiliyor. Önümüzdeki dönemde saldırganların bölümlenmiş ortamlar, silolanmış ekipler ve araçların yanı sıra büyük bir genişletilmiş saldırı yüzeyinden yararlandığını, saldırıların genişletilmiş ağın daha dışına, hatta uzaya dek yayıldığını göreceğiz. Bu tehditler, arkalarında, olası her saldırı yolunu önlemek için çırpınan BT ekipleri bırakacak. Gelişen bu tehditlerle mücadele etmek için kurumların siber güvenlik ağı mimarisinde bulunan bir Security Fabric platformunu benimsemesi gerekiyor.”

**Siber Suçlular Her Yeri Hedefliyor—Cüzdanınız, Uzay ve Eviniz**

Savunma hattındakileri, artan sayıda saldırı veya siber düşmanların gelişen tekniklerinden çok daha fazlası bekliyor. Daha da geniş bir saldırı yüzeyini kapsayan yeni sömürü alanları araştırılıyor. Ama artık tüm bunları yapabilmek çok daha zor çünkü aynı zamanda dünyanın dört bir yanındaki kurumlar, sadece ofis değil her yerden çalışma (WFA), uzaktan öğrenme ve yeni bulut hizmetleri tarafından yönlendirilen yeni ağ sınırları ile ağlarını genişletmeye devam edecekler. Benzer şekilde, evde, çevrimiçi eğitim öğrenme ve oyun oynama gibi yaygın faaliyetler de sürüyor, hatta bunların popülaritesi artıyor. Her yerde ve her zaman hızlı bağlantıdaki bu artış, siber suçlular için muazzam bir saldırı fırsatı sunuyor. Tehdit aktörlerinin, önemli kaynakları, yalnızca çekirdek ağı hedeflemek yerine, genişletilmiş ağ genelinde ortaya çıkan uç ve "her yerdeki" ortamları hedeflemek ve bunlardan yararlanmak için değiştirmesi bekleniyor.

* ***Siber Suçlar Uzayı da Hedefliyor:*** FortiGuard Labs, uydu tabanlı internet erişimi büyümeye devam ettikçe, önümüzdeki yıl uydu ağlarını hedef alan yeni proof-of-concept (POC) tehditlerinin de görüleceğini öngörüyor. En büyük hedefler, çevrimiçi oyun veya kritik hizmetleri uzak konumlara sunma gibi düşük gecikmeli etkinlikleri desteklemek için uydu tabanlı bağlantıya güvenen kurumlar ve ayrıca uzak saha ofisleri, üretim hatları veya deniz ve havayolları olacaktır. Kurumlar, uzaktan çalışan OT cihazları gibi önceden şebekeden bağımsız sistemleri birbirine bağlı ağlarına bağlamak için uydu ağları ekledikçe potansiyel saldırı yüzeyi de genişleyecektir. Bu gerçekleştiğinde, fidye yazılımı gibi saldırı türleri de büyük olasılıkla onları izleyecek.
* ***Dijital Ceplerinizi Koruyun:*** Finansal kurumlar işlemleri şifrelediğinden ve çok faktörlü kimlik doğrulama (MFA) gerektirdiğinden, elektronik havaleleri ele geçirmek siber suçlular için giderek daha zor hale geldi. Dijital cüzdanlar ise bazen o kadar güvenli olmayabiliyor. Bireysel cüzdanların getirisi o kadar büyük olmasa da, işletmeler çevrimiçi işlemler için para birimi olarak dijital cüzdanları giderek daha fazla kullanmaya başladıkça bu durum değişebilir. Bu gerçekleştiğinde, saklanan kimlik bilgilerini hedeflemek ve dijital cüzdanları boşaltmak için özel olarak daha fazla kötü amaçlı yazılım tasarlanacaktır.
* ***Esporlar da Hedef***: Esporlar, genellikle profesyonel oyuncuların ve takımların dahil olduğu, organize, çok oyunculu video oyunu yarışmalarıdır. Oyunlar aynı zamanda bu yıl geliri 1 milyar doları aşma yolunda olan gelişen bir endüstri. E-sporlar, DDoS saldırıları, fidye yazılımları, finansal ve işlemsel hırsızlık veya sosyal mühendislik saldırıları gibi siber suçlular için davetkar bir hedef, çünkü oyunlar sürekli bağlantı gerektiriyor ve genellikle güvenliği tutarsız ev ağlarında veya Wi-Fi ağlarının erişime açık olduğu durumlarda oynanıyor. Oyun oynamanın etkileşimli doğası nedeniyle, aynı zamanda sosyal mühendislik tuzakları ve saldırılarına hedef oluyorlar. Büyüme hızı ve artan ilgi göz önüne alındığında, e-spor ve çevrimiçi oyunların 2022'de büyük saldırı hedefleri olması muhtemel.

**Sınırda Yeni Bölgelerde Yaşamak**

Artan sayıda Nesnelerin İnterneti (IoT) ve OT cihazlarının yanı sıra, gerçek zamanlı işlemlerin ve uygulamaların oluşturulmasını sağlayan 5G ve YZ tarafından desteklenen akıllı cihazlar tarafından daha fazla sınır desteği mevcut. Siber suçlular, bir saldırı için giriş noktası olarak tüm genişletilmiş ağı hedefledikçe, yeni sınır tabanlı tehditler ortaya çıkmaya devam edecek. Siber suçlular, benzeri görülmemiş bir ölçekte gelişmiş ve daha yıkıcı tehditler oluşturmak için akıllı sınırlar ve bilgi işlem gücündeki ilerlemeler tarafından yaratılan olası güvenlik açıklarını en üst düzeye çıkarmak için çalışacak. Sınır cihazlar daha yerel yeteneklerle daha güçlü hale geldikçe, yeni saldırılar "sınırda yaşamak" için tasarlanacak. BT ve OT ağlarının yakınsaması devam ederken, özellikle sınırda OT'yi hedef alan saldırılarda bir artış olması muhtemel.

* ***Siber Suçlular LotL(Living off the Land) konusunda Gelişiyor***: Yeni bir sınır tabanlı tehdit ortaya çıkıyor. “LotL” yaklaşımıyla üretilmiş kötü amaçlı yazılımlar, güvenliği ihlal edilmiş ortamlardaki mevcut araç setlerinden ve yeteneklerden yararlanıyor fakat saldırılar ve veri hırsızlığı normal sistem etkinliği gibi göründüğü için fark edilmiyor. Microsoft Exchange sunucularına yapılan Hafnium saldırıları, bu tekniği etki alanı denetleyicilerinde yaşamak ve orada kalmak için kullandı. LotL denebilecek bu saldırılar oldukça etkili çünkü hain faaliyetlerini gerçekleştirmek için meşru araçlar kullanıyorlar. LotL ve Sınır-Erişim Truva Atları (EAT'ler) kombinasyonu, sınır cihazlar daha güçlü, ortamın yerlisi olarak daha yetenekli ve elbette daha fazla ayrıcalık sahibi oldukça, yeni saldırılar sınırda da yaşamak üzere tasarlanacaktır. Sınıra yönelik kötü amaçlı yazılımlar, sınır etkinlikleri ve verileri izleyebiliyor ve kimseye sezdirmeden kritik sistemleri, uygulamaları ve bilgileri çalabiliyor, ele geçirebiliyor ve hatta fidye alabiliyor.
* ***Dark Web, Kritik Altyapıya Yönelik Saldırıları Ölçeklenebilir Hale Getiriyor***: Siber suçlular, kötü amaçlı yazılımlarını bir hizmet olarak çevrimiçi satarak para kazanabileceklerini öğrendiler. Benzer araçlar sunan başkalarıyla rekabet etmek yerine, özellikle sınırda OT ve BT yakınsaması devam ederken, portföylerini OT tabanlı saldırıları içerecek şekilde genişletecekler. Fidye için bu tür sistemlere ve kritik altyapıya sahip olmak kazançlı olacak, ancak bu durumun, bireylerin yaşamlarını ve güvenliklerini etkilemek de dahil olmak üzere korkunç sonuçları da olabilir. Ağlar giderek daha fazla birbirine bağlı olduğundan, hemen hemen her erişim noktası, BT ağına giriş elde etmek için bir hedef olabilir. Geleneksel olarak, OT sistemlerine yönelik saldırılar, daha uzmanlaşmış tehdit aktörlerinin etki alanıydı; ancak bu tür yetenekler, karanlık ağda satın alınabilen saldırı kitlerine giderek daha fazla dahil ediliyor ve bu da onları çok daha geniş bir saldırgan kümesine açık hale getiriyor.

**Cybersecurity Mesh Mimarisi Üzerine Kurulan Security Fabric Platformu**

Ortamlar artık daha parçalı hale geldi ve siber güvenlik ekipleri genellikle silolarda faaliyet gösteriyor. Aynı zamanda, birçok kurum çoklu bulut veya hibrit bir modele geçiş yapıyor. Tüm bu faktörler, siber suçluların bütünsel ve sofistike bir yaklaşım benimsemesi için mükemmel bir fırsat yaratıyor. Siber güvenlik ağı mimarileri, güvenlik kontrollerini geniş çapta dağıtılmış ağlara ve varlıklara entegre ediyor. Security Fabric yaklaşımıyla birlikte kurumlar, şirket içinde, veri merkezinde ve bulutta veya sınırda bulunan tüm varlıkları güvence altına alan entegre bir güvenlik platformundan yararlanabiliyor. Savunma hattındakilerin, tehdit önleme, algılama ve müdahaleyi hızlandırmak için yapay zeka ve makine öğreniminin (ML) gücünden yararlanarak şimdiden plan yapması gerekiyor. Uç nokta algılama ve yanıt (EDR) gibi gelişmiş sınır nokta teknolojileri, davranışa dayalı olarak kötü niyetli tehditlerin belirlenmesine yardımcı olabilir. Ayrıca, sıfır güven ağ erişimi (ZTNA), korumaları mobil çalışanlara, öğrencilere genişletmek ve güvenli uygulama erişimi için kritik olurken, Güvenli SD-WAN da gelişen WAN uçlarını korumak için önemlidir. Ayrıca, segmentasyon, siber suçluların bir ağ içindeki yanal hareketini kısıtlamak ve ihlalleri ağın daha küçük bir bölümüyle sınırlı tutmak için temel bir strateji olmaya devam edecek. Eyleme dönüştürülebilir ve entegre tehdit istihbaratı, saldırıların hızı artmaya devam ederken bir kuruluşun gerçek zamanlı savunma yeteneğini geliştirebilir. Bu arada, tüm sektörlerde ve kurum türlerinde, paylaşılan veriler ve ortaklık, daha etkili yanıtlar sağlayabilir ve düşman çabalarını caydırmak için gelecekteki teknikleri daha iyi tahmin edebilir. İşbirliği yaparak güçleri birleştirmeye, siber suçluların tedarik zinciri çabalarını onlar aynı şeyi yapmaya kalkışmadan önce bozmaya öncelik verilmesi gerekiyor.

**Ek Kaynaklar**

* 2022 tahminlerinin tamamına erişmek ve önemli başlıklar 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" \t "_blank) içeriğini okuyabilirsiniz.
* [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" \t "_blank) 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" \t "_blank)’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" \t "_blank) 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" \t "_blank), [LinkedIn](https://www.linkedin.com/company/fortinet" \t "_blank), [Facebook](https://www.facebook.com/fortinet/) ve [Instagram](https://www.instagram.com/behindthefirewall/" \t "_blank)’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](mailto:berilp@marjinal.com.tr)

Beril Pelesen – Marjinal Porter Novelli  
0537 220 49 39  
[berilp@marjinal.com.tr](mailto: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.