**BASIN BÜLTENİ**

**Fortinet, siber saldırganların önüne geçmek için, kurumların siber tehditlerle mücadelede daha fazla otomasyon uygulayacağını öngörüyor**

**Yapay zeka fuzzing tekniği ve makine öğrenme uygulamalarına zarar verilmesi yeni ağ ve yazılım zafiyetlerini ortaya çıkaracak.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), FortiGuard Laboratuvarlarının 2019 ve sonrası için tehdit görünümü öngörülerini duyurdu. Bu öngörüler, Fortinet araştırmacıları yakın gelecekte siber suçlarının uygulayacağı yöntem ve teknikler ile yaklaşan saldırılara karşı savunmada kurumlara yardımcı olacak önemli stratejik değişiklikleri açıklıyor. Öngörüler hakkında daha detaylı bilgi ve Baş Güvenlik Yöneticileri için önemli ipuçları [blog](https://www.fortinet.com/blog/industry-trends/predictions--ai-fuzzing-and-machine-learning-poisoning-.html)sayfasında yer alıyor.

Fortinet Güvenlik Yaklaşımları ve Global Tehdit Ortaklığı Başkanı Derek Manky paylaşılan öngörülere dair şunları söyledi: “Yapay zekadan ve otomasyondan faydalanan siber suç araçları ve yöntemlerinde önemli gelişmeler olduğunu görüyoruz. Kurumlar tehditleri daha net öngörebilmek ve her şeye yeniden başlamalarına yol açan ekonomik motivasyonlarla mücadele edebilmek için stratejilerini yeniden gözden geçirmelidir. Sürekli bir silahlanma yarışı içerisinde olmak yerine, kurumların, yaklaşımlarını ihlalden tespite ve tespitten hapsetmeye geçiş sürecini kısaltmak için otomasyonu ve yapay zekayı benimsemeleri gerekiyor. Bunun yolu da güvenlik unsurlarının, nesnelerin internetinden çoklu bulut ortamlarına kadar ağ segmentinin tüm noktalarında kapsamlı koruma ve vizibilete için dinamik bir şekilde tehdit bilgisini paylaşan bütüncül bir güvenlik dokusuna entegre edilmesinden geçiyor.”

Raporun öne çıkan öngörüleri şöyle:

**Siber saldırılar daha akıllı ve daha sofistike bir yapıya sahip olacak**

Pek çok suç örgütü saldırı tekniklerini hem etkinlik hem de bu tekniklerin geliştirilmesi, güncellenmesi ve uygulanması için gereken maliyet açısından değerlendiriyor. Bu sebeple, saldırı stratejilerinin pek çoğu, siber suçluların uyguladığı ekonomik model ele alınarak sekteye uğratılabilir. Kişiler, süreçler ve teknolojilerde yapılacak stratejik değişiklikler, siber suç örgütlerinin belirli kurumları hedefleyerek elde edecekleri finansal değeri yeniden düşünmeye zorlayabilir. Bunu başaran kurumların uyguladığı yöntemlerden biri ise normal koşullarda yüksek oranda insan müdahalesi ve gözetimi gerektiren zahmetli ve zaman alan aktivitelerin üstesinden gelmek için makine öğrenme ve otomasyon gibi yeni teknoloji ve stratejilerin benimsenmesine dayanıyor. Bu yeni savunma stratejileri siber suç stratejilerini büyük oranda etkileyerek saldırganların saldırı yöntemlerini değiştirmelerine ve saldırı geliştirme çabalarına hız kazandırmalarına yol açıyor. Artan makine öğrenme ve otomasyon kullanımına adapte olabilmek için, Fortinet, siber suç topluluklarının aşağıdaki saldırı stratejilerini benimseyeceğini ve tüm siber güvenlik endüstrisinin bu saldırı stratejilerini yakından takip etmesi gerektiğini öngörüyor.

* **Yapay zeka fuzzing tekniği ve güvenlik zafiyetleri:** Fuzzing, donanım ve yazılım arayüzü ve uygulamalardaki güvenlik açıklarını tespit etmek için profesyonel tehdit araştırmacılarının laboratuvar ortamlarında kullandığı ileri düzey bir tekniktir. Araştırmacılar bu tekniği, geçersiz, beklenmeyen veya yarı-rastlantısal veriyi bir arayüz ya da programa enjekte edip daha sonrasında arızalar, hata yakalama seyrinde beklenmedik artışlar, kod onaylama işlemlerinin başarısızlığa uğraması ve muhtemel bellek sızıntıları gibi olayları gözlemleyerek uygularlar. Geçmişte, bu teknik laboratuvar ortamlarında çalışan birkaç yetenekli mühendis tarafından uygulanabiliyordu. Ancak, Fortinet, makine öğrenme modellerinin bu sürece dahil edilmesiyle birlikte, bu tekniğin hem daha etkili ve ihtiyaca yönelik bir şekilde tasarlanacağını hem de teknik donanımı yeterince güçlü olmayan daha çok saldırgan tarafından uygulanabileceğini öngörüyor. Siber suçlular otomatik fuzzing programlar geliştirmek için makine öğrenmeden yararlanmaya başladığı için, farklı program ve platformları hedefleyen sıfırıncı gün saldırılarında artışa yol açacak sıfırıncı gün zafiyetlerinin keşfedilmesi sürecini de hızlandırabilecekler.
	+ ***Yapay zeka fuzzing tekniği kullanan sıfırıncı gün madenciliği:*** Yapay zekaya dayalı fuzzing yerini alır almaz, sıfırıncı gün istismarları için çalışmaya başlamak amacıyla kontrollü bir ortamda kodda işaretlenebilir. Bu, sıfırıncı gün istismarlarının geliştirilme hızını önemli ölçüde artıracak. Bu süreç organize edildiğinde, Sıfırıncı gün madenciliği hizmet olarak uygulanmaya başlanacak, böylece bireysel hedeflere yönelik özel tasarlanmış saldırıların ortaya çıkmasına neden olacak. Bu durum, kurumların güvenlik yaklaşımını değiştirecek. Çünkü kurumlar, ne sıfırıncı gün saldırılarının nerelerde ortaya çıkabileceğini ne de bunlara karşı nasıl etkin bir savunma geliştirebileceklerini öngörebilecek. Bu durum, bugün pek çok kurumun ağlarında kurulu olan izole edilmiş ve geleneksel güvenlik araçların kullanımını göz önünde bulundurulduğunda çok daha zorlu olacak.
	+ ***Sıfırıncı gün istismarlarının “bedeli”****:* Eskiden beri, sıfırıncı gün istismarlarının bedeli epey yüksek oldu. Çünkü bu tür istismarları ortaya çıkarmak zaman, çaba ve yetenek gerektiriyordu. Fakat, zaman içerisinde yapay zeka teknolojisi uygulandıkça, bu istismarlar son derece nadir görülen istisnalar olmaktan çıkıp bir elverişli bir metaya dönüşecek. Fidye yazılım ve botnetler gibi daha geleneksel istismar yöntemlerinin metalaşmasına hali hazırda tanık olunmuş durumda ve sonuçlar pek çok geleneksel güvenlik çözümlerinin sınırlarını zorladı. Mevcut zafiyetlerin ve istismarların sayıca ve tür olarak artması ve bunların hızlı bir şekilde sıfırıncı gün istismarları oluşturabilme ve bunları hizmet olarak sunabilme becerileri, karanlık ağda mevcut olan hizmet çeşitlerini ve maliyetlerini etkileyecek.
* **Hizmet olarak swarm (toplu saldırılar)**: Swarm (toplu saldırı) tabanlı zeka teknolojisiyle güçlenen sofistike saldırılardaki kayda değer gelişmeler,bizi hivenet olarak bilinen swarm (toplu saldırı) tabanlı botnet gerçekliğine yaklaştırıyor. Bu yeni ortaya çıkan tehdit jenerasyondaki ilerleme, işbirliği halinde ve bağımsız olarak çalışabilen akıllı botnetlerden oluşan geniş çaplı saldırılar için kullanılacak. Bu swarm ağlar hem kurumları savunmak için gereken teknolojiler açısından çıtayı yükseltecek, hem de sıfırıncı gün madenciliğinde olduğu gibi, saldırıların temelinde yatan siber suç iş modelini etkileyecek. Günün sonunda, istismar teknolojileri ve saldırı metodolojileri evrimleştikçe, bunların en önemli etkisi siber suç topluluklarının uyguladığı iş modelleri üzerinde olacak. Günümüzde, suç ekosistemi ağırlıklı olarak insan odaklı bir şekilde çalışıyor. Kiralık profesyonel siber saldırganlar, belirli bir ücret karşılığında özel istismarlar tasarlayabiliyor; hatta, Hizmet olarak Fidye Yazılım gibi yeni gelişmeler, korsan mühendislerin istismarlar oluşturma, test etme ve arka plan C2 sunucularını yönetme gibi farklı kaynaklar kullanmalarına yol açıyor. Ancak bağımsız, kendi kendine öğrenen Hizmet olarak Toplu Saldırılar, siber saldırgan-müşteri ile korsan girişimci arasındaki etkileşim miktarını büyük ölçüde azaltıyor.
	+ **Swarm (toplu) saldırılarda alakart menüsü:** İstenilen sonucu elde etmek için bir swarm’ı farklı görevlere bölmek, dünyanın sanallaşmaya doğru ilerlediği yola çok benziyor. Sanallaştırılmış bir ağda, kaynaklar, sanal makinelerin (VM) bant genişliği gibi birtakım sorunları çözme ihtiyacına dayalı olarak, hızlarını artırıp düşürebiliyor.Benzer şekilde, bir swarm ağındaki kaynaklar, saldırı zincirinde karşılaşılan spesifik güçlüklerin çözümü için art arda tahsis edilebiliyordu. Siber suç girişimcilerinin bir dizi analiz aracı ve istismarıyla önceden programladıkları bir swarm, saldırı protokollerini düzeltmek için swarmların bir grup olarak çalışmalarını mümkün kılan kendi kendine öğrenme protokolleriyle de birleşerek siber suçluların bir alakart menüden seçim yapar gibi kolay bir şekilde saldırı satın almasına yol açıyor.
* **Makine öğrenmenin zarar görmesi:** Makine öğrenme, savunma amaçlı güvenlik araçları arasında en çok umut vaat eden araçlardan biri. Güvenlik araçları ve sistemleri, davranışları temellendirme, sofistike tehdit tespiti için davranışsal analizleri uygulama veya cihazları izleme ve yamalama gibi belirli görevleri kendi başına yerine getirmek üzere eğitilebilir. Maalesef, bu süreç de siber saldırganlar tarafından istismar edilebilir. Siber suçlular, makine öğrenme süreçlerini hedefleyerek, cihazlara yama ve güncelleme yapılmasını engellemek, belirli uygulama ve davranış türlerini göz ardı etmek, tespiti atlatma için belirli bir trafiği loglamamasını sağlamak için cihaz ve sistemleri eğitebilecek. Bu durumun, makine öğrenme ve yapay zeka teknolojisinin geleceğinde devrim yaratacak bir etkisi olacak.

**Savunmalar da daha sofistike bir hal alacak**

Bu gelişmelere karşılık olarak, kurumların da siber suçlulara yönelik savunma çıtalarını yükseltmeye devam etmeleri gerekecek. Bu savunma stratejilerinin her biri, siber suç örgütlerinin yöntemlerini ve saldırılarını değiştirmeye, fırsatları değerlendirmek için yeni yollar geliştirmeye zorlayarak bu örgütleri etkileyecek. Siber suç örgütlerinin saldırılarını başlatma maliyetleri artacak, böylece siber suç geliştiricilerin aynı sonuçları elde etmesi için daha çok kaynak sarf etmesi ya da istismar edebilecekleri daha erişilebilir bir ağ bulması gerekecek.

* **Gelişmiş atlatma taktikleri:** Aldatma tekniklerinin yanlış bilgi etrafında şekillenen ağ varyasyonları sunan güvenlik stratejilerine entegre edilmesi, saldırganları kendi tehdit istihbaratlarını sürekli olarak doğrulamak, yanlış pozitifleri saptamak için zaman ve kaynak sarf etmek ve görebildikleri ağ bağlantılı kaynakların gerçek olduğundan emin olmaya zorlayacak.Sahte ağ kaynaklarındaki herhangi bir saldırı, otomatik olarak karşı tedbirleri harekete geçirerek anında tespit edileceği için, saldırganlar ağı delmek gibi basit taktikleri uygularken bile son derece dikkatli davranmak zorunda kalacak.
* **Birleştirilmiş açık işbirliği:** Siber saldırganların mevcut bir saldırıdan en üst seviyede kazançlı çıkmasını ve tespitleri atlatmasını sağlamanın en kolay yollarından biri, IP adresi değiştirmek kadar basit bir değişiklik yapmaktır. Bu değişikliklere ayak uydurmanın en etkili yolu, tehdit istihbaratının aktif olarak paylaşılmasıdır. Sürekli olarak güncellenen tehdit istihbaratı güvenlik sağlayıcılarının ve onların müşterilerinin en son tehdit görünümleriyle aynı seviyede yer almasını sağlar. Tehdit araştırma organizasyonları, sektör işbirlikleri, güvenlik üreticileri ve yasa uygulama mercileri arasındaki açık işbirliği çabaları, saldırganların kullandığı taktikleri açığa çıkararak ve paylaşımını yaparak, yeni tehditlerin tespit edilme süresini önemli ölçüde kısaltacak. Ancak, yalnızca gerektiğinde karşılık veren olmak yerine, açık işbirliği aracılığıyla veri beslemelerini hayata geçirmek için davranışsal analizlerin uygulanması, savunmada yer alan tarafların zararlı yazılımın davranışlarını öngörmesini sağlayacak, böylece siber suçluların uyguladığı mevcut modelin, mevcut zararlı yazılımdan yalnızca küçük değişiklikler yaparak tekrar tekrar faydalanmasının önüne geçecek.

**Hız, entegrasyon ve otomasyon kritik öneme sahip siber güvenlik esasları**

Gelecekte, tehditlere akıllı bir karşılık vermek amacıyla entegre bir şekilde tehdit bilgisini toplayan, işleyen ve bu bilgiye göre eyleme geçecek bir araç olmadan otomasyon ve makine öğrenimini kapsayan bir savunma stratejisi mevcut değil. Giderek gelişen tehditlere karşı mücadele etmeyi amaçlayan kurumlar, hızlı ve kapsamlı tespit ve müdahale için tüm güvenlik unsurlarını bir güvenlik dokusuna (*security fabric*) entegre etmeleri gerekiyor. Tüm güvenlik unsurlarıyla ilişki kuran ve paylaşılan gelişmiş tehdit istihbaratının, gerekli tespit pencerelerini daraltmak ve hızla çözüm sağlamak için otomatik hale getirilmesi gerekiyor. Dağıtık ağda kurulu uç ürünlerin entegrasyonunun stratejik segmentasyonla buluşması, giderek daha akıllı ve otomatik bir yapıya bürünen saldırılarla mücadele edilmesine yardımcı olacak.

**Ek kaynaklar:**

* Öngörüler hakkında daha fazla bilgi için [blog](https://www.fortinet.com/blog/industry-trends/predictions--ai-fuzzing-and-machine-learning-poisoning-.html) yazımızı okuyabilirsiniz.
* Fortinet Tehdit Görünümü raporunun en sonuncusuna ve 2018’in 3. Çeyreğindeki botnet, zararlı yazılım ve istismarları hakkında detaylı bilgiye [blog](https://www.fortinet.com/blog/industry-trends/as-the-holiday-season-draws-near--mobile-malware-attacks-are-pre.html) üzerinden erişebilirsiniz.
* [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 [portföyüne ulaşmak için tıklayın.](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services)
* Güvenlik denetimleri ve en iyi uygulamalar sunan FortiGuard [Güvenlik Derecelendirme Hizmeti için tıklayın.](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)
* Haftalık [FortiGuard Tehdit İstihbarat Özetlerine abone olmak için tıklayın.](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta)
* [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) veya [FortiVets program](https://www.fortinet.com/corporate/careers/vets.html?utm_source=blog&utm_campaign=2018-q2-fortivet)’ımımız hakkında ayrıntılı bilgi için tıklayın.
* [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric) veya [Third Generation of Network Security](https://www.fortinet.com/blog/business-and-technology/executive-insights--the-third-generation-of-security-is-here.html) bağlantılarından ayrıntılı bilgiler edinebilirsiniz.
* Fortinet’i on [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.

**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 360 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/).