**BASIN BÜLTENİ**

**Siber saldırganların yeni hedefi: Operasyonel Teknolojiler**

**Fortinet 2019 Operasyonel Teknoloji Güvenlik Trendleri Raporu OT/BT kesişimi ile ilişkilendirilen risklerin ciddi bir tehdit oluşturduğunu ve bu risklerin ICS/SCADA sistemlerini BT ağlarına bağlayan her kurum tarafından dikkatli bir şekilde değerlendirilmesi gerektiğini ortaya koyuyor.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet (NASDAQ: FTNT), operasyonel teknoloji (OT) ağlarına yönelik güvenlik trendlerini incelediği Fortinet 2019 Operasyonel Teknoloji Güvenlik Trendleri Raporunu yayımladı. Rapor, merkezi kontrol ve veri toplama sistemleri (SCADA) ile endüstriyel kontrol sistemlerinin (ICS) siber güvenlik durumunu tespit etmek için milyonlarca Fortinet cihazından toplanan verileri analiz ediyor. Bu analize göre, OT sistemlerine yapılan saldırılar, yamalanmamış yazılımlarla çalışan eski cihazları hedef alıyor. Ayrıca, artık BT ağlarında etkili olmayan eski saldırı yöntemlerine dayalı BT tabanlı saldırılar da OT sistemlerini her geçen gün daha fazla hedef alıyor. Öte yandan, tüm siber güvenlik sektörü, belirli bir amaca göre tasarlanmış, SCADA ve ICS sistemlerini hedef alan OT saldırılarında ciddi bir artış olduğunu gözlemliyor. Raporda, bu saldırıların OT ağlarının en zayıf bölümlerini hedef aldığı ve saldırganların standart protokollerin olmayışının yarattığı karmaşıklıktan faydalandıkları öne çıkan bulgular arasında yer alıyor. Ayrıca, her tür dikey pazar ve bölgede görülen önemli saldırılardan anlaşıldığı üzere, tehdit aktörleri sektör ya da coğrafya ayrımı yapmıyor.

Raporun öne çıkan bulguları arasında şunlar yer alıyor:

* 2018’de neredeyse her ICS/SCADA sağlayıcısında istismarlar hem sayıca hem de yaygınlık açısından arttı.
* Saldırganlar OT sistemlerini hedef almak için düzenli olarak BT tehditlerinde geri-dönüşüme gidiyorlar.
* 2018’de saptanan tekil tehditlerin yüzde 85’i OPC Classic, BACnet ve Modbus protokollerinin çalıştığı cihazları hedef aldı.
* BACnet saldırıları Ocak-Nisan 2018 arasında arttı; bu saldırılar Mirai botneti ile örtüşüyor.
* Moxa 313 zafiyeti, özellikle Japonya’da yoğun bir şekilde yaşanıyor.

**BT-tabanlı saldırılar OT sistemlerini giderek daha çok hedefliyor**

Fortinet’in 2019 Operasyonel Teknoloji Güvenlik Trendleri Raporu, siber suçluların OT sistemlerine saldırmak için BT-tabanlı eski tehditleri kullanabileceğini ortaya koyuyor. Saldırıların çoğu, yamalanmamış uygulamalar ve işletim sistemleri gibi eski teknolojileri hedefliyor. Bunun yanı sıra, siber suçlular çok çeşitli OT protokollerini hedef alarak cihazlara saldırmayı amaçlıyor. BT sistemlerinin uzun yıllardır TCP/IP protokolü üzerinde standartlaşmış olmasına karşın, OT sistemleri, büyük çoğunluğu işleve, sektöre ve coğrafi konuma özgü olan geniş bir yelpazede farklı protokoller kullanıyor. Bu durum, ortamlarını korumak isteyen güvenlik yöneticilerinin birbirinden çok uzakta sistemler oluşturmasını gerektirerek çeşitli güçlüklere neden oluyor. Böylece, sağlayıcı çözümleri ve ürünlerinin karmaşıklığı sorunu da ortaya çıkıyor. Geleneksel BT tabanlı zararlı yazılım saldırılarıyla da, bu yapısal sorunlar, pek çok OT ortamında dijital dönüşüm çabaları nedeniyle istenmeyen güvenlik hijyeni uygulamaları sonucuyla daha da karmaşık bir hal alabiliyor.

**Özel tasarlanmış OT saldırıları yükselişte**

Özellikle ICS ve SCADA sistemlerini hedef alan zararlı yazılımlar 10 yılı aşkın süredir geliştiriliyor. Örnekler çok fazla olmasa da, giderek bir hedef haline gelen emniyet sistemleriyle birlikte, OT sistemleri için özel olarak tasarlanmış saldırıların artmaya başladığı görülüyor.

Son on yılda öne çıkan OT tabanlı saldırılar arasında Stuxnet, Havex, Industroyer ve yakın zamanda dahil olan Triton/Trisis yer alıyor. Özellikle, Triton/Trisis’in, pek çok açıdan OT sistemlerine gerçekleştirilen ilk siber-fiziksel saldırı olması sebebiyle pek çok uzmanı alarma geçirdiği biliniyor. Zararlı yazılımın emniyet sistemlerini hedef aldığı düşünüldüğünde, makinelere zarar vermesi ve insan hayatını tehdit etmesi gibi çok daha kötü bir olay yaşanabilir.

Siber suçlular hem eski hem de yeni ağlar ve teknolojilerde bulunan zafiyetleri ve korunmayan sistemleri istismar etmeye devam ederek geliştirdikleri her yeni tehditten maksimum fayda sağlayabiliyor. Dijital dönüşüm çabalarına bağlı olarak BT entegrasyonu ve yakınsaması bu durumu daha da ciddileştiriyor. Bu yeni durumla mücadele etmenin yolu ise, çözümü sadeleştiren, organizasyondaki BT ve OT uzmanlarının birlikte çalıştığı kapsamlı bir stratejik yaklaşım benimsemekten ve onu uygulamaktan geçiyor.

**İlgili Kişi:**  
Eray Çoşan Akkuş   
Marjinal Porter Novelli  
0 533 927 23 97  
[erayc@marjinal.com](mailto: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 400 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/).