**BASIN BÜLTENİ**

**Dikkat: Nesnelerin İnternetine yönelik saldırılar 4 kat arttı**

**FortiGuard Labs çalışmalarından elde edilen rakamlar çarpıcı bir hacim büyümesine dikkat çekmekle birlikte zararlı yazılımların evrilmekte olduğunun da altını çiziyor:**

* **2017’nin dördüncü çeyreğinde, firma başına ortalama 274 saldırı gerçekleşti.**
* **Bir önceki çeyrekle karşılaştırıldığında yüzde 82 gibi kayda değer bir artış olduğu tespit edildi.**
* **Var olan zararlı yazılım ailelerinin sayısı da 3.317’e yükselerek yüzde 25’lik bir artış gösterdi.**
* **Tekil zararlı yazılım türleri de yüzde 19 artarak 17.761 seviyesine ulaştı.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet®’in (NASDAQ: FTNT), 2017’nin dördüncü çeyreği için yayımladığı Tehdit Görünümü raporunda özellikle nesnelerin internetine yönelik saldırıların bu zaman aralığında dört katına çıktığı görülüyor. Bu bulgular, Fortinet’in canlı üretim ortamlarında hizmete aldığı bir dizi ağ cihazları ve sensörleri tarafından toplanan milyarlarca tehdit vaka ve olaylarını temel alıyor.

**Fortinet Sistem Mühendisliği Bölge Direktörü Melih Kırkgöz** konuyu şöyle değerlendiriyor: “Zararlı yazılımların evrimi ağırlıklı olarak nesnelerin internetinin yaygınlaşmasından güç alıyor. Gartner’ın verilerine göre 2017’deki bağlantılı nesne sayısı 8 milyar olarak belirlendi. 2020’ye kadar bu rakamın üç katına çıkması beklenirken dünyada kişi başına aşağı yukarı ortalama üç bağlantılı cihaz olacağı öngörüsünden yola çıkılıyor. Özetle, siber suçlular için ağa giriş yapma veya ağın bir kısmını (ya da tamamını) rehin alma fırsatı azalma işareti vermediği gibi, katlanarak artıyor.”

Ortada dolaşan birçok tehdit olduğuna şüphe yok. Örneğin, WPA2 protokolüne karşı Anahtarı Yeniden Yükleme Saldırıları (KRACK), “tek kullanımlık anahtar” kelimesini kriptocuların sözlüğünden çıkarıp ana akıma dahil etti. Fidye yazılımlara da “.asasin” ve “Bad Rabbit” gibi kötü niyetli olduğu adından belli olan isimler eklendi. ‘Kriptomadencilik’ saldırıları da aniden arttı ve sistemleri çökertti.

**Nesnelerin İnterneti Saldırıları Artışta**

Bununla birlikte nesnelerin interneti temelli saldırılar dördüncü çeyrekte ilk sırada yer aldı. GoAhead, WIFICAM, MVPower, DVR, Netcore Netis cihazlarına ve Ubiqiti Networks’e ait AirOS ekipmanlarına karşı gerçekleştirilen saldırılar, dördüncü çeyrekte sensörler boyunca yayılmayı artırarak tespit edilen saldırılar listesinde ilk 20’de yer aldı. Özellikle WIFICAM saptama saldırıları listede bir anda yükseldi. Firmaların yüzde 8’i bu saldırılara üçüncü çeyrekte maruz kalırken dördüncü çeyrekte bu rakam dört katına çıktı.

Nesnelerin interneti saldırılarının vektörünü daha da tehlikeli kılan şey ise bu istismarların tamamının, bilinen veya adlandırılmış bir ‘Yaygın Zafiyet ve Maruziyet (CVE) ile ilişkili olmaması. Bu da nesnelerin internetindeki savunmasız cihazların sayısındaki hızlı artışının getirdiği endişe verici sonuçlardan birisi olarak dikkat çekiyor.

İlk 20 listesinde yer alan saldırıların üçü, dördüncü çeyrekte hedef aldıkları nesnelerin interneti cihazlarında da saptandı. Fakat tekil bir zafiyeti istismar eden önceki nesnelerin interneti saldırılarının aksine Reaper ve Hajime gibi yeni nesnelerin interneti botnetleri birden çok zafiyeti aynı anda hedef alabiliyor. Bu çok vektörlü yaklaşıma karşı mücadele etmek çok daha zor. Reaper’ın Lua motoru ve kodu üzerine kurulan esnek yapısı, önceki nesnelerin interneti zafiyetlerine yönelik sabit ve önceden programlanmış saldırılar yerine kodunun kolayca güncellenebileceği anlamına geliyor. Böylece halihazırda aktif bir botnet üzerinde kullanılabilir hale gelmesiyle daha hızlı toplanarak yeni ve daha zararlı saldırılar gerçekleştirebiliyor.

Ekim ayının başında Reaper’ın istismar hacmi birkaç günde normale düşmeden önce 50 binden 2,7 milyona fırladı. Bu tarz bir evrim potansiyelinin endişe verici olduğu belirtiliyor.

**Bizi neler bekliyor**

Melih Kırkgöz yakın gelecekte bizleri nelerin beklediğini özetlerken, “Nesnelerin interneti odaklı, savunmasız ve yamalanamayan cihazları hedef alan ve sayıları giderek saldırıların yansıması, geçmişte de görüldüğü gibi her şeyi daha kötü yapacak toplanma özelliğine sahip büyük botnetler şeklinde olacaktır. Dyn’e karşı gerçekleştirilen Mirai temelli saldırılar da bunun bir örneği. Bu tür toplu saldırı ağları (hivenet), insan denetiminin en az olduğu savunmasız sistemleri saptamak ve hedef almak için öğrenen makinaları ve çoklu vektör yaklaşımlarını kullanabiliyor” diyor. Geleneksel botnetler, bot yöneticisinden komutları beklerken hivenetlerde yer alan cihazlar, hedefi analiz edip sahip olabileceği zafiyetleri saptadıktan sonra bağımsız bir şekilde ortamı istismar edecek en muhtemel saldırı türünü seçebiliyor. Böylece daha hızlı yayılarak hiç olmadığı kadar yıkıcı sonuçlar oluşturabiliyor.

Fortinet Sistem Mühendisliği Bölge Direktörü Melih Kırkgöz, “2018 Tehdit Ortamı Öngörüleri” raporunda da belirttiğimiz gibi hivenetler, gizliliği ihlal edilmiş cihazların yığınını farklı saldırı vektörlerini saptamak ve saldırmak için kullanabiliyor. Daha fazla cihazı saptayıp gizliliğini ihlal ettikçe bir hivenet çok hızlı bir şekilde büyürken aynı anda birçok hedefe saldırma yeteneğini artırarak BT ekiplerinin yamayı, zararlı yazılıma karşı bir yazılımı veya izinsiz girişi engelleyici izinleri uygulama yeteneğini bastırabiliyor. Bu yüzden kuruluşunuzun şu anki hizmet engelleyici dağıtık savunmaları yakın zamanda değerlendirmesi, nesnelerin internetine yönelik toplu bir saldırı yolunuza çıktığı zaman sorun yaşamamanız için kritik bir öneme sahip” diyor.

Nesnelerin interneti saldırılarına karşı daha iyi savunabilmek için en iyi uygulamalar ağınıza bağlı cihazları saptamayla başlayıp envanterini yaptıktan sonra nasıl yapılandırıldığını ve ağ erişim noktalarının doğrulanmasını nasıl kontrol ettiklerini belgeliyor. Tam görünürlük elde edildikten sonra kuruluşlar, nesnelerin interneti cihazlarını dinamik olarak özelleştirilmiş ilkelere sahip güvenli ağ alanlarına ayırabiliyor.

Bununla birlikte, etkili koruma için, özellikle erişim noktalarında bu ağın tümünü kapsayabilecek, yanal genişleyen ağ trafiğiyle kesişebilen, hatta güvenlik cihazlarının ve platformlarının çoğunun yapamadığı bir şeyi yaparak çoklu bulut ortamlarına da yayılabilen entegre ve otomatikleştirilmiş güvenlik dokusunu veya yapısını kullanarak bu segmentlerin tümünün dinamik bir şekilde birbirine bağlanması gerekiyor.

**Önemli Olanı Korumak**

2018’de nesnelerin interneti, önemi gittikçe artan bir siber güvenlik problemi olmaya devam ediyor. Suçlular yalnızca güvenli olmayan ve savunmasız nesnelerin interneti cihazlarından faydalanmıyor. Nesnelerin internetinin sorunları, bildirilmiş zafiyetlere cevap veren ürün güvenlik ve olay müdahale ekibine (PSIRT) sahip nesnelerin interneti imalatçı sayısının çok az olması gibi birçok kritik güçlük ile şiddetleniyor. Devamında ise mevzuatın yetersiz olması da nesnelerin interneti imalatçılarının bildirilmiş bir tehdidi bile öncelik haline getirmesinin moral bozucu olması anlamına geliyor. Bilinen zafiyetleri hedef alan ve onlara dair resmi bir CVE eklenmemiş olan saldırıların sayısı da bunu destekliyor.

Nesnelerin interneti temelli zararlı yazılım ailelerinin çarpıcı bir şekilde artması, bu tehdidin inanılmaz derecede çabuk çoğalan yapısının altını çiziyor. “Çoğal ve saldır” stratejisi yeni olmasa da tek nokta, imza temelli zararlı yazılıma karşı yazılımların basitçe modern zararlı yazılımların hacmine, hızına ve çeşitlerine karşı savunmaya yeterli olmadığını bir kere daha hatırlatıyor. Ağınızın ve oradaki verinizin daha iyi korunması için kuruluşun, günümüzün ayrık ve dinamik ağ ortamının çoklu katmanında yer alan, bilinen ve bilinmeyen tüm tehditleri saptayacak zararlı yazılıma karşı savunma yeteneklerini son noktalardan çekirdeğe ve bulutun dışına entegre etmesi gerekiyor.

**İlgili Kişi**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 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 330 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.