**BASIN BÜLTENİ**

**Fortinet Küresel Tehdit Raporu’na göre siber suçlular halihazırda bilinen açıkları ve “Sürü” teknolojisini kullanarak hızlı ve büyük ölçekli saldırılar gerçekleştiriyor**

*Yüksek oranlardaki Botnet sıklığı ve otomatik hale getirilmiş kötü niyetli yazılımlar, olay yönetim stratejileri ile birleşen Akıllı ve otomatize güvenlik kontrollerinin önemini göstermektedir~~.~~*

Yüksek performanslı siber güvenlik çözümlerinde küresel lider olan Fortinet (NASDAQ: FTNT) Küresel Tehdit Raporu’nun sonuçlarını paylaştı. Araştırmaya göre botnetlerin yüksek oranlardaki tekrarlanma sıklığı ve otomatik hale getirilmiş kötü niyetli yazılımlardaki artış siber suçluların bilinen açıklardan faydalanırken otomatik hale getirilmiş saldırı yöntemlerini benzeri görülmemiş hızda ve ölçekte kullanmalarını sağlıyor.

**Fortinet Teknik Müdürü İlker İmamoğlu konuyla ilgili yaptığı açıklamada:**

“İster mayıs ayında karşılaştığımız WannaCry’ın kullandığı isterse de geçtiğimiz eylülde karşımıza çıkan Apache Struts olsun, uzun süredir bilinen ve hala yaması yapılmamış güvenlik açıkları ataklar için hala geçit vazifesi görüyor. Diğer açıklar ve tetikte bekleyen tehditlere karşı kurumların kendi ortamlarında neler olduğunu daha geniş bir açıyla bilmeleri önem kazanmaktadır. Güvenlik hijyeni ve otomasyon, entegrasyon ve stratejik segmentasyonu arttırıp desekleyen fabric-tabanlı güvenlik yaklaşımlarının öncelikli hale getirilmesi bir aciliyet haline geldi. Siber saldırganlar artık otomatik hale getirilmiş yeni eski birçok tekniği daha fazla kullanmaya başlıyor, bizim de bugünün yeni normali diyebileceğimiz saldırılarla başa çıkarken savunmamızın değerini yükseltmeliyiz” dedi.

**Daha da otomatikleştirilmiş ataklar ve sürü teknolojisi yaygın hale geliyor**

Sürü saldırıları ile başa çıkmak, yeniden tekrarlanan botnet’ler ile uğraşmak ya da en yeni fidye yazılımlar birçok stratejik ya da kadrolu güvenlik ekibinin işini zorlaştırmaya başlamış durumda. Gerekli önemler alınmaz ise her organizasyon sayısı artan bu atakların kurbanı olabilir**.** Gerçek sistemler üzerinde neler yaşandığını öğrenip dersler çıkarmayı amaçlayan Fortinet (NASDAQ: FTNT) Küresel Tehdit Raporu siber tehdit görünümünü birçok farklı bakış açısından ele alıyor. Rapor, tehdit görünümündeki uygulama suiistimalleri, kötü niyetli yazılımlar ve botnetlerden oluşan üç temel ve tamamlayıcı konuya odaklanıyor. Ayrıca önemli sıfır-gün zayıflıklarını gözden geçirirken kuruluşları zamanla etkisi altına alan siber saldırıların izlediği yola dair bilgiler edinmek amacıyla altyapı trendlerini ve saldırı yüzeylerini inceliyor.

* **Saldırıların önem derecesi aciliyet doğuruyor:** Şirketlerin yüzde 79’u 2017’nin üçüncü çeyreğinde şiddetli saldırılarla karşı karşıya kaldı. Elde edilen verilere göre 5973 tekil açık tespit edilirken, 2646 farklı kötü niyetli yazılım ailesinden gelen 14904 tekil kötü niyetli yazılım türü ve 245 tekil botnet tespit edildi. Fortinet, ek olarak bu yıl içinde 185 adet sıfır-gün açığını fark etti.
* **Yeniden tekrarlanan Botnetler:** Birçok kuruluş aynı botnetin neden olduğu bulaşmaları birden fazla defa yaşadı. Böylesi bir veri bir ikaz anlamına geliyor. Kuruluşlar ya gerçekten bu ihlallerin kapsamını tam anlamamış oluyor ve botnetler iş süreçlerinin tekrar normale dönmesi durumunda aktif hale gelecek şekilde uykuya dalıp bekliyor ya da ana sebep asla bulunamadığından aynı zararlı kuruma tekrar bulaşıyor.
* **Yoğun kullanılan Zayıflıklar:** Equifax’a saldırı için kullanılan uygulama açığı, geçen çeyrekte ve bu çeyrekte 6000 den fazla tekil tespit ile en yaygın olanıydı. Bu durum siber suçluların yaygın ve onaylanmış bir zayıflığın kokusunu aldıklarında, ekip halinde toplu olarak bu noktaya kilitlendiklerini ve yeni atak metotları oluştururken tercih ettiklerini bizlere gösteriyor.
* **Mobil Tehlikeler:** Her dört şirketten biri mobil kötü niyetli yazılım tespit etti. Dört mobil kötü niyetli yazılım ailesi tekrarlanma sıklıkları ile ilk defa öne çıktılar. Bu durum mobilin giderek artan bir şekilde hedef haline geldiğini ve tehditlerin de daha otomatik hale getirilmiş ve çok biçimli olduğunu gösteriyor. Alışveriş sezonunun hareketlenmesiyle beraber bu durum mobil cihazlardan daha sık yapılacak satın alma işlemlerini ve hediye olarak satın alınan IoT cihazlarını da ilgilendirecek.
* **Her tarafa yayılan, kendini saklayan kötücül yazılımlar:** Yaygın kötücül yazılım ailelerinin en yaygın fonksiyonu zararlı bileşenleri, yazılımları indirmek, yüklemek. Kötü niyetli yazılım yükleri bunlara ek olarak uzaktan erişim bağlantıları kurmak, kullanıcı girdisini yakalamak ve sistem bilgilerini toplamak gibi işlemleri de gerçekleştiriyor. Böylesi ileri seviye tekniklerin kullanılması giderek yaygın hale gelirken kötü niyetli yazılımların artan zekasını ve otomatik hale getirilmiş doğasını da gözler önüne seriyor.
* **Fidye yazılım tehdidi devam ediyor:** Bu yılın ilk yarısındaki bir boşluktan sonra Locky adlı fidye yazılım üç yeni dalga ile etkisini artırmıştı. Yaklaşık olarak şirketlerin yüzde 10’u Locky’yi raporlarken kurumların en az yüzde 22’si çeyrek boyunca fidye yazılım tespit ettiler.
* **Siber suçlular her büyüklükten şirketi hedefliyor:** Orta ölçekli kuruluşların daha yüksek oranlarda botnet bulaşmaları ile karşı karşıya kalmaları güvenlik sorunları açısından kendilerine düşmesi gerekenden daha fazla sorunla başa çıkmaya çalıştıklarını bizlere gösteriyor. Siber suçlular büyük şirketlerle karşılaştırıldığında, yeterli güvenlik kaynak ve teknolojilerine sahip olmaması ancak değerli verileri bünyelerinde bulundurmalarından ötürü orta ölçekli kuruluşları endüstrinin “yumuşak karnı” olarak görüyorlar. Ayrıca orta ölçekli kuruluşların her geçen gün artarak buluta yönelmesi de saldırı yüzeyinin hızla artmasına neden oluyor.
* **SCADA hayati bir öneme sahip:** Apache Struts’u hedef alan yoğun ataklara ek olarak bazı tehditler bazen tespit edilmez ya da bulaştıkları kurumun dışında da ciddi sonuçlara neden olabilirler. SCADA (Düzenleyici Kontrol ve Veri Erişimi) sistemlerini hedefleyen açıklardan sadece 1/1000’i tekrarlanma sıklığı eşiğini geçerken sadece yüzde 1’lik bir dilimde yer alan şirketler bu açıkları bildirdi. Kurumsal ağ ihlalleri ve sızıntılarının kötü etkisi yanında, maalesef SCADA ortamlarında gerçekleşebilecek ihlaller birçok hayatın bağlı olduğu fiziksel sistemleri riske atmakta ve istatistiklerin ne kadar önemli olduğunu bizlere göstermektedir.

**Eyleme geçirilebilir istihbarat ve otomatik hale getirilmiş güvenlik ile otomatik hale getirilmiş saldırılarla savaşın**

Bu çeyrekte karşımıza çıkan sonuçların birçoğu FortiGuard Labs küresel araştırma ekibinin yakın zamanda paylaştığı 2018 tahminlerini tekrar doğruluyor. Trendlerden ve tehditlerden elde edilen veri, yakın gelecekte karşımıza çıkacak potansiyel yeni saldırı dalgalarının olacağını gösteriyor. Siber suç topluluğu otomasyondaki en yeni gelişmelerden hünerli bir şekilde faydalanarak açıkları ve zayıflıkları suiistimal edecek artan kötü niyetli yazılım veri yükünü büyük ölçeklere çok hızlı bir şekilde taşıyabiliyor.

Tehdit bilgilendirme paylaşımı ve güvenlik ve ağ bileşenlerini tek, otomatik hale getirilmiş, proaktif bir savunma ve tepki sistemine bağlayan açık bir mimariye sahip bir güvenlik sistemi gelecekteki tehlikelere karşı korunmanızı sağlayabilir. Sürekli dönüşen saldırı yüzeyine karşı en yeni güvenlik stratejilerini ve çözümlerini, en gelişmiş teknolojileri ve yöntemleri var olan altyapıyı çöpe atmadan entegre hale getirmek bir zorunluluk haline geliyor.

Saldırıların otomasyon, hacim ve hızı artarken aktif sistemlerimizde neler gerçekleşebileceğini kestirmek için en kritik konulara odaklanıp bir yamalama önceliğine sahip olmak önem kazanıyor. Bunun dışında kuruluşların teknoloji ve bilgilendirmeleri süreçleri hızlandırmak için kullanacakları bir stratejik tehdit tespiti ve durum tepki stratejisine sahip olduklarından emin olmaları gerekiyor.

**Metodoloji**

Fortinet Küresel Tehdit Raporu her çeyrekte yayınlanan ve FortiGuard Labs’in Fortinet’in geniş çaplı sensörlerinden elde ettiği 2017 yılının 3. çeyrek bilgilendirmelerini yansıtan bir raporudur. Araştırmadaki veriler küresel, bölgesel, endüstri ve kurumsal bakış açılarını içerir. Fortinet raporun tamamlayıcısı niteliğindeki abonelik gerektiren, ücretsiz Threat Intelligence Brief ise haftalık olarak en yeni kötü niyetli yazılımlar, virüsler, web-tabanlı tehditleri Fortinet’in o hafta içindeki en değerli araştırmalarını da dahil ederek paylaşıyor.

**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.