**BASIN BÜLTENİ**

**Fortinet, sağlık sektörünü hedef alan 3 önemli saldırı trendine karşı uyarıyor**

**Siber saldırıların ardından toparlanmak için sağlık kurumlarının 1,4 milyon dolar harcama yapması gerekiyor! Kurumlar, ağlara sızmak amacıyla tasarlanan yeni yöntemlerden sürekli haberdar olur ve bu doğrultuda siber güvenlik çabalarına yönelik yeni taktikler geliştirirse siber saldırıların başarılı olma riski azalıyor.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet, ağ kesintilerinin insan yaşamını tehdit eden durumlara yol açabileceği sağlık sektöründe tehdit istihbaratının önemine değinerek sağlık sektörünü hedef alan tehditleri açıkladı. Sağlık sistemlerinde teknolojiye bağımlılık ve bağlantılı cihazların giderek artması doğrudan hastaları ve hasta bakımını da etkiliyor. Ayrıca, ortalama bir sağlık kurumunun bir siber ihlalin yarattığı hasarları gidermesi 1,4 milyon dolara mal olurken, hastanenin mali kaynakları, hasta deneyiminin en önemli iki bileşeni olan hastane itibarı ve hastaneye duyulan güven ciddi şekilde zarar görüyor.

**Sağlık sektörünü hedef alan tehditler**

Güvenlik ekiplerinin, diğer sektörleri hedef aldığı düşünülen tehditler dahil olmak üzere tüm önemli tehdit trendlerine karşı hazırlıklı olması gerekirken, Fortinet’in 2019 1. Çeyreğinde topladığı verileri incelediği Tehdit Raporu’nda öne çıkan tehdit türlerinin, özel olarak sağlık sektörünü de etkileyebildiği öne çıktı.

Fortinet, bu tehditler arasında öne çıkan şu üç tehdide karşı sağlık sektöründe çalışan BT ve güvenlik ekiplerini uyarıyor:

**Gizlenmek için yasal görünen araçlardan faydalanma**

Bu saldırı türü 2019’un 1. çeyreğinde sık sık görülen bir saldırı yöntemi olarak ortaya çıkıyor. Siber suçlular, PowerShell gibi, hedef aldıkları sistemlerde önceden kurulu olan ve saldırı başlatmak için istismar edilebilen araçlardan faydalanıyor. Bu yaklaşımda, sisteme bulaştırılan zararlı kod onaylanmış bir sürecin bir parçası olarak göründüğü için atlatma tekniklerini kolaylaştırıyor, böylece güvenlik ekipleri tarafından tespit edilmesi ve tanımlanması zorlaşıyor. Windows cihazlarda kurulu olan PowerShell bu saldırı türlerinin en popüler hedeflerinden biri olarak kabul ediliyor. Siber suçlular, verileri şifrelemek ve ağ boyunca yanal hareketlerini sürdürerek fidye talep etmek için PowerShell’den faydalanıyor.

Özellikle internete bağlı IoT cihazı sayısı düşünüldüğünde, sağlık sektöründeki BT ekiplerinin bu saldırı yönteminden haberdar olmaları gerekiyor. Sağlık sistemleri, sürekli olarak, pek çoğu güvenlik düşünülerek tasarlanmamış olan hasta tedavilerinin bir parçası olan yeni bağlantılı araçların kurulumunu yapıyor. Bu tehditten korunmak için, BT ekiplerinin hiçbir önceden kurulu aracın ele geçirilmediğinden ve böylece ağda bir açık kapı bırakılmadığından emin olmak için cihazlarda düzenli kontroller uygulaması gerekiyor.

**Özel hedefli fidye yazılımlar**

Bu yıl gerçekleşen yüksek profilli fidye yazılım saldırılarının gelişmiş düzeyde hedeflendiği ve planlandığı görülüyor. Aslında, LockerGoga vakalarının birinde, saldırganlar, zararlı yazılımın uygulanmasını sağlayan imtiyazlı kimlik bilgilerine erişim için ayrıntılı inceleme ve hazırlık sürecini çoktan tamamlamıştı. Bu kimlik bilgileri sayesinde, minimum düzeyde atlatma ve gizleme taktiği kullanarak saldırı yürütebilmişlerdi. Bu durum, bu yöntemi kullanan saldırganların çoktan ağ savunmalarını değerlendirdiklerini ve bu önlemleri işlevsiz kıldıklarını gösteriyor.

Mümkün olduğunca çok sayıda dosyayı şifreleyen ve minimum düzeyde onarım şansı bırakan Anatova da 1.çeyrekteki fidye yazılımları arasında öne çıkıyor. Anatova, saldırganların, spesifik olarak seçtikleri ağlara odaklanmak için tamamen şansa dayalı bir zararlı yazılım dağıtım modelinden uzaklaştıklarını gösteriyor.

Fortinet uzmanları, sağlık sistemlerinin bu saldırıları akılda tutarak, zararlı yazılım savunmalarını güçlendirmeleri ve halihazırda veri yedeklerinin olduğundan emin olmaları gerektiğini belirtiyor. Büyük olasılıkla veri kurtarımı ve süreklilik süreçlerindeki eksiklikler ve yetersiz planlama sebebiyle çalınan veriler için daha fazla para ödeyeme hazır olan hastanelerin fidye yazılım saldırıları için özel hedefler olduğu biliniyor. Fidyenin ödenmesiyle geri alınan veri ise bozulmuş ya da eksik olabiliyor ve böylece hasta güvenliği üzerinde potansiyel bir etki yaratıyor.

**Ele geçirme öncesi ve sonrası aksiyon trafiği**

* Saldırganların kullandığı web sitesi türlerini ve erişim sağladıkları siber ölüm zincirinin fazını değerlendirmek, siber saldırganların eylemlerini nasıl yapılandırdıklarına dair öngörüler ortaya koyuyor. Bu sebeple ele geçirme eylemi öncesi ve sonrasındaki gelişmelerin kaydedilmesi önem arz ediyor. Ele geçirme öncesi eylemlerin, çalışanların sık sık tuzağa düştüğü iş günlerinde gerçekleşme olasılığının üç kat daha fazla olduğu görülüyor. Ele geçirme sonrası eylemlerin ise kullanıcı arayüzünün çok az ya da hiç gerekmemesi sebebiyle, iş günleri ve hafta sonlarında istikrarlı bir şekilde gerçekleştiği tespit ediliyor.

**Sağlık sektöründe güvenlik için segmentasyon şart**

Bu gelişmeler, segmentasyona dair önemli bir noktayı akıllara getiriyor. Sağlık sektörünün her daim çalışan bir sektör olduğu biliniyor. Örneğin, acil servis ağının hafta sonu dahil olmak üzere sürekli çalışıyor olması, bir saldırı sebebiyle çalışmasının durmaması ya da yavaşlamaması gerekiyor. Öte yandan, her zaman çalışır durumda olması gerekmeyen departmanların da olduğu biliniyor. Örneğin böyle bir departmanda, mesai süresi dışında bir cihaza giriş yapılması bir saldırı sinyali olabiliyor. Saldırıları başlatmak, genişletmek ya da ağda yatay hareket etmek için düzensiz çalışma saatlerinde çalışan ele geçirilmiş cihazlar, acil servisteki gibi son derece gerekli olan ağları etkileyebiliyor. Bu sebeple, sağlık sistemlerinin ek bir savunma katmanı ekleyerek önemli ağlarda segmentasyona başvurmaları ve ne amaçla kullanıldıkları anlaşılana kadar anormal davranışlar gösteren cihazları izole etmeleri öneriliyor.

**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/).