**Şirketinizi WCry fidye yazılımından koruyun**

Malware tehditleri içerisinde en hızlı büyüyen yazılım olan fidye yazılımları, ev kullanıcılarından sağlık kurumlarının sistemlerine ve şirket ağlarına kadar herkesi hedef alıyor. Yapılan analizlere göre 1 Ocak 2016’dan bu yana günde ortalama 4 binden fazla saldırı fidye yazılımları ile gerçekleştiriliyor.

12 Mayıs’ta [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html), gün içerisinde hızla yayılan yeni bir fidye yazılımını takibe aldı. Kendi kendini kopyalayarak çok büyük zararlar veren bu yazılım, Rusya İçişleri Bakanlığı, Çin’deki üniversiteleri, Macaristan ve İspanya’daki telekom şirketlerini ve İngiliz Ulusal Sağlık Hizmetleri bünyesindeki hastaneleri ve klinikleri etkiledi. Yazılımın ayrıca iki düzineden fazla dil desteğine sahip olması da dikkat çekiciydi.

Bu fidye yazılımına WCry, WannaCry, WanaCrypt0r, WannaCrypt ve Wana Decrypt0r gibi isimler verildi. Fidye yazılım, iddiaya göre NSA’in (ABD Ulusal Güvenlik Ajansı) kullandığı ETERNALBLUE açığı vasıtasıyla yayılıyor. Microsoft Server Message Block 1.0 (SMBv1) protokolü içerisindeki bir açığı kullanan ETERNALBLUE, The Shadow Brokers isimli hacker grubu tarafından geçen ay online olarak sızdırılmıştı.

**Saldırıdan etkilenen Microsoft ürünleri:**

* Windows Vista
* Windows Server 2008
* Windows 7
* Windows Server 2008 R2
* Windows 8.1
* Windows Server 2012 ve Windows Server 2012 R2
* Windows RT 8.1
* Windows 10
* Windows Server 2016
* Windows Server Core yükleme seçeneği

Microsoft, Mart ayında yayınladığı güvenlik bülteni [MS17-010](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) ile bu açığı kapatan bir yama yayınlamıştı. Aynı ay Fortinet de bu açığı tespit edip engelleyen bir [IPS imzasını yayınladı](https://fortiguard.com/encyclopedia/ips/43796). Ayrıca bugün de bu saldırıyı tespit edip engelleyen yeni AV imzalarını yayınladık. Yapılan üçüncü taraf testleri, Fortinet Anti-Virus ve FortiSandbox’ın bu zararlı yazılımı etkili bir şekilde engellediğini kanıtlıyor. IPS ve AV imzalarıyla ilgili detaylı bilgileri bu makalenin sonunda bulabilirsiniz.

**Tüm müşterilerimize aşağıdaki adımları uygulamalarını şiddetle tavsiye ediyoruz:**

* Etkilenen tüm ağlar için Microsoft tarafından yayınlanmış yamayı uygulayın.
* Zararlı yazılımın indirilmesini engellemek için Fortinet AV ve IPS denetimlerinin yanı sıra web filtreleme motorlarının açık olduğundan emin olunuz. Ayrıca bu web filtrelemelerinin komuta ve kontrol sunucularına giden iletişimleri engellediğinden de emin olunuz.
* UDP 137 / 138 ve TCP 139 / 445 portlarındaki iletişimleri izole ediniz.

**Ayrıca kullanıcılara ve şirketlere aşağıdaki önlemleri almalarını tavsiye ediyoruz:**

* Tüm cihazlarınızdaki işletim sistemlerinizi, yazılımlarınızı ve sürümlerinizi yamalamak için düzenli olarak yayınlanan yamaları takip ediniz. Çok fazla kurulu cihazı olan büyük şirketlerin merkezi yama yönetim sistemine geçmesi faydalı olacaktır.
* IPS, AV ve Web Filtreleme teknolojilerini kullanın ve bu teknolojileri sürekli güncel tutun.
* Verilerinizi düzenli olarak yedekleyin. Bu yedeklerin bütünlüğünü doğrulayın, şifreleyin ve doğru çalıştığından emin olmak için yeniden yüklemeleri test edin.
* Tehditleri tespit etmek için gelen ve giden tüm e-postları tarayın ve son kullanıcılara ulaşan çalıştırılabilir dosyaları filtreleyin.
* Antivirüs ve anti-malware programlarınızı genel taramaları otomatik yapacak şekilde ayarlayın.
* E-posta üzerinden aktarılan dosyalar içerisindeki makro eklentileri etkisizleştirin. Microsoft Office eklentilerini açmak için Office uygulamaları yerine Office Viewer gibi araçları kullanın.
* Saldırılara karşı eylem ve iş sürekliliği stratejileri belirleyin. Güvenlik açıkları ile ilgili olarak düzenli değerlendirmeler yapın.

**Eğer şirketiniz fidye yazılım saldırısına maruz kaldıysa yapmanız gerekenler:**

* Fidye yazılımının ağınıza veya paylaşımlı sürücülerinize yayılmasını önlemek için saldırıdan etkilenen cihazlarınızın ağ ile bağlantılarını derhal kesiniz.
* Eğer ağınız bu saldırıya maruz kalmış ise tüm cihazlarınızın ağ ile bağlantısını hemen kesiniz.
* Saldırıdan etkilenmiş ancak kapalı olan cihazlar tamamen zarar görmemiştir. Bu da size temizlik yapmanız, verileri geri kurtarmanız, zararları sınırlandırmanız ve durumun daha da kötüleşmesini önlemeniz için zaman kazandıracaktır.
* Yedekleri internet bağlantısı olmayacak şekilde tutun. Saldırı tespit edildiğinde yedekleme sistemlerinizin internet bağlantısını kapatın ve bu yedeklerinizi tarayarak saldırının buraya sıçramadığından emin olunuz.
* Herhangi bir fidye yazılım saldırısı ile karşılaştığında bunu hemen yasal mercilere bildiriniz ve yardım talep ediniz.

Müşterilerinin güvenliği Fortinet için hayati öneme sahiptir. Yeni zararlı aktivitelere karşı aksiyon almak için son gelişmeleri sürekli ve aktif şekilde izliyoruz. Yeni bir gelişme ortaya çıktığında bunu derhal duyuruyoruz.

**Çözümler**

**IPS İmzası:**

MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution

**Antivirüs imzaları:**

W32/Filecoder\_WannaCryptor.B!tr

W32/WannaCryptor.B!tr

W32/Generic.AC.3EE509!tr

W32/GenKryptik.1C25!tr

**CVE güvenlik açığı veritabanı:**

2017-0143 thru 2017-0148