Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

WannaCry Saldırısından Çıkarılacak Dersler

Genel Bakış

Son günlerde "WannaCry" adında yeni bir siber saldırının haberlerin çok önemli bir kısmını kapladığını farketmişsinizdir. "WannaCry", Birleşik Krallık'taki hastanelerin de aralarında olduğu birçok farklı organizasyona ait 200 binin üzerinde bilgisayara bulaştı ve verilerini şifreledi. Bu saldırının bu kadar çok dikkat çekmesinin birkaç nedeni var. İlk nedeni, Windows işletim sistemlerinin bilinen bir açığını kullanarak bilgisayardan bigisayara çok hızlı bir şekilde yayılmış olması.

Konuk Yazar

Dr. Johannes Ullrich SANS Teknoloji Enstitüsü'nde Araştırma Dekanı ve Dshield.org sitesinin kurucusudur. Kendisi aynı zamanda güncel siber güvenlik tehditlerini izleyen **SANS Internet Storm Center** 'ın da sorumlusu ve Web Uygulamaları Güvenliği (**DEV522**), Saldırı Tespit (**SEC503**) ve IPv6 (**SEC546**) derslerinin eğitmenidir.

İkinci nedeni, saldırının kötü niyetli yazılım türlerinden olan Fidye Yazılım (ramsomware) türünde olması ve bilgisayarınıza bulaştığında tüm verilerinizi şifreleyerek, erişememenizi sağlaması. Bu durumda, verilerinizi geri kurtarmanızın tek yolu ya yedeklerinizden geri dönmek ya da saldırganlara istedikleri 300 dolarlık fidyeyi ödeyerek, şifreledikleri veriyi açmalarını beklemek. Üçüncü ve belki de en önemli nedeni ise, bu saldırının aslında hiç gerçekleşemeyebilecek olması. Microsoft, WannaCry saldırısında kullanılan açıklığı gayet iyi biliyordu ve yamalarını aylarca önceden hazırlayıp yayınlamıştı. Ancak birçok organizasyon ya bu yamaları uygulamayı başaramadı ya da desteği yıllardır devam etmeyen Windows XP gibi eski işletim sistemlerini kullanmaya devam etti. Sizlerle "WannaCry" benzeri saldırıların sizi asla etkilememelerini sağlayacak 3 basit adım paylaşmak istiyoruz.

Yama Yönetimi

Öncelikle bilgisayarlarınızın, mobil cihazlarınızın, uygulamalarınızın ve internete bağlı herşeyinizin "güncel" olduğundan emin olun. Siber suçlular, sürekli olarak sizin kullandığınız cihazlardaki yeni açıklıkları arıyorlar. Buldukları anda da, cihazlarınıza sızmak için özel programlar kullanıyorlar. Bu sırada kullandığınız yazılımları üreten kurumlar da, sürekli yeni yamalar yayınlayarak bu açıklıkları kapatmak için uğraşıyorlar. Sizler de bilgisayarlarınız ve mobil cihazlarınıza bu yamaları kurarak, siber saldırganların işini zorlaştırabilirsiniz. WannaCry'ın yayılımında endişe verici olan da buydu. Saldırıyı durdurmak için gerekli olan yamalar neredeyse 2 ay öncesinde Microsoft tarafından yayınlanmıştı. Eğer organizasyonlar başarılı bir yama yönetimi yaparak bilgisayarlarını güncel tutmuş olsalardı, bu saldırı asla başarıya ulaşamazdı. Cihazlarınızın sürekli güncel kaldığından emin olmak için mümkün olan her durumda "otomatik güncelleme" seçeneklerini aktif yapın. Bu kural sadece bilgisayarlarınız ve mobil cihazlarınız için değil, internete bağlı akıllı televizyonlarınız, ev ağı cihazlarınız, oyun konsollarınız

WannaCry Saldırısından Çıkarılacak Dersler

ve belki de arabanız için de geçerli. Eğer işletim sistemleriniz ya da cihazlarınız çok eski ve artık güvenlik yamaları ile desteklenmiyorsa (Windows XP gibi), onları desteklenen yenileri ile değiştirin.

Kendinizi WannaCry gibi saldırılardan korumanın anahtarı şu 3 adımdır; bilgisayarlarınızı güncel tutun, oltama saldırıları hakkında dikkatli olun, sistemlerinizi düzenli olarak yedekleyin.

Yedeklemeler

Bazı durumlarda fidye yazılımları ile yapılanlara benzer siber saldırılar, güncel sistemleri de etkileyebilir. Bu durumda yedeklemeleriniz kurtarıcınız olabilir. Yedeklemeleriniz, bilgisayarlarınız ya da mobil cihazlarınızın bilgilerinin başka bir yerde saklanan kopyalarıdır. Değerli verilerinizi kaybettiğinizde, yedeklemelerinizden geri kurtarabilirsiniz. Maalesef birçok insan basit ve ucuz olmasına rağmen, düzenli yedekleme yapmakta başarılı değil. Verilerinizi yedeklemenin iki yöntemi var : fiziksel ortamlar ya da bulut tabanlı saklama hizmetleri. İki yaklaşımın da avantaj ve dezavantajları var. Eğer hangisini seçeceğinizden emin değilseniz, ikisini de aynı anda kullanabilirsiniz.

Fiziksel ortamlar sizin kontrolünüzde olan harici USB cihazlar ya da evinizde veya ofisinizdeki Wi-Fi erişimli ağ cihazları olabilir. Bu yaklaşımın avantajı büyük miktarda veriyi çok hızlı yedekleyip, kurtarabilmenizdir. Dezavantajı ise eğer orjinal verilerinize fidye yazılımları gibi kötü niyetli bir yazılım bulaşırsa, yedeklerinize de bulaşma ihtimalinin yüksek olmasıdır. Fiziksel ortamlara yedekleme yapıyorsanız, yedeklerinizin kopyalarını dışarıda güvenli bir yerde saklamalısınız. Sakladığınız yedeklemelerinizin uygun şekilde etiketlendiğinden de emin olun. Bulut tabanlı depolama çözümleri, yedeklenen dosyalarınızın internette herhangi bir yerde tutulduğu bir hizmettir. Genel olarak bilgisayarınıza bir uygulama kurarak başlarsınız. Bu yaklaşımın avantajı kullanım kolaylığıdır. Aynı zamanda fidye yazılımlarından etkilendiyseniz, bu durum bulut tabanlı yedeklemelerinize yansımayacaktır. Dezavantajı ise büyük miktarda veriyi yedekleme ve kurtarma sürecinin uzun sürüyor olmasıdır. Ayrıca, bulut tabanlı hizmetlerdeki gizlilik ve güvenlik konularını araştırdığınızdan emin olun. Acaba yedekleme hizmet sağlayıcınız verilerinizi şifrelemek ve güçlü erişim kontrolleri uygulamak gibi önemli güvenlik kontrollerini uyguluyor mu?

Oltalama Saldırıları

Suçlular her zaman saldırı yöntemlerini güncelliyor ve değiştiriyor. Ancak siber suçlular genellikle kurbanlarını tuzağa düşürmek için “oltalama saldırıları (phishing)”nı kullanıyorlar. Bu saldırılar, siber suçluların bir e-posta ile sizi kandırarak kötü niyetli bir yazılım içeren ekli dosyaları açmanızı ya da bağlantıları tıklamanızı isteyerek gerçekleştiriliyor. Bunu yaptığınızda,

WannaCry Saldırısından Çıkarılacak Dersler

bilgisayarınıza bulaşıyor. WannaCry doğrudan bu yöntemi kullanmadıysa da, birçok fidye yazılımı ve diğer kötü niyetli yazılımın bu şekilde bulaştığını biliyoruz. Ek olarak, WannaCry'ı geliştiren saldırganların önümüzdeki aylarda oltamala saldırıları gibi teknikler kullanarak daha fazla bilgisayara bulaşmayı sağlayacak güncellemeleri yapacaklarına şüphe yok. Bu tarz e-posta tabanlı saldırılarda kendinizi korumanın anahtarı "sağduyu". Eğer bir e-posta tuhaf, şüpheli ya da gerçek olamayacak kadar iyi görünüyorsa, muhtemelen bir saldırıdır.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SxANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce (https://tr.linkedin.com/in/semayuce), Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Kötü Amaçlı Yazılım Nedir ?:	https://securingthehuman.sans.org/ouch/2016#march2016
Fidye Yazılımları:	https://securingthehuman.sans.org/ouch/2016#august2016
Yedeklemeler:	https://securingthehuman.sans.org/ouch/2015#august2015
Oltalama Saldırıları:	https://securingthehuman.sans.org/ouch/2015#december2015
Bulutu Güvenle Kullanmak:	https://securingthehuman.sans.org/ouch/2016#november2016

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley