Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Kötü Amaçlı Yazılım Nedir?

Genel Bakış

İnsanlar siber güvenlik ile ilgili konuşuyorken virüs, trojen, fidye yazılımı (ransomware) ya da korsanlık amaçlı programlar (rootkit) gibi terimleri duymuş olabilirsiniz. Bu kelimelerin hepsi aynı şeyi anlatmaktadır: siber suçluların bilgisayarlara ve cihazlara bulaştırmak için kullandıkları çeşitli programlar. Kötü amaçlı yazılım (malware), tüm bu farklı programların hepsini tanımlamak için yaygın bir terim olarak kullanılır. Bu sayıda kötü amaçlı yazılımın ne olduğunu, kimin bu yazılımları yazdığını, neden yazdıklarını ve en önemlisi ise kendinizi bunlara karşı korumak için ne yapabileceğinizi açıklayacağız

Konuk Yazar

Cheryl Conley, Lockheed Martin'de 100.000'den fazla çalışana ulaşan "Ben (The "I" ™)" kampanyasının ve Güvenlik Eğitimi ve Farkındalığı ekibinin yöneticisidir. Bu kampanya oltama saldırıları ile mücadele eden kurum çapındaki odak grupların birlikteliği ve savunuculuğunu da kapsıyor. Cheryl'i **@conleychera** hesabından takip edebilirsiniz.

Kötü Amaçlı Yazılım Nedir?

Basitçe söylemek gerekirse, kötü amaçlı yazılım (malware), bir bilgisayar programı, kötü niyetli eylemleri gerçekleştiren bir yazılımdır. Hatta İngilizce'de "malware" terimi, "malicious" ve "software" kelimelerinin birleşimi ile oluşturulmuştur. Siber suçlular, kötü amaçlı yazılımı kontrolü ele geçirmek veya içindeki bilgilere ulaşmak için sizin bilgisayarınız ya da cihazlarınıza kurarlar. Bir kere yüklendikten sonra bu saldırganlar kötü amaçlı yazılımı çevirim-içi işlemlerinizi gözetlemek, şifrelerinizi ya da dosyalarınız çalmak veya sizin sisteminizi kullanarak diğerlerine saldırmak için kullanırlar. Hatta kötü amaçlı yazılım, kendi dosyalarınıza erişiminizi engelleyerek bu dosyalara tekrar erişmek için saldırgana fidye ödeme yapmanızı talep edebilir.

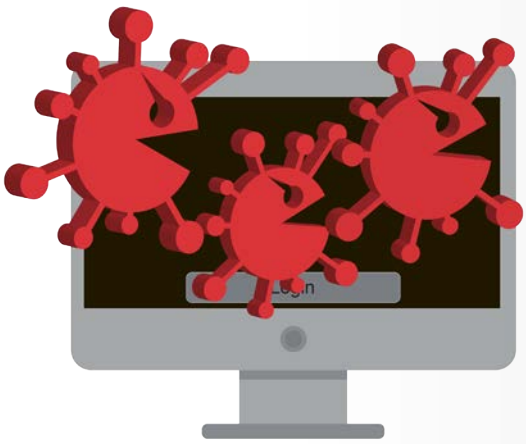
Birçok kişi kötü amaçlı yazılımın sadece Windows yüklü bilgisayarların bir problemi olduğu yanılgısını taşımaktadır. Windows yaygın bir kullanıma sahip iken, ki bu yüzden büyük bire hedeftir, kötü amaçlı yazılım Mac bilgisayarlar, akıllı telefonlar ya da tabletler gibi her cihaza bulaşabilir. Siber suçlular ne kadar çok bilgisayar ve cihaza kötü amaçlı yazılımı bulaştırırlarsa o kadar çok para kazanırlar. Bu yüzden siz dahil herkes hedeftir.

Kötü Amaçlı Yazılımları Kim Yazıyor?

Kötü amaçlı yazılım artık sadece meraklı hobiciler ya da amatör korsanlar tarafından değil, tecrübeli siber suçlar tarafından yazılmaktadır. Amaçları, belki sizden çaldıkları verileri satarak, spam e-postalar göndererek, hizmeti engelleme saldırıları (denial of service attacks) yaparak ya da şantaj yaparak bulaştırdıkları bilgisayar ya da cihazlardan para kazanmaktır. Kötü amaçlı yazılımları yazan, dağıtan ve bundan yarar sağlayan kişiler, kendi kendine hareket eden kişiler ile iyi örgütlenmiş suçlu grupları

Kötü Amaçlı Yazılım Nedir?

arasında dağılım gösterir. Komplike kötü amaçlı yazılımları yazanlar çoğunlukla bu işe kendilerini adamışlar, tam zamanlı olarak bu tip yazılımları geliştirmektedirler. Ayrıca, bir kez kötü amaçlı yazılımı yazdıklarında çoğunlukla bunu diğer kişilere veya organizasyonlara satarlar. Hatta "müşterilerine" düzenli olarak güncelleme ve destek sağlayarak.



Şüpheli mesajlara karşı kuşkucu davranarak, cihazlarınızı günce tutarak ve fırsat oldukça güncel anti-virüs yazılımlarını yükleyerek kötü amaçlı yazılımlardan kendisiniz koruyun.

Kendinizi Korumak

Kendinizi korumak için güvenilir sağlayıcılardan anti-virüs yazılımları yüklemek kullanılan yaygın bir adımdır. Bu gibi araçlar, bazen "kötü yazılıma karşı olan yazılımlar" olarak da adlandırılan, kötü amaçlı yazılımları tespit etmek ve durdurmak üzerine tasarlanmışlardır. Ancak, anti-virüs yazılımları tüm kötü amaçlı yazılımları engelleyerek kaldıramamaktadır. Siber suçlular, tespiti engellemek için sürekli yenilikler ve değişiklikler yaparak yeni ve daha karmaşık yazılımlar yazmaktadırlar. Bunu karşılığında da anti-virüs sağlayıcıları yeni kötü amaçlı yazılımların tespiti için yeni kabiliyetler ekleyerek ürünlerini sürekli olarak güncellemektedirler. Bu bir çok bakımdan iki tarafın birbirini alt etmek istediği bir silahlanma yarışına dönüşmektedir. Ne yazık ki kötü adamlar genellikle bir adım öndedir. Bu yüzden sadece anti-virüs programlarına bel bağlayamazsınız, kendinizi korumak için alabileceğiniz ek tedbirler aşağıda anlatılmaktadır:

- Siber suçlular, çoğunlukla bilgisayar ve tabletlerde yüklü yazılımların açıklarından yararlanarak cihazlarınıza kötü amaçlı yazılımı bulaştırırlar. Ne kadar güncel bir sisteminiz var ise sisteminizde o kadar az açık bulunmaktadır ki bu da siber suçluların kötü amaçlı yazılımı bulaştırmalarını zorlaştırır. Bu yüzden işletim sisteminizin, uygulamalarınızın ve cihazlarınızın güncellemeleri otomatik olarak yüklemelerinin etkin olduğundan emin olun.
- Sibel suçluların mobil cihazlarınıza kötü yazılım bulaştırmada kullandıkları bilindik yol, sahte bir uygulama yaratıktan sonra internete koyarak insanların bu programı indirmesi ve yüklemesi için kandırmaktır. Bu yüzden sadece güvenilir çevrim-içi mağazalardan uygulama indirin ve yükleyin. Ayrıca sadece uzun zaman önce internete yüklenmiş, büyük bir kitle tarafından yüklenmiş ve birçok olumlu değerlendirmesi olan mobil uygulamaları indirin.
- Bilgisayarlarda "yönetici" ya da "kök (root)" hesapları gibi ayrıcalıklı bir hesap yerine limitli hakları olan standart bir hesap kullanın. Bu birçok kötü amaçlı yazılımın kendini yüklemesini engelleyerek ek bir koruma sağlayacaktır.
- Siber suçlular genellikle insanları onların yerine kötü amaçlı yazılımları yüklemeleri için kandırırlar. Örneğin, görünüşte geçerli, bir eki ya da bağlantı içeren bir e-posta gönderirler. Belki de bu e-posta bankanızdan ya da arkadaşınızdan geliyormuş gibi görünebilir. Ancak eğer ekli dosyayı açarsanız ya da bağlantıyı tıklarsanız, kötü amaçlı yazılımın yüklenmesini tetikleyen kodu aktive etmiş olursunuz. Eğer bir mesaj güçlü bir aciliyet hissi yaratıyorsa, kafa karıştırıcıysa ya da fazlasıyla iyiyse, o zaman bu bir saldırı olabilir. Şüpheci olun, sağduyu genelde sizin en iyi savunmanızdır.

Kötü Amaçlı Yazılım Nedir?

- Düzenli olarak sisteminizi, dosyalarınızı bulut tabanlı servislere yedekleyin ya da yedeklerinizi örneğin harici bellek kullanarak çevrim-dışı saklayın. Bu, kötü amaçlı yazılımların dosyalarınızı şifreleme ya da silme girişimleri durumunda yedeklerinizi korumanızı sağlayacaktır. Yedeklemeler kritiktir ve çoğunlukla kötü yazılımların bulaşma durumlarından kurtulmanın tek yoludur.

Sonuç olarak, kötü amaçlı yazılımlara karşı kendinizi savunmanın en iyi yolu, yazılımları güncel tutmak, iyi bilinen sağlayıcılardan güvenilir anti-virüs yazılımları yüklemek ve sisteminize kötü amaçlı yazılım bulaştırmak için herhangibirinin sizi kandırabileceği konusunda alarm durumunda olmaktır.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS 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, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Oltalama:	https://securingthehuman.sans.org/ouch/2015#december2015
Sosyal Mühendislik:	https://securingthehuman.sans.org/ouch/2014#november2014
Mobil Uygulamalarını Güvenli Kullanmak:	https://securingthehuman.sans.org/ouch/2015#january2015
Yeni Tabletinizi Güvenli Hale Getirmek:	https://securingthehuman.sans.org/ouch/2016#january2016
Yedeklemeler:	https://securingthehuman.sans.org/ouch/2015#august2015

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis