Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Kötü Amaçlı Yazılımlar Nelerdir?

Özet

İnsanlar siber güvenlik hakkındakonuşuyorken virüs, solucan, trojen ya da rootkit (korsan amaçlı işletim sisteminde arka tarafta çalışan gizli programlar) gibi isimlendirmeleri duymuş olabilirsiniz. Bu isimlendirmeler, siber suçlular tarafından mobil cihazlara ve bilgisayarların yönetimini ele geçirmek için kullandıkları farklı türlerdeki yazılımları tanımlamaktadırlar. Bugün bu isimlendirmeler tek bir isim altında "kötü amaçlı yazılım" olarak adlandırılmaktadır. Bu sayıda, kötü amaçlı yazılımın ne olduğunu, kimlerin bu yazılımları geliştirdiğini ve geliştirme nedenlerini ve bu yazılımlara karşı kendinizi nasıl koruyacağınızı açıklayacağız.

Konuk Editör

Lenny Zeltser NCR Corp'da özellikle müşterilerinin Bilgi Teknolojileri (BT) çalışmalarının korunmasında çalışmakta ve kötü amaçlı yazılımlarla savaş konusunda SANS Enstitüsünde ders vermektedir. Lenny'i Twitter'da **@lennyzeltser**'den ve **blog.zeltser.com** güvenlik günlüğünden takip edebilirsiniz.

Kötü Amaçlı Yazılım Nedir?

Basitçe kötü amaçlı yazılım zararlı işlemleri yapmaya yarayan bir bilgisayar programıdır. İngilizce'de "malware" olarak bilinen bu yazılımlar, yine İngilizce "malicious" ve "software" kelimelerinin birleşiminden ortaya çıkmıştır. Siber suçluların nihai amacı kötü amaçlı yazılımları bilgisayarınıza ya da mobil cihazlarınıza yüklemektir. Bu programlar bir kez yüklendiğinde bu saldırgan kişiler büyük olasılıkla cihazlarınızın bütün kontrolünü ele geçirir. Çoğu insan, kötü amaçlı yazılımların sadece Windows tabanlı işletim sistemine sahip bilgisayarların problemi olduğu yanılgısındadır. Windows yaygın olarak kullanıldığı için büyük bir hedef oluşturduğundan kötü amaçlı yazılımlar akıllı telefonlar ve tabletler dahil birçok cihaza bulaşabilir. Hatta kötü amaçlı yazılımların mobil cihazlara buluşma sıklığı durmadan artmaktadır. Ancak unutmayın, siz dahil herkes bir hedeftir. Sibel suçlular ne kadar çok bilgisayar ve mobil cihaza kötü amaçlı yazılım bulaştırırsa o kadar çok para kazanabilirler. Bu suçlular genellikle bu yazılımları bulaştırabildikleri kadar çok kişiye bulaştırdıkları sürece kim olduklarını önemsemezler.

Kim ve Neden

Kötü amaçlı yazılımlar artık sadece meraklılar ya da amatör bilgisayar korsanları tarafından değil, belli ve özel amaçlara ulaşmak için bilgili ve uzman siber suçlular tarafından yazılıyorlar. Bu amaçlardan bazıları gizli bilgilerin çalınması, oturum bilgileri ve şifrelerin toplanması, spam maillerin atılması, hizmet dışı bırakma saldırılarının yapılması, para sızdırma ya da kimlik çalmadır. Örneğin, Cryptolocker olarak bilinen kötü amaçlı yazılım siber suçlular tarafından bilgisayarınızdaki tüm dosyaları şifrelemek için kullanılır. Bir kez bu yazılımı bulaştırıp dosyaları şifreledikten sonra siber suçlular dosyalarınızın şifrelerini çözmeleri karşılığında fidye isterler.

Kötü Amaçlı Yazılımlar Nelerdir?

Kötü amaçlı yazılımları yazan, yayan ve bundan yararlananlar, bireysel olarak çalışanlar ile iyi organize olmuş suçlu grupları ya da devlet kurumları arasında dağılım göstermektedir. Günümüzde karmaşık kötü amaçlı yazılımlar yazan kişiler genellikle bu amaçla tam zamanlı olarak çalışmaktadırlar. Aslına bakılırsa bu kişiler kötü amaçlı yazılımları geliştirdikten sonra genellikle diğer kişi ya da organizasyonlara satmaktadırlar ve düzenli olarak güncellemeler yaparak "müşterilerine" destek sağlamaktadırlar. Bu tür yazılımlar bir kez alındığında diğer suçlular, bu yazılımları milyonlarca kurbanın sistemine yükleyerek ve bu bulaşmış bilgisayarlardan bir ağ (botnet) yaratarak para kazanırlar. Böylece siber suçluların kendi amaçları için kullanabilecekleri ya da diğer suçlulara satabilecekleri bu ağ, uzaktan kontrol edilebilir bir ordu haline gelir.

Kötü amaçlı yazılımlara karşı kendinizi korumanın en iyi yolu cihazlarınızın güncel olduğundan, geçerli bir virüse karşı koruma yazılımının yüklü olduğundan emin olmanız ve son olarak da saldırılara karşı tetikte olmanızdır.

Kendinizi Koruma

Bilgisayarlarınızı ve mobil cihazlarınızı kötü amaçlı yazılımlardan korumanın yaygın bir yolu güvenilir sağlayıcıların virüslere karşı koruma yazılımlarını (anti-virus) yüklemektir. Kötü amaçlara karşı koruma yazılımları (anti-malware) olarak da adlandırılan virüslere karşı koruma yazılımları, kötü amaçlı yazılımlarını saptamak ve durdurmak için tasarlanmış güvenlik yazılımlarıdır. Ancak virüslere karşı koruma yazılımları tüm kötü amaçlı yazılımları engelleyemez ya da kaldıramazlar. Siber suçlular sürekli olarak virüslere karşı koruma programlarını atlatmak için yenilikler yaparak karmaşık saldırılar geliştirirler. Bunun üzerine virüslere karşı koruma yazılım sağlayıcıları ise yeni ortaya çıkan kötü amaçlı yazılımlarını tespit etmek için sürekli olarak ürünlerini yeni özellikler ile güncellerler. Birçok açıdan bu, bir tarafın zekası ile diğer tarafı alt etmeye çalıştığı bir silahlanma yarışına benzer. Maalesef siber suçlular neredeyse her zaman galip gelirler. Gerçekte, virüslere karşı koruma yazılımı sağlayıcıları birçok kötü amaçlı yazılım tespit ederek engelliyorken saldırganların her zaman bu yazılımların yeni versiyonlarını hazırlıyor olduklarını hatırlayın. Sonuç olarak sadece virüslere karşı koruma yazılımların sizi koruyacağına güvenemezsiniz, kendinizi korumanız için ek tedbirler almanız gereklidir.

İlk olarak, işletim sisteminizin ve uygulamalarınızın otomatik olarak güvenlik güncellemelerini yüklediğinden emin olun. Yazılımlarınız ne kadar güncel olursa siber suçluların bilgisayar ya da mobil cihazlarınıza kötü amaçlı yazılım bulaştırmaları o kadar zor olacaktır.

İkinci olarak, sizin kötü amaçlı yazılımlara karşı kendinizi en iyi savunacaklardan biri olduğunuzu unutmayın. Kötü amaçlı yazılım bulaşma vakaları, genellikle saldırganların sizi kandırarak kötü amaçlı yazılımları kendiliğinizden yüklemenizi sağlayan sosyal mühendisliği içerir. Bunun bir yaygın örneği oltalama saldırılarıdır. Bunlar bilgisayarınıza kötü amaçlı yazılım bulaştırmak için sizi kandırmaya yönelik tasarlanmış gerçek gibi görünen sahte e-postalardır. Mesela, bir siber suçlu bir bankadan geliyormuşçasına bir bağlantının üzerini tıklamanızı isteyen bir e-posta gönderebilir. Eğer bağlantıyı tıklarsanız, bilgisayarınızı ele geçirmeye ve kötü amaçlı yazılım

Kötü Amaçlı Yazılımlar Nelerdir?

bulaştırmaya çalışan bir ağ sayfasına yönlendirilirsiniz. Ya da size paketinizin gönderilemediğini belirten ve açıldığı anda bilgisayarınızı bozacak olan bir takip dokümanını indirmenizi isteyen bir e-posta gönderebilirler. Sosyal mühendislik saldırıları telefonlar gibi diğer teknolojiler için de geçerlidir. Örneğin, bilgisayar korsanları sizi arayıp Microsoft teknik destekten arıyormuş gibi yaparak bilgisayarınıza kötü amaçlı yazılım bulaştığını söyleyebilirler. Hikayeleri baştan sona yalandır ve bilgisayarınızla ilgili herhangi bir sorun yoktur. Amaçları sizi kandırarak bilgisayarınıza kötü amaçlı yazılımın bulaştığına inandırmak, sonra sizin sisteminize uzaktan ulaşım bilgilerini sizden almak ya da aslında kötü amaçlı yazılım olan kendi güvenlik yazılımlarını almanız için sizi oyuna getirmeye çalışmaktır. Sağduyunuzu kullanın. Eğer bir telefon araması ya da mesajı tuhaf, şüpheli ya da inanılmayacak kadar iyi geliyorsa o zaman büyük olasılıkla kandırılmaya çalışılıyorsunuzdur.

Sonuç olarak, kötü amaçlı yazılımlara karşı kendinizi savunmanızın en iyi yolu yazılımlarınızı güncel tutmak, iyi bilinen sağlayıcılardan aldığınız güvenilir virüse karşı koruma yazılımları yüklemek ve bilgisayarınıza kötü amaçlı yazılım yüklemek için sizi oyuna getirecekler için tetikte 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

OUCH Oltalama:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH Bilgisayarınızı Koruma:

www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

Siz Hedefsiniz:

http://www.securingthehuman.org/resources/posters

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