Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Ele Geçirildim, Şimdi Ne Olacak?

Giriş

Bilgisayarınızı ve bilgilerinizi koruma konusunda endişelendiğinizi ve onları güvenli tutmak için önlemler aldığınızı biliyoruz. Ancak, araba kullanmak gibi, ne kadar güvenli kullanırsanız kullanın, eninde sonunda bir kazaya karışabilirsiniz. Bu sayıda, bilgisayarınızın ele geçirilmiş olduğuna kanaat getirmek için nelere bakmanız gerektiğine ve eğer ele geçirilmişse bu konuda neler yapabileceğinizi açıklayacağız. Sonuçta bilgisayarınızın ele geçirildiğini ne kadar hızlı farkederseniz bu duruma o kadar hızlı cevap verir, size ve çalıştığınız şirkete kötü etkilerini o kadar iyi yönetisiniz.

Konuk Yazar

Jake Williams (@MalwareJake; malwarejake.blogspot.com) CSRgroup Computer Security Consultants'da başuzmandır ve ayrıca SANS'da verilen Memory Forensics (FOR526) ve Malware Reverse Engineering (FOR610) derslerinin ortak yazarıdır.

Ele Geçirildiğinizin Belirtileri

Bilgisayarınızın ele geçirilip geçirilmediğine karar vermek için çoğu durumda tek bir adımın yeterli olmadığını bilmelisiniz. Hatta genelllikle birden fazla belirti vardır. Eğer bu belirtilerin bir kombinasyonuna rastlarsanız, bu sizin bilgisayarınızın ele geçirildiğine işaret eder. Aşağıda bir kaç örnek verilmiştir:

- Anti-virüs programınız bilgisayarınıza kötü amaçlı bir yazılım bulaştığını belirten bir alarm vermiştir ve özellikle etkilenmiş dosyaların kaldırılamadığını ya da karantina altına alınamadığını söylüyordur.
- Tarayıcınızın ana sayfası beklenmedik bir şekilde değişmiştir ya da tarayıcınız sizi gitmek istemediğiniz bir ağ sayfasına yönlendiriyordur.
- Daha önce yaratmadığınız yeni hesaplar bilgisayarınızda belirmiştir.
- Daha önce yüklemediğiniz yeni programlar çalışıyordur.
- Bilgisayarınız devamlı olarak olağandışı kapanıyordur ya da çok yavaş çalışıyordur.
- Siz bilfiil bir uygulama yüklememenize ya da varolan bir uygulamayı güncellememenize rağmen bilgisayarınızdaki bir program sisteminizde değişiklikler yapmak için sizden izin istiyordur.
- Güvenlik duvarınız sizin tanımadığınız bir programın internet erişim izni istediği uyarısını veriyordur.

Nasıl Karşılık Vermelisiniz?

Eğer bilgisayarınızın ele geçirildiğine kanaat getirdiyseniz, ne kadar hızlı müdahale ederseniz o kadar iyi olacaktır. Eğer kullandığınız bilgisayar işvereniniz tarafından size verildiyse ya da iş amaçlı kullanılıyorsa, kendi kendinize düzeltmeyi denemeyin ve bilgisayarı kapatmayın. İyi birşey yapayım derken sadece durumu

Ele Geçirildim, Şimdi Ne Olacak?

daha kötüleştirmekle kalmazsınız değerli bir kanıtı da yok edebilirsiniz. Bunun yerine, genellikle yardım masası, güvenlik takımı ya da danışmanı ile iletişime geçerek hemen bu durumu işvereninize bildirin. Eğer herhangi bir nedenle şirketiniz ile iletişime geçemiyorsanız ya da gecikme durumundan endişeli iseniz o zaman bilgisayarınızın ağ ile bağlantısını kesin ve uyku moduna alın. Bilgisayarınızın ele geçirilip geçirilmediğinden emin olmasanız bile bunu her ihtimale karşı raporlamanız en iyisi olacaktır. Çok büyük ihtimalle şirketinizin bu durumların üstesinden gelecek süreçleri ve bir takımı vardır, bırakın onlar bu durumla başa çıksınlar.

Eninde sonunda bilgisayarınız ele geçirilebilir, bu durumu ne kadar hızlı farkederseniz, o kadar erken önlem alırsınız ki bu da en iyisidir.

Eğer bilgisayarınız sizin kişisel kullanımınızda ise, kendinizin takip edebileceği bazı adımlar şöyledir:

- **Yedeklemeler**. Yedekleme yaparak hazırlıklı olmak takip edebileceğiniz en önemli adımdır. Verilerinizi özellikle düzenli olarak yedekleyin ve periyodik olarak yedekleme dosyalarını geri yükeleyip yükeleyemediğinizi kontrol edin. Çoğu zaman bir bilgisayar ele geçirildiğinde tek seçeneğiniz sabit diskinizi silip yeniden işletim sistemi kurmak ya da yeni bilgisayar almaktır. Her durumda kişisel bilgilerinizi kurtarmak için yedeklerinize ihtiyacınız vardır.
- **Şifrelerinizi Değiştirin**. Tüm şifrelerinizi değiştirdiğinizden emin olun. Bu sadece bilgisayarınızdaki ve mobil cihazlarınızdaki şifreleri değil tüm çevrim-içi şifrelerinizi kapsar. Tüm çevrim-içi şifrelerinizi güvenli olduğunu bildiğiniz farklı bir bilgisayarı kullanarak değiştirin.
- **Anti-virus Programları**. Eğer anti-virüs programınız kötü yazılım bulaşmış bir dosya hakkında sizi bilgilendiriyorsa programınızın önerdiği eylemleri takip edebilirsiniz. Bu eylemler genellikle dosyaları karantina altına almayı, dosyayı temizlemeyi ya da silmeyi içermektedir. Çoğu anti-virüs programı size bulaşmış kötü amaçlı yazılım hakkında daha fazla bilgiye ulaşabileceğiniz bağlantılar sunacaktır. Eğer şüpheye düşerseniz dosyayı karantina altına alın. Eğer bu mümkün değilse silin.
- **Geri yükleme**. Eğer anti-virüs programı ile bilgisayarınızı temizleme imkanınız yok ise bilgisayarınızı kurtarmanın en güvenli yollarından biri bilgisayarınızı yeni baştan kurmaktır. İlk olarak bilgisayarınızın ağ bağlantısını kesin. Daha sonra sistem üreticinizin direktiflerini takip edin, bu çoğu zaman işletim sisteminin yeniden yüklenmesi için hazırda var olan kurtarma bölümünün kullanılması anlamına gelir. Eğer kurtarma bölümü kayıp, bozuk ya da kötü amaçlı yazılım içeriyor ise o zaman üreticinizle iletişime geçin ve kurtarma DVD'si göndermelerini isteyin. Yedeklerinizden işletim sistemi yüklemeyin. Çünkü yedekleriniz, saldırganların sizin bilgisayarınıza ulaşmak için daha önce yararlandığı zafiyetler içeriyor olabilir. Yedeklerinizi sadece kişisel verilerinizi kurtarmak için kullanın. Ayrıca, eğer bilgisayarınız eski bir

Ele Geçirildim, Şimdi Ne Olacak?

teknolojiye sahipse bilgisayarınızı yeniden kurmak için saatler harcamak yerine yeni bir bilgisayar almak daha ucuz ve kolay olacaktır.

- **Uzman Yardımı**. Eğer bilgisayarınızın ele geçirildiğinizden endişe duyuyorsanız ama bunun üstesinden gelecek kadar bilgi ve beceriye sahip olmadığınızı düşünüyorsanız, bilgisayarınızı bir uzmana teslim etmek isteyebilirsiniz. Örneğin, bilgisayarınız ele geçirildikten sonra yedeklerinizin eksik ya da eski olduğunu farkedebilirsiniz. Fotoğraf, doküman ve video gibi kritik dosyalarınızı kötü yazılım bulaşmış bilgisayarınızdan yeni bilgisayarınıza aktarmak isteyebilirsiniz. Ancak bunu yaparak kazara kötü yazılımları da aktarabilir, aynı zamanda yeni bilgisyarınıza da bu kötü yazılımları bulaştırabilirsiniz. En güvenli seçenek kötü yazılım bulaşmış olan bilgisayarınızı, dosyalarınızı güvenli bir şekilde kurtaracak bilgili bir teknisyene götürmenizdir.

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! Yedeklemeler:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Şifreler:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Kötü Amaçlı Yazılımlar Nelerdir?:	http://www.securingthehuman.org/ouch/2014#february2014
Zararları Farketme Posteri:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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