Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Ele Geçirildim, Şimdi Ne Olacak?

Giriş

Bilgisayarınızı ve mobil cihazlarınızı koruma konusunda endişelendiğinizi ve onları güvenli tutmak için önlemler aldığınızı biliyoruz. Ancak, teknolojiyi ne kadar güvenli kullanırsanız kullanın, eninde sonunda ele geçirilebilirsiniz. Bu sayıda, bilgisayarınızın ya da mobil cihazınızın ele geçirilmiş olduğuna kanaat getirmek için nelere bakmanız gerektiğini ve eğer ele geçirilmişse bu konuda neler yapabileceğinizi açıklayacağız. Sonuçta birşeylerin ters gittiğini ne kadar hızlı farkederseniz bu duruma o kadar hızlı cevap verir, ve siber saldırganların yol açabileceği zararı azaltabilirsiniz.

Konuk Yazar

Samantha Davison (**@sam_e_davison**) Uber'de dünya çapında 350'den fazla şehirdeki çalışanları kapsayan Bilgi Güvenliği Farkındalığı ve Eğitimi Program Müdürüdür.

Ele Geçirildiğinizin Belirtileri

Ele geçirilip geçirilmediğinize karar vermek için çoğu durumda tek bir adımın yeterli olmadığını bilmelisiniz. Hatta genelllikle birden fazla belirti vardır. Bu belirtilere ne kadar yaklaşırsanız, ele geçirilmiş olma ihtimaliniz o kadar yüksektir.

- 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 ya da daha önce yüklemediğiniz yeni programlar çalışıyordur.
- Bilgisayarınız ya da uygulamalarınız devamlı olarak olağandışı kapanıyordur, bilmediğiniz uygulamalara ait ikonlar belirmiştir ya da garip pencereler açılıyordur.
- Siz bilfiil bir uygulama yüklememenize ya da varolan bir uygulamayı güncellememenize rağmen bilgisayarınızdaki bir program sisteminizde değişiklikler yapmak için sizden izin istiyordur.
- Parolanızın doğru olduğundan emin olmanıza rağmen, sisteminize ya da çevrimiçi bir uygulamaya girmeye çalıştığınızda parolanız gerçersiz olmuştur.
- Arkadaşlarınız sizin hiç göndermediğiniz gereksiz e-postalardan şikayet ediyordur.
- Mobil cihazınız özel numaralara atılan kısa mesajlar nedeniyle ekstra ücretler oluşturuyordur.

Ele Geçirildim, Şimdi Ne Olacak?

- Mobil cihazınız aniden ve anlaşılamaz yüksek veri ya da pil kullanıyordur.

Nasıl Karşılık Vermelisiniz ?

Eğer bilgisayarınızın ya da mobil cihazınızın 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. İyi birşey yapayım derken sadece durumu 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. Eğer bilgisayarınız ya da mobil cihazınız sizin kişisel kullanımınızda ise, kendinizin takip edebileceği bazı adımlar şöyledir:

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

- **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 ya da cihazı 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.
- **Yeniden Oluşturma**: Eğer sisteminizin kurtarıldığından tamamen emin olmak istiyorsanız ya da sisteminizi kurtaramadıysanız, en güvenli seçenek onu yeniden oluşturmaktır. Bilgisayarlarınız için üreticilerinin talimatlarını izleyin. Birçok durumda bu mevcut yardımcı progrmaları kullanarak işletim sistemini yeniden kurmak anlamına gelir. Eğer bu yardımcı araçlar da olumsuzluktan etkliendiyse, üretici ile iletişime geçin ya da internet sitelerini ziyaret edin. İşletim sisteminizi yedeklerinden geri yüklemeyin zira saldırganın sisteminizi ele geçrimesine neden olan zafiyetler yedeklerinizde de olabilir. Yedeklemeleri sadece verilerinizi geri yüklemek için kullanmalısınız. Mobil cihazlarınız için üretici ya da servis sağlayıcısının internet sitelerinde de yer alan talimatlarını izleyin. Çoğu zaman bu işlem, mobil cihazınızı fabrika ayarlarına döndürmek kadar basit olabilir. Yeniden oluşturma süreci hakkında kendinizi rahat hissetmiyorsanız, size yardımcı olacak bir profesyonel desteği almayı değerlendirin. Ya da bilgisyarınız veya mobil cihazınız eski ise, yenisini almak daha basit

Ele Geçirildim, Şimdi Ne Olacak?

ve uygun fiyatlı bile olabilir. Son olarak, yeniden de oluştursanız, yeni de alsanız, mümkün olan her seçenek için otomatik güncellemelerin açık olduğundan ve tamamıyla güncel sürümleri kullandığınızdan emin olun.

- **Yedeklemeler**: Yedekleme yaparak hazırlıklı olmak takip edebileceğiniz en önemli adımdır. Ne kadar sık yapıyorsanız, o kadar iyidir. Bazı çözümler her saat için değişen ya da yeni oluşturulan her dosyanın yedeğini otomatik olarak alır. Hangi yedekleme çözümünü kullandığınızdan bağımsız olarak verilerinizi özellikle düzenli olarak yedekleyin ve periyodik olarak yedekleme dosyalarını geri yükleyip yükleyemediğinizi kontrol edin. Genellikle ele geçirildiğinizde tek seçeneğiniz yedeklerinizden geri dönerek verilerinizi kurtarmak olacaktır.
- **Kanuni Yaptırımlar**: Eğer herhangi bir şekilde tehdit edildiğinizi hissederseniz, olayı kanuni merciilere raporlayın.

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

Yedeklemeler:	https://securingthehuman.sans.org/ouch/2015#august2015
Parolalar:	https://securingthehuman.sans.org/ouch/2015#april2015
Kötü Niyetli Yazılım Nedir?:	https://securingthehuman.sans.org/ouch/2016#march2016
Yeni Tabletinizi Güvenli Hale Getirmek:	https://securingthehuman.sans.org/ouch/2016#january2016

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