Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Kötü Niyetli Uygulamaları Durdurun

Genel Bakış

Büyük ihtimalle insanlar siber güvenlik konusunda konuştuğunda virüs, Trojan, fidye yazılımı (ransomware) veya rootkit kavramlarından bahsettiğini duymuşsunuzdur. Tüm bu programlar kötü niyetli uygulama olarak isimlendirilen ve siber suçluların bilgisayar ve benzeri cihazları enfekte etmek için kullandıkları kötü niyetli yazılımlardır. Bir kez kurulduklarında siber suçlular ne isterse onu yapabilirler. Kötü niyetli uygulamaların ne olduğunu, ne gibi tehlikeler oluşturduğunu ve en önemlisi kendinizi koruyabilmek için neler yapabileceğinizi öğrenin.

Kötü Niyetli Yazılım (Malware) Nedir?

Basitçe söylemek gerekirse, kötü niyetli işlemler yapmak için kullanılan bir bilgisayar yazılımıdır. Bu terim İngilizcedeki malicious (kötü niyet) ve software (yazılım) kelimelerinin birleşimidir. Siber suçlular kötü niyetli yazılımı sizin bilgisayar yada cihazınızın üzerine onu kontrol edebilmek amacıyla kurarlar. Bir kez kurulduğunda kötü niyetli yazılım suçluların tüm çevrimiçi hareketleriniz üzerinde casusluk yapabilmelerini, parolalarınızı ya da dosyalarınızı çalabilmelerini veya sizin sisteminizi kullanarak başkalarına saldırabilmelerini sağlar. Kötü niyetli yazılım, size ait dosyaların kontrolünü ele geçirebilir ve geri vermek için sizden fidye talep edilebilir. Pekçok insan kötü niyetli yazılımların sadece Windows işletim sistemi kullanan bilgisayarlar için sorun olduğuna inanmaktadır. Maalesef kötü niyetli yazılımlar, Mac bilgisayarlardan akıllı telefonlara, DVR'lerden güvenlik kameralarına kadar herhangi bir cihaza bulaşabilir. Siber suçlular para kazanabilmek için her geçen gün daha fazla bilgisayar ve cihaza kötü niyetli yazılım bulaştırmaktadır. Bu yüzden siz de dahil olmak üzere herkes kötü niyetli kişilerin hedefi haline gelmiştir.

Kendinizi Koruyun – Kötü Niyetli Yazılımları Durdurun

Kötü niyetli yazılımlardan korunmak için antivirüs yazılımları gibi güvenlik programları kurmak zorunda olduğunuzu düşünebilirsiniz. Ancak antivirüs programları bütün kötü niyetli yazılımları durduramamaktadır. Siber suçlular tespit edilmekten kurtulabilmek için sürekli olarak yeni ve daha karmaşık kötü niyetli yazılımlar geliştirmektedir. Bu döngü içerisinde antivirüs yazılım sağlayıcıları da sürekli olarak kötü niyetli yazılımları tespit edebilmek üzere ürünlerini yeni yetkinliklerle güncellemektedir. Bu konu pek çok yönden bir yarışa dönüşmüştür ve kötü niyetli kişiler genellikle bir adım öndedirler. Sadece antivirüs yazılımlarına güvenmeniz yeterli olmayacağından, kendinizi koruyabilmek için alabileceğiniz ek önlemler şunlardır:

Siber suçlular sıklıkla kullandığınız yazılımların zaafiyetlerinden faydalanarak bilgisayar ve cihazlara kötü niyetli yazılım bulaştırırlar. Yazılımlarınız ne kadar güncelse, sistemlerinizde o kadar az zaafiyet vardır ve siber suçluların onlara bulaşması zorlaşır. Her zaman, kullandığınız işletim sistemlerinin, uygulamaların, internet tarayıcınızın, internet tarayıcı eklentilerinizin ve cihazınızın geçerli ve güncel sürümlerde olduğundan emin olun. Uygulamalarınızın her zaman güncel olduğundan emin olmanın en kolay yolu mümkün olan her durumda otomatik güncellemeyi aktif hale getirmektir.

Siber suçluların kötü niyetli yazılımları bilgisayarlar ya da mobil cihazları ele geçirmek için kullandıkları yaygın bir yöntem, sahte bilgisayar uygulamaları ya da mobil uygulamalar geliştirmek, internet üzerinden yayınlamak ve sizi kandırarak programı indirip kurmanızı sağlamaktır. Programları ve uygulamaları sadece güvenilir çevrimiçi mağazalardan indirip kurun. Ayrıca yeni yayınlanmış, hakkında sadece birkaç olumlu görüş olan, nadiren güncelleme yapılan veya sadece çok sınırlı sayıda kullanıcı tarafından indirilmiş uygulamalardan uzak durun. Bir bilgisayar programını veya mobil uygulamayı kullanmıyor musunuz? Zaman kaybetmeden silin.

Siber suçlular sıklıkla insanları kötü niyetli uygulamaları kurmak üzere kandırırlar. Örneğin size gerçek gibi görünen ve içerisinde geçerli bir eklenti ya da bağlantı içeren bir e-posta gönderirler. E-posta bankanızdan yada yakın bir arkadaşınızdan geliyor gibi görünebilir. Ancak, eğer eklenen dosyayı açar ya da bağlantının üzerine tıklarsanız kötü niyetli yazılımı aktif hale getirerek sisteminize kurulmasına neden olursunuz. Eğer mesaj acil bir aksiyon alma ihtiyacı uyandırıyor ya da gerçek olamayacak kadar iyi görünüyorsa, bu bir saldırı olabilir. Şüpheci olun, unutmayın mantığınız sizin en iyi savunma mekanizmanızdır.

Düzenli aralıklarla sisteminizi ve dosyalarınızı bulut tabanlı servisler üzerinden yedekleyin ya da yedeklerinizi herhangi bir sisteme bağlı olmayan harici cihazlara alın. Bu işlem yedeklerinizi, kötü niyetli yazılımların şifreleme veya silme denemelerinden korur. Yedekleriniz kritik derecede önemlidir, zira bir kötü niyetli yazılım bulaştığında, genellikle geri dönebilmenizin tek yoludur.

Sonuç olarak, kötü niyetli yazılımlara karşı korunmanın en iyi yöntemi yazılım ve cihazlarınızı her zaman güncel tutmak, güvenilir bir antivirüs yazılımı kullanmak ve sizi kandırarak kötü niyetli yazılımlar bulaştırmak isteyebilecek herkese karşı uyanık olmaktır. Bütün önlemler işe yaramadığında, düzenli alınan yedekler, genellikle geri dönebilmenizin tek yoludur.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, 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 yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Yazar

Lenny Zeltser, *Minerva Labs firmasında geliştirdiği uç nokta güvenlik ürünleri ile kötü niyetli uygulamalara karşı mücadele etmekte ve SANS Enstitüsünde kötü niyetli uygulamalar üzerine eğitimler vermektedir. Lenny, @lennyzeltser hesabını Twitter üzerinde aktif olarak kullanmakta ve zeltser.com isimli güvenlik güncesinde yazılar yayınlamaktadır.*

Kaynaklar

Fidye Yazılımları (Ransomware):	https://www.sans.org/u/EdI
Yedeklemeler:	https://www.sans.org/u/EdN
Oltalama Saldırılarını Durdurmak:	https://www.sans.org/u/EdS