Sadece Antivirüs Değil, Farkındalık da Lazım

İnternet üzerindeki tehditlerin dev bir yeraltı ekonomisini beslediği günümüzde, bilginizi ve paranızı cebinizde tutabilmek için sadece güvenlik yazılımlarına bel bağlamak yetmiyor.

Şu bir gerçek ki, ilk bilgisayar virüslerinin ortaya çıkmaya başladığı günlerden beri bilgi işlem güvenliği kavramı etrafında çok şey değişti. Uzunca bir süredir güvenlik konferanslarında, güvenlik raporlarında hep şuna benzer ifadeler yer alıyor: "Bilgisayar korsanları bir zamanlar isimlerini duyurmak, şan ve şöhret kazanmak için bu işi yaparlardı. Günümüzde ise tehditler şan şöhret için değil, büyük şirketlerin endüstriyel sırlarını çalmak veya kullanıcıların banka hesaplarını boşaltmak için kullanılıyor. Diğer bir deyişle, para nerede ise tehditler de o tarafa kayıyor."

Bu iş, kendi finansal döngüsü, hiyerarşisi, organizasyon yapıları olan dev bir endüstri halini almış durumda. Saldırılar artık sistemlerinizi çökertmeyi değil, kredi kartlarınızın ve banka hesaplarınızın detaylarını ele geçirmek için kullanılıyor. İş yerindeki bilgisayarınız masanızın üzerindeki metin dosyasının içeriğini bozmak için değil, ana sunucuya erişim sağlayarak değerli şirket sırlarına ulaşmak veya sizi binlerce bilgisayardan oluşan dev bir saldırı ağının parçası yapmak için kurcalanıyor. Bunu da çoğu zaman kullanıcıya hissettirmeden yapıyorlar. 2009'da iflas eden Nortel'in üst düzey yöneticilerinin e-posta hesaplarının şifrelerinin 2000 yılı başlarında ele geçirilmesi ve şirketin bunun yıllarca farkına varamaması, bu konuda yaşanmış en çarpıcı örneklerden biri olsa gerek.

İnternet üzerinde bu bilgilerin topluca satıldığı pazar yerleri var, hatta bu amaçla kullanılmak üzere özel olarak geliştirilmiş araçlar satarak bunlara servis desteği verenler dahi var. Güvenlik şirketi RSA'nın konferanslarında dile getirdiği üzere bu işin ortaya koyduğu ekonomik büyüklük, uyuşturucu ticaretinin ekonomik büyüklüğüyle yarışacak seviyelerde.

>>>

Korunmak İçin Dikkat Gerek

İnternet üzerindeki bu sinsi tehditlerden korunmak içinse sadece güncel antivirüsleri sisteminizde bulundurmak yetmiyor. Bunun yanı sıra özellikle sizden doğrudan bilgi sızdırmaya yönelik girişimlere ve yaygın dolandırıcılık tekniklerine karşı uyanık olmak gerekiyor.

Bunun için internet üzerinde yaygın olarak karşılaşabileceğiniz kişisel tehditlere ve bunlara karşı alınabilecek önlemlere dair bir liste hazırladık. İşte 10 maddeden oluşan o liste.

Virüsler ve Zararlı Yazılımlar

Genellikle sistem açıklarını kullanarak veya indirdiğiniz yazılımlar üzerinden sisteme bulaşırlar. Güncellemeleri düzenli olarak yapılmayan işletim sistemleri ve yazılımlar, arkasında büyük vaatler olan ücretsiz programlar, ücretli yazılımları bedava kullanma vaadiyle sunulan anahtar kod üreticileri gibi yollarla sisteminize girerler. Sisteminize girdikleri andan itibaren çevrimiçi hesaplarınıza dair şifreleri çalmaktan sisteminizin kontrolünü bütünüyle ele geçirmeye kadar birçok şey mümkün hale gelir. Korunmak için yapabileceğiniz en iyi şey bilgisayarınızda bir güvenlik ürünü kullanmak ve yazılımlarınızı güncel tutmaktır.

Oltalama Saldırıları

Banka hesabınızın veya e-posta kutunuzun şifresi gibi önemli bilgileri ele geçirmek üzere kurgulanmış bir saldırı çeşididir. Güvenli bir kaynaktan geliyormuş gibi süslenmiş bir mesaj, hesap bilgilerinizin detaylarını güncellemeniz gerektiğini ifade eder ve "Eğer bunu yapmazsanız hesabınız kullanılamaz hale gelecektir" gibi ifadelerle sizi bir an önce işlem yapmaya zorlar. İlgili bağlantıya tıkladığınızda gerçeğine uygun şekilde tasarlanmış bir web sitesi üzerindeki forma, şifreniz de dâhil olmak üzere tüm bilgilerinizi girmeniz istenir. Girerseniz hesabınızın arkasından el sallayabilirsiniz.

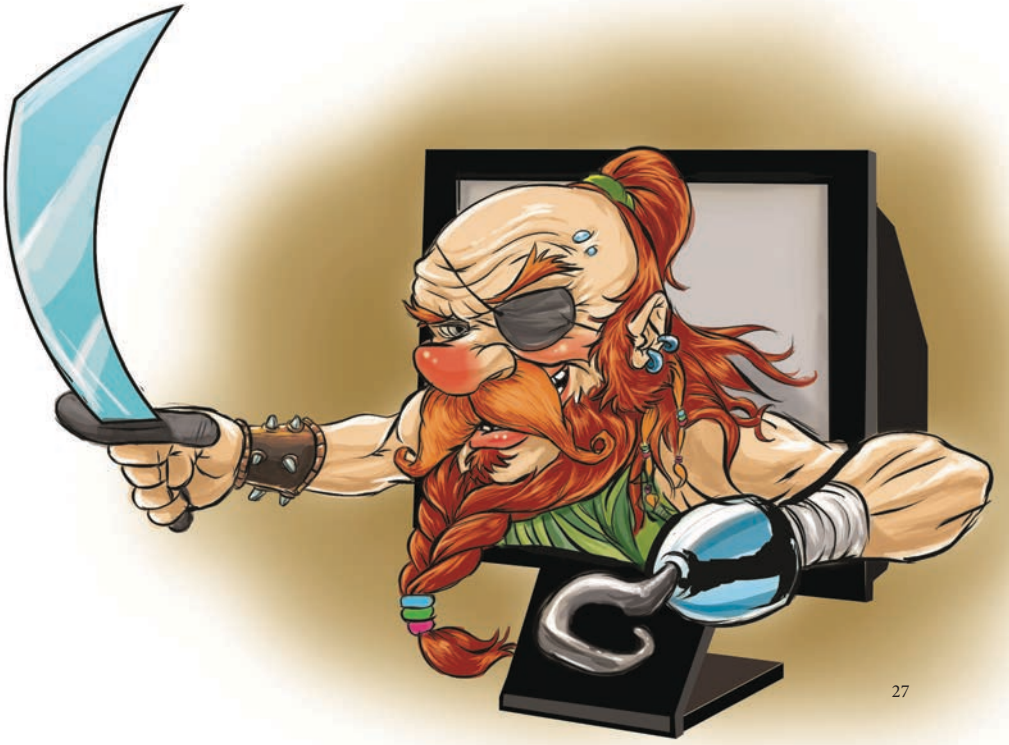
Bununla birlikte, biraz dikkat yardımıyla bu gibi saldırılardan korunmanız mümkün. Örneğin size gelen mesajdaki yazım yanlışları ve özensiz dil bunun en büyük belirtisidir. Gittiğiniz sitedeki formun sizden şifrenizi ayan beyan yazmanızı talep etmesi de şüphelenmenizi gerektirir. Sizi bir an önce işlem yapmaya zorlayan ifadeler de yine oltalamanın en büyük belirtilerindendir.

Büyük Kazanç Vaatleri

1920'lerde "Spanish Prison" (İspanyol Mahkûm) adıyla mektuplar üzerinden yapılan, 80'lerde faks makinelerine sıçrayan, günümüzde e-posta yoluyla devam eden hayli eski bir dolandırıcılık taktiğidir. Birileri kimi zaman Nijerya'dan, kimi zaman Demokratik Kongo Cumhuriyeti'nden yüklü miktarda parayı ülke dışına çıkarmak istemektedir ve tesadüfen de sizin adresinizi bulmuştur. Miktarı birkaç milyon dolarla birkaç yüz milyon dolar arasında değişen bu parayı sizin hesabınız üzerinden ülke dışına çıkarma karşılığında da neredeyse paranın yarısına denk gelen bir komisyon teklif edilmektedir. Kabul edecek olursanız gayet normal bir şekilde süreç başlar. Ancak hep son anda bir aksilik çıkar. Banka komisyon ister, banka memuru rüşvet ister, yol parasıdır, vergidir derken sizden öbek öbek para talep etmeye başlarlar. Bu arada da son derece profesyonelce hazırlanmış gazete kupürleri ve imzalı resmi evraklarla sanki işler yürüyormuş gibi sizi ümitlendirmeyi ihmal etmezler. Bir türlü mutlu sona ulaşamayıp dolandırıldığınızı anladığınızda sizden aldıkları paralarla birlikte sırra kadem basarlar. Piyangodan büyük para kazandığınızı iddia eden veya yurtdışından evlilik vaadinde bulunan çeşitlemeleri de vardır. Çok basit bir yöntem gibi görünebilir, ama tek bir vakada milyonlarca dolar kaptırmış kişiler var. Neyse ki gönderilen mesajların neredeyse tamamı İngilizce olduğu için ülkemizde çalışması zor.

Korku Tacirleri

Korku taciri yazılımlar, genellikle kendilerini güvenlik yazılımı olarak tanıtır. Vaatleri bilgisayarınızdaki güvenlik tehditlerini algılamak ve temizlemektir. İyi, güzel. Programı kurarsınız, çalıştırırsınız ve tarama yaptığınızda bir de bakarsınız ki yüzlerce zararlı yazılım bilgisayarınızda kol geziyor. "Eyvah, ne yapacağım" derken uygulama size teklifini sunar ve yazılımın tam sürümünü satın almanız halinde listede görünen tüm zararlı yazılımları temizleyeceğini vaat eder. Parayı ödeyip yazılımı satın alırsınız, temizle komutunu verirsiniz ve sisteminiz mucizevi bir şekilde bir anda pırıl pırıl olur.



Sorun şu ki, size gösterilen liste aslında gerçek bir tehdit değildir, sadece sizi korkutmak ve yazılıma para ödemeye zorlamak için oluşturulmuştur. Parayı ödediğinizde de sadece bu göz boyama ortadan kalkar. İşin daha da kötü tarafı, siz para ödeyip güvenlik yazılımı satın aldığınızı ve tehditlerden korunduğunuzu düşünürken bu yazılımlar size aslında gerçek bir koruma da sağlamaz. Bu tuzağa düşmemek için yazılımı satın almadan önce internette bir araştırma yapın. Ücretsiz bir güvenlik ürünü kullanmak istiyorsanız da tanınmış markaların ücretsiz alternatiflerine yönelin.

Fidye Yazılımları

Şu aralar yeni karşılaşılan tehditler arasında en can sıkıcı olanlardan biri. Zararlı yazılım sisteme girip çalıştırıldığında sizin için önemli olabilecek bilgi ve belgeleri, fotoğrafları bir güzel şifreleyerek açamayacağınız hale dönüştürür. Daha sonra sizi bu dosyalara ulaşabileceğiniz bir şifre çözücü yazılım satın almaya zorlar. Ümidinizi artırmak için genellikle yazılımın bedava sürümünde birkaç dosyanın kurtarılmasına da izin verir. Para verip satın alırsanız diğer dosyaları da kurtarabileceğinizin garantisi yok. Satın almazsanız gayet güçlü bir şekilde şifrelenmiş dosyaları kurtarmaya imkân da yok. Kullanılan şifreleme anahtarları her bir sistemde farklı olabildiği için antivirüs benzeri bir çözüm de üretilemiyor.

Casus Yazılımlar

Doğrudan dosyaları ve sistemleri etkileyen zararlı yazılımlardan farklı olarak, sistemdeki davranışlarınızı takip etmek amacıyla kullanılırlar. Genellikle tarayıcı üzerindeki ücretsiz araç çubukları, mesajlarınız için gülümseyen yüzler gibi ilgi çekici teklifler eşliğinde bizzat kullanıcının kendisi tarafından sisteme buyur edilirler. Ardından internette hangi siteleri gezdiniz, fareniz ekranınızın daha çok hangi bölgesinde duruyor gibi reklamcıların işine yarayacak davranışları bir bir merkeze bildirirler. Bu işler için sistem kaynaklarınızın bir bölümünü harcayarak bilgisayarınızın yavaşlamasına neden oldukları gibi, tarayıcı ana sayfanızı istedikleri sayfalara yönlendirmekten veya her fırsatta kendi reklamlarını göstermekten çekinmezler. Çoğu kapsamlı güvenlik paketinde bu gibi yazılımları temizleyen araçlar olduğu gibi, internette de sırf bu gibi yazılımları bulup ayıklama üzerine uzmanlaşmış çözümler var.

Tuş Vuruşu Kaydediciler

Adı üstünde, klavyedeki tuş vuruşlarınızı size hissettirmeden kaydederler ve düzenli olarak bu işin arkasındaki kişiye bilgi sızdırırlar. Arada girdiğiniz şifreler de doğal olarak karşı tarafa yollanır. İnternet bankacılığında ve başka bazı servislerde sanal klavye adı verilen uygulamanın gündeme gelmesinin en büyük sebebi bunlardır. Bazı durumlarda klavye ve bilgisayar bağlantısı arasına takılan bir donanım olarak da karşınıza çıkabilirler ki, bu durum özellikle internet kafeler için risk oluşturur.

Kimlik Hırsızlığı

Bazen internetteki saldırganlar doğrudan sizin değil, ancak bir tanıdığınızın hesabını ele geçirir ve onun adına sizden taleplerde bulunur. Bu nedenle internet gibi insanların yüzünü görmediğiniz bir ortamda, uzun süredir tanıdığınız birinden gelen beklenmedik taleplere şüpheyle yaklaşın. Arkadaşınız, tanıdığınız sizden hiç huyu olmadığı halde para, kontör veya profesyonel bir ortamda özel bir sistem için giriş yetkisi mi istiyor? Başka yollardan kendisine ulaşın, doğrulayın.

Sosyal Mühendislik

Aygıtlar veya sistemlerle uğraşmak yerine kişilerin güvenini kazanarak veya olaylar arasında bağlantı kurarak bilgi sızdırma işine sosyal mühendislik deniyor. Günümüzde sosyal medyanın ne kadar yaygın olduğunu ve insanların bu ortamlarda farkında olmadan kendilerine dair ne kadar çok bilgi paylaştığını düşününce, bu yöntemin giderek yaygınlaşmasına şaşırmamak gerek. Sosyal medyada paylaştıklarınızın ucu ise farklı noktalara gidebiliyor. Siz tatilde ayağınızı kumlara uzatarak yan gelip yattığınızı Facebook'ta paylaşırken hırsızların evinizi ziyarete gelmesi en basit örneklerden. Ama bunun ötesi de var, örneğin tüm sosyal hesaplarınızın bağlı olduğu e-posta adresinizin şifresine dair ipuçları profilinizde yer alıyor olabilir mi? Şifrenizi unuttuğunuzda sorulması için ayarladığınız gizli sorunun cevabını çoktan bir yerlere yazmış olmayasınız? Bu konuyu biraz detaylı düşünmekte, çapraz bağlantıları atlamamakta fayda var.

Bedavacılık

İnternet üzerinden kolay yoldan para kazanma veya çıkar elde etme üzerine kurgulanmış modelleri içerir. Genellikle internet reklamları üzerinden yönlendirir, size form veya anket doldurma gibi yardımlar karşılığında para, bilgisayar gibi ödüller vaat eder. Tıklarsınız, formlar akmaya başlar. Bir form doldur, bir tane daha doldur, tamam bu son, bu gerçekten son, ödül için başvuru öncesi bir de şu bağlantıya tıkla derken kendinizi ucu bucağı olmayan bir döngünün içinde bulursunuz. Bu döngü sırasında da büyük ihtimalle zararlı kodlar ve casus yazılımlarla dolu bağlantılardan geçer, birkaç tanesini de yanınıza alırsınız. Kısacası internet üzerinde zahmetsiz kazanç tuzağına düşmeyin, zararlı çıkan siz olursunuz.

Güvenlik Konusunda Daha Fazla Bilgi İçin:

www.bilgiguvenligi.gov.tr
www.bilgiguvenligi.org.tr
www.iscturkey.org
www.malwarehelp.org
housecall.trendmicro.com
virusscan.jotti.org
www.cert.org/homeusers/HomeComputerSecurity
www.osvdb.org
www.safegadget.com
http://www.symantec.com/threatreport/