AYLIK POPÜLER BİLİM DERGİSİ

BİLİM ve TEKNİK

TÜBİTAK

YENİ UFUKLARA

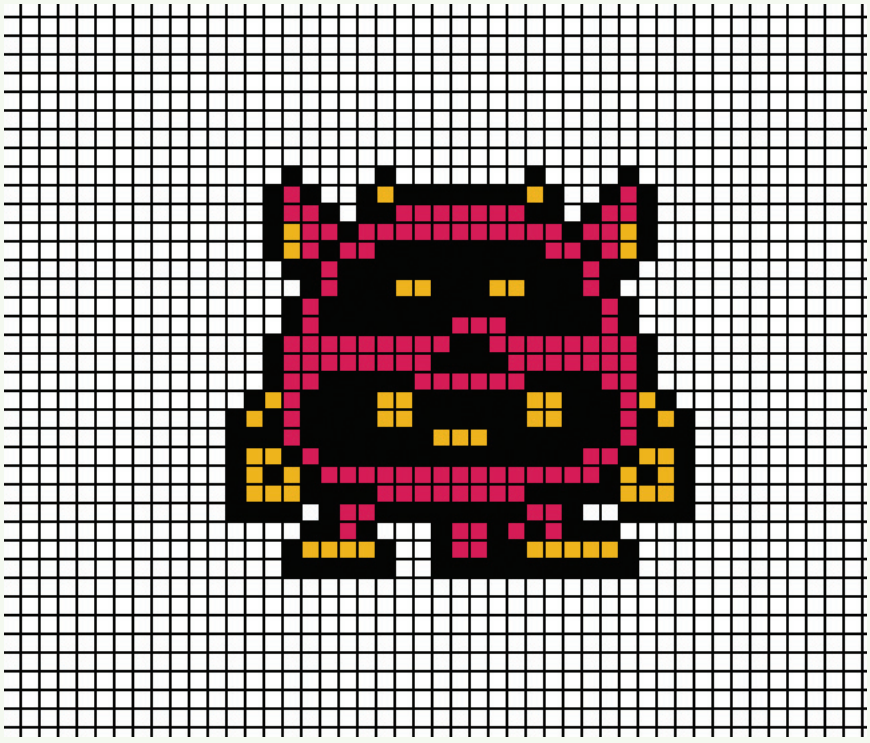
SANAL TEHDİT

BİLGİSAYAR VİRÜSLERİ

MAYIS 2005 SAYISININ ÜCRETSİZ EKİDİR

HAZIRLAYAN : LEVENT DAŞKIRAN

SANAL DÜNYANIN TEHDİTLERİ



Bilgisayarlar ve bilgisayar ağlarından oluşan sanal dünyalar hayatımızı çepeçevre sarmış durumda, hatta bazılarımız için yavaş yavaş hayatın ta kendini olma yolunda ilerliyor. Evde, işte, eğitim ve eğlencede, finans çevrelerinde, iletişim ve bilgilendirme alanlarında bu cihazlarla birlikte yaşamaya ve onlardan yardım almaya öylesine alıştık ki, bir sürelik yoklukları bile günlük hayatı aksatıyor. Lakin sanal dünyanın her şeyi bir anda kolaylaştıran büyülü yapısı kusursuz olmadığı gibi, bilgisayarları başında bu dünyanın bir parçası olarak yer alan kişilerin tamamının iyi niyetli olduğu da söylenemez. Kimi zaman zevk için yazılmış birkaç satır kod, kimi zaman sisteminize sızmak için fırsat arayan küçük bir program, ya da ustaca hazırlanmış bir elektronik posta mesajının getireceği maddi ve manevi zararlar beklenmedik ölçülerde olabiliyor. Kaybolan bazen günlerce süren bir emek oluyor, bazen yılların arşivi, bazen bilgisayarınızda sakladığınız en mahrem sırlarınız, bazen de boşaltılmış bir banka hesabı.

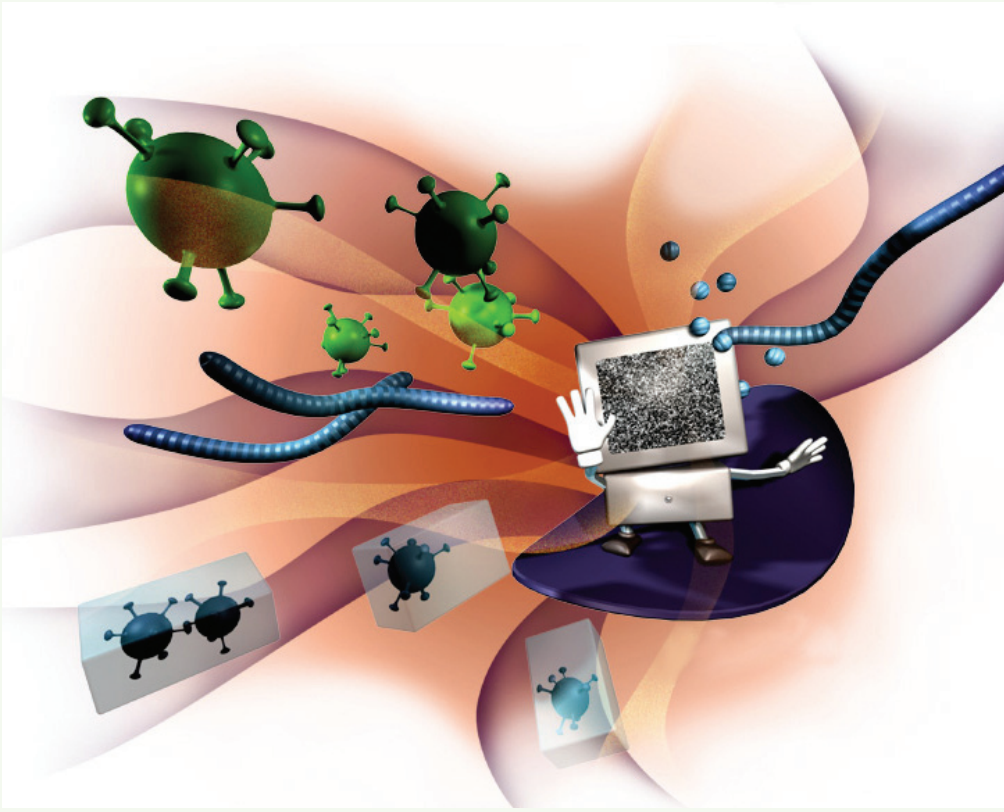
Elinizde tuttuğunuz eki bilgisayar kullanırken karşılaşabileceğiniz tüm bu tehlikelerin bilincine varmanızı sağlamak ve kendinizi bunlardan nasıl koruyabileceğiniz hakkında bilgilenmenize yardımcı olmak amacıyla hazırladık. Bilgisayar virüslerinden Truva atlarına, e-posta yoluyla gerçekleştirilen dolandırıcılık yöntemlerinden astronomik telefon faturalarının sorumlusu olan yazılımlara kadar, çalışmalarınıza ve bütçenize doğrudan zarar verebilecek akla gelen tüm tehditleri ve korunmak için neler yapabileceğinizi bir arada bu ekin içinde bulacaksınız.

BİLGİSAYAR VİRÜSLERİ: MODERN ÇAĞIN KABUSU

Bilgisayar virüsleri hakkında birçok şey söylenir ve bu söylenenlerin çoğu birçok kullanıcının beyninde fikir kırıntıları haline dönüşür. Örneğin herkes bilgisayar virüsünün kötü bir şey olduğunu bilir, sistemlere ve dosyalara zarar verdiğini bilir, çabuk yayılma eğiliminde olduğunu da bilir. Peki bunların ötesinde, bilgisayar virüsleriyle ilgili başka neleri bilmek gerekir? En önemlisi de, bilgisayar virüslerinden nasıl korunabilirsiniz?

Bu soruların yanıtlarını detaylı olarak vermeden önce düşmanı biraz daha yakından tanımakta fayda var. Bilgisayar virüsleri, temelde çalıştırılabilir küçük bir programdan ibarettirler. Ancak tıpkı hastalık yayan biyolojik virüsler gibi varlıklarını hissettirmeden hızla çoğalabilir ve bir şekilde bağlantıda oldukları diğer bilgisayara da bulaşabilirler. Virüsler hemen her türden dosyaya kendilerini ekleyebilirler, kolay fark edilmemek için çok çeşitli yöntemler kullanırlar ve nihayetinde öyle ya da böyle, bir zarara neden olurlar. Bu zarar beklemediğiniz zamanlarda ekrana çıkan saçma sapan mesajlardan tutun da, virüsün bulaştığı dosyaların tamir edilemeyecek ölçüde hasar görmesine, hatta sabit diskinizdeki tüm bilgilerinizin tümüyle kaybedilmesine kadar gidebilir.

Tüm bunlar insanı kara kara düşündüren şeyler, yine de bilgisayar virüslerine karşı savunmasız değilsiniz. Virüs tehditlerinden nasıl korunabileceğiniz konusunda biraz bilgi edinerek ve bazı prensipleri uygulamaya koyarak bu zararlı yazılımları sisteminizden ve çalışmalarınızdan uzak tutabilirsiniz.



Virüsleri konu alan bölümün devamında virüs tehditlerine dair üç farklı uyarı seviyesi belirleyerek, bu seviyelerin her birinde nasıl davranmanız gerektiğinden etraflıca bahsedeceğiz. Bunlar virüslerin henüz bulaşmadığı varsayılan temiz bir sistemde olası virüs saldırılarına karşı alınabilecek önlemleri konu alan yeşil alarm, sistemde virüs şüphesinin mevcut olduğu durumları konu alan sarı alarm ve virüslerin saldırısına uğradığı kesinleşmiş, veriler üzerinde geri döndürülmesi zor hasarların söz konusu olduğu sistemlerin kurtarılmasını konu alan kırmızı alarm.

Bilgisayar Virüslerinin Özet Tarihi

1949: Kendi kendini çoğaltabilen programlarla ilgili ilk kuram ortaya atıldı.

1970'lerin Başları: Dönemin ana bilgisayarlarında, sistem üzerinde sürekli çalışarak sistem kaynaklarını azaltıp verimin düşmesine neden olan ve The Rabbit (tavşan) olarak adlandırılan programlar ortaya çıktı. Bu programlar sistemden sisteme kendilerini kopyalama özelliğine sahip olmamalarına karşın, olasılıkla servis personelinin bilgisizliği ve işgüzarlığı sayesinde yayılabiliyorlardı. Bu dönemde bilgisayar virüsü sınıfına sokulabilecek ilk program, Univax 1108 modeli sistemleri etkileyen Pervading Animal oldu. Pervading Animal, tıpkı günümüzde modern virüslerin yaptığı gibi kendisini gizlemek için çalıştırılabilir dosyaların arkasına yerleşiyordu.

1970'lerin Ortaları: Tenex işletim sistemi üzerinde çalışan The Creeper (sarmaşık) virüsü ortaya çıktı. Bu virüs, küresel bilgisayar ağlarını ve modem bağlantılarını kullanarak farklı bilgisayar ağlarına kendini yerleştirebilme yeteneğine sahipti. Bu virüsle başa çıkabilmek için The Reeper adlı bir program hazırlandı. The Reeper, bilinen ilk antivirüs programıdır.

1980'lerin Başları: Bilgisayarların son kullanıcılar arasında hızlı yayılması, serbest dosya paylaşımı amacıyla BBS (Bulletin Board Service) adlı dosya paylaşım platformlarının ortaya çıkması sonucunu doğurdu. İlk truva atları da bu tarihlerde görüldü.

1981: Apple II işletim sistemi üzerinde yayılan ilk virüsler ortaya çıktı. Apple Virus 1,2 ve 3 olarak adlandırılan bu virüsler, el altından kanunsuz biçimde dağıtılan kopya oyunlar sayesinde yayılıyorlardı. Elk Cloner adlı Apple virüsü ise yayılmak için disketlerin açılış sektörlerini kullanıyordu.

1983: Dr. Fred Cohen, bilgisayar virüsünün resmi olarak ilk tanımını yaptı.

1986: Brain adıyla bilinen ilk IBM PC virüsü ortaya çıktı. Yazılım satma işiyle uğraşan Pakistanlı Basit ve Amjad kardeşlerin yazdığı bu virüs, 360K kapasiteli disketlerin açılış sektörlerine kendilerini yerleştiriyor ve kopyalanan her diskete bulaşıyordu. Sonradan anlattıklarına göre Basit ve Amjad, bu virüsü kopya yazılımların Pakistan sınırları içinde ne şekilde yayıldığını görebilmek amacıyla yazmışlar, fakat olayın bu kadar

VİRÜS ÇEŞİTLERİ

Bilgisayar virüsleri kendi aralarında çeşitlere ayrıldıkları gibi, bilgisayarınızdaki zarar vermeye yönelik her program da virüs olarak tanımlanmayabilir. Çeşitlerine göre virüsler ve zarar verme amacı güden diğer yazılımlar şunlardır:

Dosya Virüsleri: Parazit virüsler olarak da bilinirler. Bu virüsler, çalıştırılabilir programlar olan COM, EXE, DRV, DLL, BIN, OVL, SYS uzantılı dosyalara bulaşır ve bu dosyalar her çalıştırıldığında belleğe yerleşerek kendilerini aynı uzantılı başka dosyalara kopyalarlar.

Açılış (Boot) Virüsleri: Bu tip virüsler bulaştıkları DOS formatlı disketlerin açılış sektörüne yerleşirler ve bilgisayarınıza bir kez bulaştıktan sonra aynı bilgisayara takılan bütün yazılabilir disketlerin açılış sektörüne bulaşırlar.

Çok Parçalı Virüsler: Bu tip virüsler hem sabit disklerin ve disketlerin açılış sektörlerini, hem de bilgisayardaki mevcut dosyaları etkileyebilme yeteneğine sahiptirler.

Makro Virüsleri: Makro virüsleri, MS Word ve Excel gibi programların oluşturduğu metin dosyalarına ekli makro kodları üzerinden bulaşırlar. Makro, dokümanlarda bazı karmaşık ya da sürekli tekrarlanması gereken işleri otomatiğe bağlamak üzere kullanılan basit programlama kodlarına verilen isimdir. Makro virüsleri, standart dökümanlarla birlikte yayıldıkları için platform değişikliğinden etkilenmezler ve günümüzün en yaygın rastlanılan virüs türlerinden birini oluştururlar.

Gizli Virüsler: Bu tarz virüsler kullandıkları çeşitli yöntemler sayesinde bulaştıkları dosyada kendilerini gizleyebilme özelliğine sahiptirler.

Polimorfik Virüsler: Polimorfik virüsler her bulaşmada kodlarındaki belirleyici yapıları sürekli değiştirerek, yalnızca belli bir karakteristik kod dizisini kontrol etme yoluyla kendilerini yakalamaya çalışan antivirüs uygulamalarından kaçmayı hedeflerler. Bu nedenle tespit edilmeleri zordur.

Kılavuz Virüsler: Sıkça kullanılan bir dosyanın yerine geçerek yayılan virüslerdir. Örneğin virüs sisteme girdiğinde sıkça kullanılan Windows bileşenlerinden biri olan Notepad.exe uygulamasının ismini değiştirir ve kendi ismini Notepad.exe yapar. Daha sonra siz Notepad programını çalıştırmak istediğinizde virüs önce kendi kodunu çalıştırır, amacını yerine getirir ve hemen ardından gerçek Notepad programını çalıştırarak her şeyin yolunda olduğunu düşünmenizi sağlar.

Zırhlı Virüsler: Yapılarını kolayca ele vermemek ve işleyiş mekanizmalarını gizlemek üzere kullandıkları farklı yöntemlerle kendilerini güven altına almaya çalışan ve bu sayede kendileriyle başa çıkılmasını güçleştiren virüslerdir.

Truva Atı (Trojan): Truva atları, kullanıcıların bilgisayarlarına gizlice yerleşerek dışarıdan istem dışı müdahalelere açık hale getiren ve böylece bilgisayarınızın kontrolünü kötü niyetli kişilerin eline bırakabilen programlardır. Genel olarak çoğalma ya da yayılma eğiliminde değildirler, bu özellikleriyle virüslerden ayrılırlar.

Taşıyıcı: Sisteme virüs ya da trojan yazılımını gizlice taşıyan dosyalara verilen isimdir.

Solucan (Worm): Kendisini dosyalara eklemek yerine, bulaşmak için ağ bağlantıları üzerinden sistem açıklarını kullanan ve büyük bir hızla yayılabilen virüs çeşididir.

büyüyeceğini tahmin etmemişlerdi.

Aynı yıl, Ralph Burger adlı bir programcı yazdığı kodu çalıştırılabilir DOS programlarına ekleyebilen bir yöntem keşfetti ve bu özelliği denemek amacıyla VirDem adlı virüsü yarattı.

1987: Vienna adlı yeni bir virüs salgını sırasında Ralph Burger, virüsün bir kopyasını ele geçirerek kodunu inceledi ve elde ettiği sonuçları "Computer Viruses: A High Tech Disease" adlı kitapta topladı. Burger'in kitabı virüs programcılığı fikrinin hızla yayılmasına neden oldu. Buna paralel olarak PC virüsleri hızla çoğalırken Apple Macintosh, Commodore Amiga ve Atari ST gibi platformlar da bu akımdan paylarına düşeni aldılar.

1987'nin son ayında Christmas Tree adlı bir virüs, küresel ağ yapısını etkilemeyi başaran ilk virüs oldu. 13 Aralık tarihinde aktif hale geçen virüs, açılışta bilgisayar ekranına bir yılbaşı ağacı resmi çıkarıyor ve sonrasında ağ üzerinden hızlı bir biçimde kopyalarını göndererek sistemi çalışamaz hale getiriyordu.

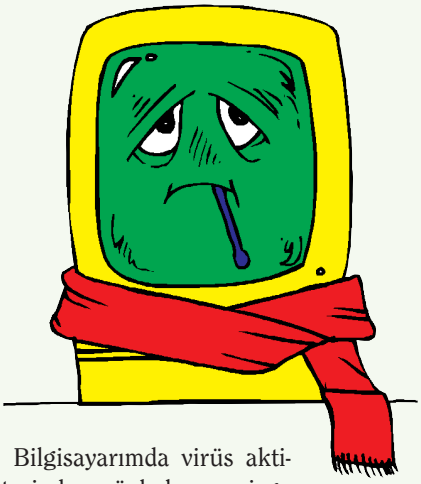
1988: 1988'e damgasını vuran en ünlü virüslerden biri, aktif hale geçmek için ayın 13'üne denk gelen cuma günlerini bekleyen ve aktif hale geçtiğinde o gün çalıştırılan tüm dosyaları silen Jerusalem oldu. O dönemlerde antivirüs programları bugünkü kadar yaygın olmadığından sistemine Jerusalem bulaşan binlerce kullanıcı, virüs aktif hale geçene kadar böyle bir tehlikeyle birlikte yaşadıklarının farkına bile varamadılar.

Oluşan bu panik, ilk yanlış alarmların ve aldatmaca (hoax) mesajlarının ortaya çıkmasına da vesile oldu. Mike RoChenle adlı birine ait olduğu düşünülen bir mesaj, BBS'ler arasında hızla yayılan bir virüsün, yayılabilmek için 2400 baud bağlantı hızına ihtiyaç duyduğu palavrasını etrafa yaydı. Bu mesajı ciddiye alan birçok BBS operatörü, bağlantı hızını hiç gerek yokken 1200 baud'a düşürme yoluna gitti.

1989: Datacrime adlı bir virüs, 13 Ekim-31 Aralık tarihleri arasında bulaştığı sistemlerdeki sabit diskleri formatlayarak çok büyük veri kayıplarına yol açtı.

Aralık 1989'da bir uyanık, AIDS adlı Truva atını içine yerleştirdiği "AIDS Information Diskette 2.0" etiketli 20.000 disketi farklı adreslere postaladı. Disketi kullananlar, 90 açılıştan sonra bilgisayarlarındaki tüm verilerin şifrelenerek gizlendiğini ve verilerini kurtarmak isteyenlerin Panama'daki bir adrese 189 dolar göndermeleri gerektiğini söyleyen bir mesajın ekranda belirdiğini görüyorlardı. Uyanık yakalandı ve cezaevine gönderildi.

1990: İlk form değiştirme özelliğine sahip



YEŞİL ALARM

Bilgisayarımda virüs aktivitesinden şüphelenmemi gerektirecek herhangi bir belirti yok, her şey normal görünüyor. Acaba sistemimin tam olarak temiz olduğundan nasıl emin olabilirim ve gelecekteki olası virüs saldırılarından korunmak için neler yapabilirim?

Aslında bilgisayarınıza güncel bir antivirüs yazılımı kurup sisteminizi ince bir virüs taramasından geçirmeden, hiç bir bilgisayar yeşil alarm kategorisine sokulamaz. Virüsler bilgisayarınıza sızmış ve sizin belki de bir köşeye atıp bir daha dönüp bakmayacağınız dosyalara bulaşmış olabilirler; bilgisayarınızdaki sistem kaynaklarının az bir kısmını kullanarak bir yavaşlamaya neden oldukları halde özellikle hızlı bir bilgisayarınız varsa bunu size hissettirmiyor olabilirler; ya da aktif hale geçmek için belli koşulların, örneğin belli bir tarihin gelmesini bekliyor olabilirler. Ancak biz yine de kullanıcısının, üzerinde herhangi bir anormal davranış gözlemediği bilgisayarları yeşil alarm kategorisinde değerlendireceğiz.

Bu kategorideki bilgisayarlar için uygulanacak stratejiler de iki kola ayrılıyor: Dışarıdan gelecek olası virüs tehditlerinin girişini engellemek ve olası bir virüs saldırısından zarar görmesi halinde telafisi mümkün olmayacak veri kayıplarının önüne geçmek.

Virüs Saldırılarına Karşı Alınabilecek Önlemler

Virüs saldırılarına karşı alınacak önlemler 8 maddede toplanıyor ve bunları uygulamak, sisteminizde etkili bir güvenlik kalkanı oluşturmak için genellikle yeterli. Unutmayın ki her bilgisayar en basit bir İnternet erişim şifresinden tutun da, yılların arşivine kadar birçok önemli bilgi ve çalışmalar içerir. Bu nedenle kullanıcı seviyeniz ve bilgisayar kullanma eğiliminiz ne olursa olsun, bu önerileri bilmenizde ve uygulamanızda fayda var.

1- Bilgisayarınızda güvenli bir kalkan oluşturmanın ilk şartı, kendini kanıtlamış bir antivirüs yazılımı kurmak ve güncel tutmaktır. Antivirüs yazılımları bilgisayarınızdaki dosyaları periyodik olarak kontrolden geçirerek virüsleri tespit etme ve temizleme özelliğine sahip olan yazılımlardır. Bu yazılımlar aynı zamanda arka planda sürekli çalışarak sisteminize giriş yapan dosyaları tek tek kontrol etme görevini de üstlenirler.

2- Özellikle dosya alışverişini sık yaptığınız bir işyeri ortamında çalışıyorsanız ya da İnternet üzerinden program indirmeye meraklıysanız, antivirüs yazılımınızın sürekli koruma mekanizmasının arka planda sürekli çalışır halde olmasını sağlamaya özen gösterin. Bu önlem, bilgisayarınıza giriş yapan dosyaları tek tek taramaya üşendiğiniz durumlarda size yardımcı olacaktır.

3- Özellikle e-posta yoluyla tanımadığınız kişilerden gelen, hatta tanıdığınız birilerinden bile geliyor olsa anlamsız konu ve içeriğe sahip mesajların ekindeki dosyaları sakın ola açmayın! Eğer e-posta yazılımınız mesaj eklerini otomatik olarak açmaya ayarlıysa, ilgili ayarı hemen bulun ve kapatın.

4- İnternet üzerinden dosya ve program indirirken güvenilir kaynakları tercih etmeye özen gösterin. Haber grupları, mesaj panoları, çalakalem tasarlanmış Web siteleri gibi kaynaklardan, gerekmiyorsa dosya almayın. Alacaksanız da dosyayı çalıştırmadan önce dosyayı mutlaka virüs taramasından geçirin.

5- Bilgisayarınızı kapatırken içinde disket bırakmayın, hatta disketten açılım işiniz için çok gerekmiyorsa BIOS ayarlarına girerek sisteminizin açılış sıralamasını A/C'den C/A'ya çevirin. Elinizde genel bir amaç için kullandığınız ve temiz olduğuna emin olduğunuz bir disket varsa bu disketin yazma koruma tırnağını açık tutun. Böylece disketinizi olası bir açılış virüsünün gazabından korumuş olursunuz.

6- Şüpheleneceğiniz bir durumla karşılaştığınızda, örneğin elinizdeki dosyanın virüslü olup olmadığına tam olarak karar veremediğiniz durumlarda tercihinizi güvensizlik yönünde kullanın. Bilmediğiniz dosyalara karşı biraz evhamlı olmak her zaman iyidir.

7- Hiç bir dosya tipine güvenmeyin. Zararsız olacağını düşündüğünüz bir DOC uzantılı metin dosyası makro virüsü taşıyor olabileceği gibi, sonunda TXT uzantısı gördüğünüz bir dosya aslında ikinci bir dosya uzantısını sizden gizlemeye çalışıyor da olabilir.

8- Önemli verilerinizin, hazır her şey yolundayken mutlaka güvenli bir yedeğini alın ve aldığınız yedeğin çalışır durumda olduğunu kontrol edin. Bu aşama virüslere karşı verileri korumanın en önemli aşamalarından biridir, ama nedense en çok da bu bölüm ihmal edilir. Hiç olmazsa bir nedenle kaybından üzüntü duyacağınız dosyaların sağlam yedeklerini almayı asla ihmal etmeyin.

Zararlı Scriptlere Dur Demek

Dosyalardan gelecek tehlikeleri bu şekilde kapattıktan sonra geriye bir delik daha kalıyor: İnternet tarayıcınız. Her ne kadar virüslerin asıl sisteme giriş yolları olarak e-posta eklentileri ve çeşitli dosyaları gösteriyor olsak da, bazı virüsler Web sayfaları üzerinden bazı kodları çalıştırarak da bulaşabiliyorlar.

Bu virüslerin en tehlikelileri genellikle Java Script yoluyla sisteme giriş yapıyorlar. Öyle ki, bunların bazıları sisteminizin "registry" kayıtlarını baştan sona değiştirebilme yeteneğine sahip. Bu nedenle varsayılan Java güvenlik seviyesini yüksek güvenlik noktasına almakta fayda var. Tarayıcı güvenliğiyle ilgili ayarları Tools-Internet Options-Security (Araçlar-İnternet Ayarları-Güvenlik) bölümünde bulabilirsiniz.

(polimorfik) virüs olan Chameleon ortaya çıktı. Bu virüs, yayılmak için kendini kopyalarken her seferinde yapısında ufak değişiklikler meydana getiriyor, böylece antivirüs programlarının kendisini fark etmesini zorlaştırıyordu. Bu virüsün ortaya koyduğu yeni yapı üzerine, antivirüs programları da kendilerini bu duruma uyarlamak zorunda kaldılar.

1991: Tequila adlı, polimorfik karaktere sahip açılış virüsü, o zamana kadar görülen en yaygın polimorfik virüs salgınına neden oldu.

1992: Michelangelo, ya da diğer adıyla March6 büyük bir salgına neden oldu. Antivirüs üreticileri, yazılımlarının önemini ön plana çıkarmak açısından bu durumu kendileri için büyük bir fırsat olarak nitelendirdiler. Ancak bu salgından etkileneceği düşünülen bilgisayar sayısının 5.000.000 civarında olduğu tahmin edilirken, bu rakam balon çıktı ve virüsten etkilenen bilgisayar sayısı yalnızca 10.000 civarında kaldı.

1993: Emmie, Metallica, Bomber, Uruguay ve Cruncher gibi, kendi kodlarını bulaştıkları dosyalarda oldukça başarılı bir biçimde gizleyebilen virüsler yayılmaya başladı. Bunlar arasında özellikle Strabge virüsü, kullandığı yöntemler sayesinde kendini gizleme konusunda bir başyapıt olarak görülüyordu.

1994: Üzerinden yıllar geçtikten sonra bile antivirüs yazılımları tarafından %100 tanımlanmasının mümkün olamayacağı SMEG.Pathogen ve SMEG.Queeq virüsleri ortaya çıktı.

Bu yıl içinde ünlü aldatmaca mesajı salgınlarından biri olan GoodTimes ortalıkta dolanmaya başladı. Bu mesaj, "Good Times" başlıklı bir e-posta mesajını alanların hemen silmesi gerektiğini, aksi halde sabit disklerindeki tüm bilgilerin bir anda silineceğini söylüyordu.

1994 yılı, virüs programcılarına karşı yasal mücadelenin de artmaya başladığı bir yıl oldu. 1994 yazında SMEG'in programcısı hapsi boylarken, İngiltere'den kendilerine ARCV (Association of Really Cruel Viruses) adını takan ve virüs programcılığıyla uğraşan bir ekibin tutuklandığı haberi geldi.

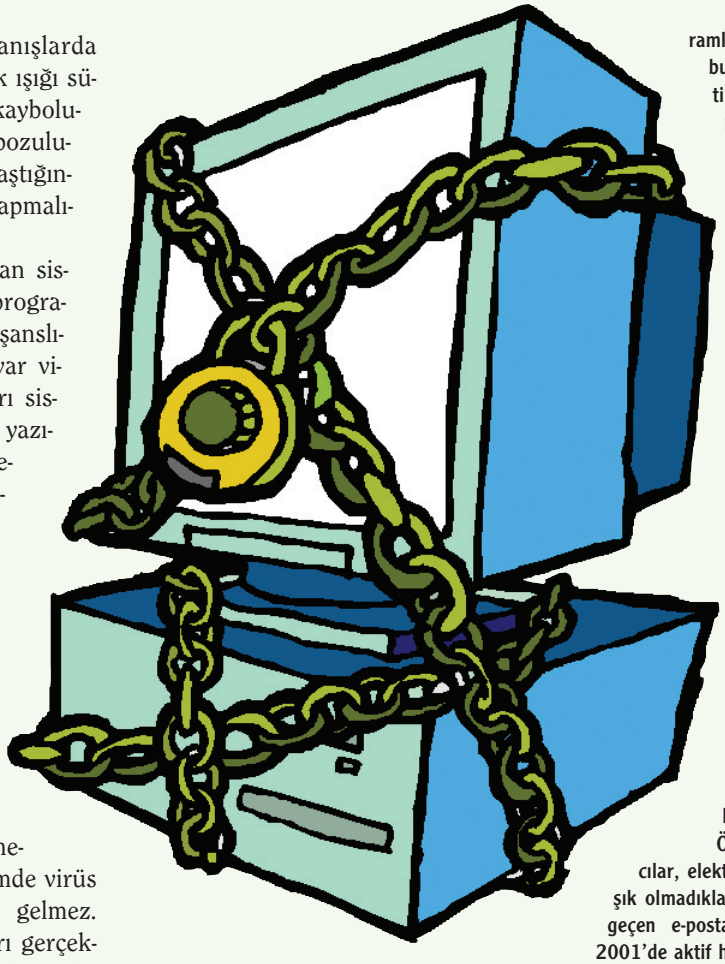
1995: Microsoft'un Windows 95 demo disketlerinin bir kısmına Form virüsünün bulaşmış olduğu ve disketlerin bu haliyle birçok kullanıcıya gönderildiği anlaşıldı.

Microsoft Word üzerinde hazırlanan dökümanlarla bulaşan Concept isimli ilk makro virüsü yine 1995 yılında ortaya çıktı. Word dökümanları o zamanlar da gerek şirketler arasında, gerek İnternet üzerinde yaygın biçimde değiş tokuş edilen bir dosya biçimiydi. Bu durum MS Word'ün

SARI ALARM

Bilgisayarım garip davranışlarda bulunmaya başladı. Sabit disk ışığı sürekli yanıyor, bazı dosyalar kayboluyor ya da durup dururken bozuluyor. Bilgisayarıma virüs bulaştığından şüpheleniyorum, ne yapmalıyım?

Sarı alarm durumunda olan sistemlerde eğer bir antivirüs programı kurup kullanabiliyorsanız şanslısınız, çünkü modern bilgisayar virüslerinin birçoğu bulaştıkları sistemde buldukları antivirüs yazılımlarını çalışamaz hale getirerek işe başlarlar. Sistemde virüs olduğundan şüphelendiğiniz halde antivirüs yazılımınızın henüz hasar görmemiş olması gibi bir durumla karşılaşmak, uyarının kırmızı alarm seviyesine taşınması halinde bu durumu mümkün olan en az hasarla atlatmanıza da yardımcı olacaktır.



Ancak sistemde virüs şüphesinin olması, tek başına sistemde virüs olduğunun kanıtı anlamına gelmez. Yukarıdaki belirtilerin bazıları gerçekten bir virüse ait olabilir de, olmayabilir de. Peki bu ayrımı nasıl yapacaksınız?

Sistemdeki Belirtiler Gerçekten Bir Virüse mi Ait?

Sisteminiz sarı alarm konumuna geçmişse, cevabını bulmanız gereken ilk soru bu olmalı. Bir kere şunu bilmelisiniz ki, sistemdeki alışılmadık davranışlar birçoğumuzun aklına hemen bilgisayar virüslerini getirse de, bu gibi durumların çoğunda sistemlerde virüs taraması yapıldığında herhangi bir sonuç alınamaz. Elbette ki virüsler zaman zaman ekrana anlamsız mesajlar çıkarırlar, bilgisayarın yavaşlamasına neden olurlar, sabit diskte alışılmadık aktivitelerin kaynağını da oluşturabilirler, ancak çoğu virüs arka planda işini yaparken ön planda hiçbir belirti göstermemeyi yeğler. Dolayısıyla virüs tehdidini çağrıştıran durumların çoğu eski program kalıntılarıyla, belleğe yerleşip kendine iş çıkaran zararsız programlarla, donanım problemleriyle ve buna benzer şeylerle ilgilidir. Bu tip işaretlerden en fazla dikkate almanız gereken, durup dururken dosyalarınızın bozulduğuna dair mesajlar almaya başladığınız andır.

Dolayısıyla karşılaştığınız durum, içinizde virüslerle karşı karşıya olduğunuza dair bir şüphe uyandırıyorsa, en başta yapılacak iş bir antivirüs programıyla tarama yaparak gerçekten de sisteme bir virüs bulaşıp bulaşmadığını kontrol etmektir.

Yalanların Arkasındaki Gerçek: Hoax (Aldatmaca)

Bazen de sisteminizde herhangi bir sorun hissetmediğiniz halde, posta kutunuzda bilgisayarınızda virüs olabileceğinden bahseden mesajlarla karşılaşıp sarı alarm durumuna geçebilirsiniz. Hatta bu mesaj güvendiğiniz bir tanıdığınızdan bile size iletilmiş olabilir.

Örneğin 2001 yılında bazı kullanıcılar, elektronik posta adreslerinde pek alışık olmadıkları bir haberle karşılaştılar. Bahsi geçen e-posta mesajının içeriği, 1 Haziran 2001'de aktif hale geçmek üzere sessizce bekleyen yeni ve çok tehlikeli bir virüsün hızla yayılma eğiliminde olduğundan ve belki de farkında olmadan sizin bilgisayarınıza da bulaşmış olabileceğinden bahsediyordu. Bu tehlikeli virüsün bilgisayarınıza bulaşıp bulaşmadığını anlamanın tek yolu ise, bilgisayarınızdaki tüm dosya ve klasörleri SULFBNK.EXE dosyası için aratmaktan geçiyordu. Dosya bulunursa tavsiye edilen şey, programı kesinlikle çalıştırmadan hemen silmek ve ardından çöp kutusunu boşaltmaktan ibaretti. Bu uyarıyı dikkate alan birçok kullanıcı, yaptıkları aramalar sonucu gerçekten de Windows\Command

metin işlemede neredeyse bir dünya standardı haline gelmiş olmasını da arkasına alarak makro virüslerini en yaygın görülen virüsler haline getirdi.

1996: İlk Windows 95 virüsü olan Win95.Boza, ilk MS Excel virüsü olan Laroux, ilk OS/2 virüsü olan OS2.AEP ve bilinen ilk yaygın Windows 3.x virüsü salgını olan Win.Tentacle boy gösterdi. Aralık 1996 yılında arka planda sürekli çalıştığı ilk belirlenen virüs olan Win95.Punch'a rastlandı.

1997: Virüsler Linux.Bliss ile Linux dünyasını da tehdit etmeye başladılar. PC virüslerinden ShareFun adlı makro virüsü ise yayılmak için MS-Mail programını kullanarak e-postayla yayılma fikrinin temellerini attı.

Bu dönemde yayılmak için farklı bir yol izleyen tek virüs ShareFun değildi. FTP protokolüyle yayılan Homer ve ünlü sohbet aracı mIRC'yi yayılmak amacıyla kullanan mIRC virüsleri de yenilikçiler kervanına katıldılar. DOS ve Windows yanında MacOS sistemlere de bulaşmayı hedefleyen ilk multiplatform virüs denemesi Esperanto ise, kodunda yer alan bol miktarda hata nedeniyle fazla yayılamadı.

1998: Haziran 1998, popülarite açısından Word ve Excel makro virüslerini bile geride bırakan Win95.CIH (Çernobil) virüsünün ilk keşfedildiği zaman oldu. Bu virüs sistemde yüklü dosya ve programlarla uğraşmak yerine, anakart üzerinde bilgisayarın açılabilmesini sağlayan verilerin yazılı olduğu Flash BIOS yongasının içeriğini değiştirerek bilgisayarı açılamaz hale getirecek biçimde tasarlanmıştı. Ayrıca ilk Java virüsü olan java.StrangeBrew ve ilk polimorfik özelliğe sahip 32 bit Windows platformu virüsleri de bu yıl görüldü.

1998 yılı, Truva atları için de oldukça verimli bir yıl oldu. Bilgisayar korsanlarının işini kolaylaştıran bir çeşit uzaktan yönetim aracı olan BackOrifice ilk kez bu yıl kullanıldı ve ardından gelecek olan NetBus, Phase gibi örneklerin yolunu açtı.

1999: 1998 Yılında keşfedilen Win95.CIH, 26 Nisan 1999 tarihinde aktif hale geçerek o zamana dek benzeri görülmemiş bir zarara neden oldu. Yalnızca Kore'deki virüsten etkilenen bilgisayar sayısının 1 milyonu aştığı tahmin ediliyor. Bugün anakartlarda sıkça görülen BIOS yongası yazma korumaları, çifte BIOS yongası gibi BIOS bilgilerini korumaya yönelik güvenlik önlemleri, bu virüsün kullanıcılara mirası olarak kaldı.

Bu yıl aynı zamanda Melissa isimli virüs için de altın bir yıl oldu. Melissa, e-posta yoluyla gönderilen dokümanların içinde yol alıyor ve doküman çalıştırıldığında içindeki bir makro kodu sa-

klasörü içinde SULFBNK.EXE dosyasının bulunduğunu görünce hemen bu dosyadan kurtulup derin bir nefes alarak ucuz atlattıklarını düşünmeye başladılar. Fakat gerçekten de ucuz mu atlatmışlardı?

Aslını sorarsanız bu kullanıcıların içine düştüğü durumun tanımı için "atlatmak" yerine "atlamak" tabiri sanırım daha uygun bir seçim olurdu. Çünkü SULFBNK.EXE, Windows dizini altında zaten doğal olarak bulunan ve uzun dosya isimlerinin düzenlenmesiyle uğraşan bir program, yani doğal bir Windows bileşeni. Bu nedenle bu sahte uyarının tuzağına düşen kullanıcılar hem kendi sistemlerinde hasar meydana getirdiler, hem de mesajı ciddiye alıp başkalarını da koruma niyetiyle, başkalarının da benzer sorunlar yaşamalarına neden oldular.

İşte, bu tarz haberleşme zincirleriyle dolaşan ve asılsız ihbar olarak nitelendirilebilecek haberlerin tamamına genel bir isim olarak hoax, yani aldatmaca adı veriliyor. Aslında aldatmaca kategorisine yalnızca sahte virüs uyarıları değil, bunun yanında yer yer bizde de çok popüler olan "sinema koltuklarında ve ankesörlü telefonların jeton iade gözünde AIDS virüsü taşıyan iğne" söylentisinden tutun da, "şu gün cep telefonunuzu açarsanız tüm cep telefonunuzu ve sim kartınızı çöpe atmanıza neden olacak bir virüs telefonlarda dolanacak" söylevlerine kadar lugatta şehir efsanesi olarak adlandırılan olayların tümü giriyor. Ancak sonuçta bu işin bilgisayar kullanıcılarının güvenliğini de ilgilendiren örnekleri mevcut olduğundan ve geçmişte SULFBNK.EXE gibi bir olay yaşandığından dolayı, aldatmacalardan nasıl korunabileceğiniz konusunda da birkaç tavsiye vermek isteriz.

Aldatmaca Mesajlarını Nasıl Anlarsınız?

Aldatmaca içeren zincir mesajlarının genellikle kendilerini ele veren tarafları mevcuttur ve işaretleri doğru algıladığınız sürece bunları normal mesajlardan ayırt etmek zor değildir.

Aldatmaca mesajları üç genel özellikleriyle kolayca anlaşılabilirler:

1- Zincir halinde dolaşan mesajlar içeriği ne olursa olsun genellikle üç karakteristik bölümden oluşurlar: Başta ilginizi çekmek için kullanılan kanca bölümü, olayı mümkün olduğunca ikna edici ya da teknik anlamda karmaşık bir dille anlatmaya çalışan gövde kısmı ve en sonunda da muhtemelen bu mesajı tanıdığınız herkese göndermenizi isteyen bölüm. Okuduğunuz mesaj bu tarz bir örgüye sahipse aldatmaca olduğundan şüphelenin. Hele "çok önemli, hemen bunu tüm tanıdıklarınıza gönderin" gibi bir ifadeyle başlayıp devamı da aşağıda bahsedilen özellikleri taşıyorsa hiç yüz vermeyin.

2- Mesajda çok fazla detaya mı inilmiş? Detayların çokluğu da bir nevi aldatmaca belirtisidir. Genellikle ortalıkta dolaşan ciddi uyarılarda, konu hakkında uyarılan kişiyi sıkmayacak ölçüde bilgi verildikten sonra daha fazla bilgi almak isteyenler için ayrıntılı bilgilerin bulunduğu Web sayfalarına yönlendirme yapılır. Size gelen e-posta baştan sona her şeyi en ince teknik detayına kadar anlatmaya ve sizi karmaşık yapısıyla ikna etmeye hevesleniyorsa şüphelenin.

Microsoft'tan geliyormuş gibi görünen ve son güvenlik yamalarını yükleme bahanesiyle sisteme virüs sokmaya çalışan tipik bir aldatmaca mesajı.

3- Mesajın kaynağı, yani ilk göndereni belli mi? Yoksa sağdan soldan size ulaşan mesajlarda ilk gönderenin kim olduğunu göremiyor musunuz? Bu durum aldatmaca mesajlarda asıl kaynağı gizli tutmak amacıyla her zaman kullanılır. Sizi uyarmak için çaba sarf eden ilk kişinin kim olduğunu göremiyorsanız ve bu kişiye ulaşabileceğiniz bir bağlantı, e-posta adresi bulamıyorsanız muhtemelen bir aldatmacayla karşı karşıyasınız demektir.

Aldatmaca Mesajı Alırsanız Ne Yapmalısınız?

Bir aldatmacayla karşılaştığınızda öncelikle içeriği ciddiye almayın, mesajı silin ve asla kimseye iletmeyin. Böylece zincir mesajlar halinde yürüyen sahte uyarıların neden olabileceği olası zararlardan hiç olmazsa kendinizi ve tanıdıklarınızı koruyabilirsiniz.

Ayrıca aldığınız bir mesajın aldatmaca olup olmadığını teyit etmek için sürekli güncellenen http://hoaxbusters.ciac.org/HBHoaxIndex.html adresini ziyaret edebilirsiniz.

yesinde adres defterindeki diğer 50 kullanıcıya kendini otomatik olarak gönderiyordu. Bu özelliği sayesinde Melissa o güne dek en hızlı yayılan virüs unvanını da eline geçirdi.

2000: LoveBug, diğer adıyla ILOVEYOU bu yılın en hatırlanan virüsleri arasında ilk sırada yer aldı. Aynen Melissa'nın yaptığı gibi bu virüs de kendini e-posta yoluyla gönderiyor ve ekli bir VBS dosyasını çalıştırarak MP3, MP2 ve JPG dosyaları da dahil olmak üzere sabit disk üzerindeki birçok dosyayı siliyordu. Hatta bununla da kalmıyor, karşılaştığı tüm servislere dair kullanıcı adı ve parola bilgilerini virüsün yapımcısına gönderiyordu.

Aynı yıl içinde kendini yalancı.txt uzantısıyla gizleyen Stages, o zamana kadar güvenli olduğu varsayılan txt uzantısının bile şüpheli dosyalar arasına girmesine yol açtı.

2001: Melissa ve LoveBug virüslerinin davranışlarını taklit eden Anna Kournikova büyük bir yayılma becerisi göstererek birçok canın yanmasına neden oldu. İşin komik tarafı, bu virüsün, basit seviye programcıların bile virüs yazabilmesine olanak veren virus creation kit adlı bir araçla yapıldığı tahmin ediliyor.

2001 yılının Temmuz ve Ağustos ayları bilgisayar ağlarına saldıran Code Red I ve II'nin şovuna sahne oldu. Code Red serisi yaklaşık 700.000 bilgisayara yayıldı ve yol açtığı ekonomik zarar 2 milyar doları aştı. Bu virüsler Windows 2000 ve NT işletim sistemlerindeki açığı kullanarak yayılıyorlardı. Microsoft bu açıkları kapatmak üzere hemen bir yama yayınlarken, bu duruma kendi sunucularının bile hazırlıksız yakalandığını itiraf etti.

Hem Linux, hem Windows işletim sistemlerine bulaşabilen bir virüs olarak ortaya çıkan Winux, programlanmasındaki hatalar nedeniyle Esperanto'yla aynı kaderi paylaşarak yaygınlaşamadı. Adobe PDF dosyalarına bulaşan ilk virüs olma özelliğine sahip PeachyPDF-A da, yayılabilmek için ücretsiz Adobe Acrobat Reader yerine Acrobat'ın tam sürümüne ihtiyaç duyduğu için pek bir varlık gösteremedi.

2002: Bu yılın başlarında Shockwave Flash (.SWF) dosyalarına bulaşabilen ilk virüs olan LFM-926 boy gösterdi. JPEG formatındaki resim dosyalarına bulaştığı için medyanın özellikle ilgi gösterdiği Perrun da bu yıla damgasını vuran virüslerdendi. Ancak Perrun JPEG dosyasından ayrılarak yayılabilmek için dosyadaki ön bilginin temizlenmesini sağlayan bir stripper programının sistemde çalışmasını şart koşuyordu. Bu nedenle hakkında yapılan haberlerin aksine, Perrun düşünüldüğü ölçüde yaygınlık kazanmadı.

KIRMIZI ALARM

Antivirüs yazılımları bilgisayarıma virüs bulaştığını söylüyor, ya da bilgisayarıma garip şeyler oluyor ve antivirüs yazılımlarım çalışmıyor. Veri kaybetme riskiyle karşı karşıyayım. Ne yapmalıyım? Bir virüs enfeksiyonuyla karşı karşıya kaldığınıza eminseniz ve bu durumdan zarar görmeye başladıysanız öncelikle sakin olun. Çoğu kullanıcı, böyle bir durumda panik yaratarak olmadık şeyler deneyip, onu açıp bunu kapatıp belki de virüsün bile veremeyeceği ölçüde veri hasarına neden olurlar. birçok kişinin sandığı üzere böyle durumlarda sabit diski formatlamak virüsten tümüyle kurtulmanızı sağlamaz, çünkü geç farkedilen virüs olasılıkla elinizdeki yedeklere de bulaşmanın bir yolunu bulmuştur.

Tamam, panik yapmıyorsunuz. Peki şimdi ne olacak? Bir kere bu işlerden pek anlamadığınızı düşünüyorsanız ortalığı kendi başınıza daha fazla kurcalamadan, bu durumla mücadele etmeyi bilen birilerini bulmaya çalışın. Örneğin sorun ofiste gerçekleştiyse, olasılıkla çalıştığınız yerin bilgi işlem servisinde bu tarz vakalarla başetmek üzere görevlendirilmiş birileri vardır.

Bu sırada şu kurallara uymaya gayret edin:

1- Virüs bulaşmış makineyle, temizleme işlemi bitene kadar çalışmayın, başkalarının çalışmasına da izin vermeyin. Virüslü bir makinede yapılacak çalışmanın tek amacının virüsün temizlenmesi yönünde olmasına özen gösterin.

2- Bilen birileri yardıma geliyorsa, ilgili gelene kadar bilgisayarı kapatın ve kapalı halde bekletin. Tabii kapatırken de öyle güç düğmesine basarak güm diye kapatmayın, tüm programları ve işletim sistemini kapatırken normal prosedürleri izleyin.

3- Çalıştığınız yerde birden fazla bilgisayar varsa ve birinde virüs tespit edilirse, diğerlerinin de virüslü olma olasılığının yüksek olduğunu düşünerek onları da kontrole tabi tutun.

4- Ortamınızda hâlâ virüs bulaşmamış makineler varsa, sağlamlığından kesinlikle emin olduğunuz disketler dışında bu makinelerde disket kullanmayın.

Daha sonra bütün bilgisayarları ve kullandığınız disketleri tek tek virüs kontrolünden geçirin.

Tamir edilebilecek durumda olanları edin, tamir edilemeyen dosyaları silin. Son olarak önemli yedeklerinizi de güncel bir antivirüs yazılımı kullanarak virüs kontrolünden geçirmeyi unutmayın.

Peki ya sisteminize giren virüs bir şekilde antivirüs yazılımınızı da bozduysa ve antivirüs sitelerine bile girmenize izin vermiyorsa? Böyle durumlarda spesifik antivirüs araçlarına yönelmekte fayda var.

Spesifik Antivirüs Araçları: Karmaşık Problemlere Basit Çözümler

Virüsler günümüzde İnternet ağ yapısının ulaştığı yaygınlık sayesinde o kadar hızlı yayılıyorlar ki, bazı durumlarda antivirüs yazılımı kullanıcıları bile henüz kullandıkları antivirüs güncelleme dosyalarında virüs tanımlaması yapılmadan ya da otomatik güncelleme periyodu gelmeden kendilerini problemin ortasında buluveriyorlar. İşin kötü tarafı, güncel virüslerin çoğunun yaptıkları şey, bulaştıkları sistemde kurulu ve çalışır durumdaki antivirüs programlarını iş göremez hale getirmek. Yani virüsün içeride olduğunu bilmenize karşın ona karşı neredeyse hiçbir şey yapamıyorsunuz.

Bu yolla gerçekleşen hızlı saldırılara, doğal olarak benzer bir hızlı savunma mantığıyla yanıt vermek gerekiyor. Bir şekilde sisteminiz virüs enfeksiyonuna yakalanmış ve antivirüs araçlarınız da kullanılamaz hale gelmişse bunları yeniden yüklemenin hiçbir anlamı yok; çünkü virüs bilgisayarınızda durduğu sürece buna izin vermeyecektir. İşte bu gibi durumlarda kullanıcıların uğrayacakları zararı mümkün olan en alt seviyede tutmaları için hemen her büyük antivirüs üreticisi, hızlı yayılan ve kullanıcılarını hazırlıksız yakalayan bu tehlikelere karşı küçük temizleme araçları hazırlıyorlar. Bu araçlar komple bir antivirüs çözümünde olduğu gibi 60.000'in üzerinde virüse karşı etkili olmak yerine, tek bir virüs çeşidine karşı etki gösteriyorlar. Dolayısıyla sisteminizde sorun çıkaran virüsü tanımlayabiliyorsanız, o virüse karşı yazılmış özel bir temizleme aracı sayesinde kurtulma şansı yaratabiliyorsunuz. Bu araçların Symantec tarafından hazırlananlarının güncel bir listesini http://securityresponse.symantec.com/avcenter/tools.list.html adresinden takip edebilirsiniz. Ayrıca hemen her antivirüs üreticisi, bu tür araçları kullanıcılara sağlayabiliyor.

Bir de, zor da olsa virüsler için elle temizleme yöntemleri mevcut. Bu konuda daha ayrıntılı bilgi almak için İnternet üzerinde

Symantec (http://www.symantec.com),
Kaspersky (http://www.kaspersky.com/),
Panda (http://www.pandasoftware.com),
Sophos (http://www.sophos.com) gibi antivirüs üreticilerinin virüs veritabanlarına göz gezdirebilirsiniz.

Aynı yıl içinde çıkan ve FreeBDS/Apache sunucularına saldıran Scalper solucanı, bulaştığı sistemlerde beklemede kalan zombi kopyalar oluşturarak, istendiği anda bir sunucu ya da servisi çökertmek üzere zombi sistemlerin tümünden aynı anda saldırı başlatabilme özelliğiyle dikkat çekiyordu.

Bu yılın diğer dikkat çeken virüs ve solucanları arasında .NET servislerine saldıran Donut, yine .NET servislerine saldıran ve bir bayan tarafından yazılmış olma özelliğine sahip Sharp-A, SQL servislerine ve kurulumlarına saldıran SQLSpider ve yayılmak için KaZaa dosya paylaşım sistemini kullanan Benjamin yer alıyordu.

2003: 2003 yılının ilk aylarında çıkan Sobig, kendi mesajlarını atabilmek için kendi SMTP programını beraberinde taşıyarak e-posta yoluyla yayılma davranışının o güne kadar görülen en abartılı örneğine imza attı. Bir başka solucan olan ve SQL 2000 sunucularını hedef alan Slammer ise saldırısında öylesine etkili oldu ki, bu virüsün etkisini en yoğun gösterdiği yerlerden biri olan Güney Kore bir süre için İnternet üzerinden silindi.

Asıl sürpriz 2003 yılı ortalarında geldi. Sobig.F, Blaster, Welchia ve Mimail solucanları yaklaşık aynı zamanlarda Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) arabirimindeki bir açığı kullanarak hızla yayılmaya başladılar. Bundan birkaç yıl önce olasılıkla bu yazıyı okuyan hemen herkesin (yazarı da dahil) başına gelmiş olan, bilgisayarların İnternet'e bağlandıktan kısa bir süre sonra "bu sistem bir hatayla karşılaştı ve 60 saniye içinde kendini kapatacaktır" mesajı eşliğinde önlenemez biçimde kendini kapatması olayı Blaster solucanının etkisiydi. Bu arada Blaster solucanının bulaştığı tüm sistemleri 16 Ağustos tarihinde windowsupdate.com sitesine saldırmaya yönlendirecek bir saatli bomba taşıdığı da ortaya çıktı. Microsoft bu saldırıdan kurtulabilmek için windowsupdate.com sitesinin İnternet kayıtlarını bir süreliğine silmek zorunda kaldı.

2004: Bu yıl içinde virüsler farklı yayılma yollarına dair arayışlarını sürdürürken, phishing adı verilen ve kullanıcı güvenine dayalı aldatma mekanizmalarının kullanımı hız kazandı. Bunlardan Trojan.Xombe, kendine Microsoft tarafından gönderilmiş bir e-posta mesajı süsü vererek kullanıcıları mesaj ekinde bulunan XP Service Pack 1 yamasını çalıştırmak için ikna etmeyi hedefliyordu. Bu esnada virüslerden para kazanma yolunda çabalar da gündeme geldi. Almanya'da yayınlanan bir dergi, Randex virüsünün bulaştığı ve virüs ta-

TRUVA ATI SALDIRILARI

Virüsler kadar yaygın olmayan, ancak duruma göre size bir virüsün yapabileceğinden çok daha fazla zarar verebilme potansiyeline sahip saldırı türlerinden biri de Truva atı (Trojan) saldırılarıdır. Truva atlarının virüslerden en belirgin farkı, dosya boyutlarının görece büyük olması ve büyük çoğunluğunun, kendi başına bulaşma yeteneğinin bulunmamasıdır. Truva atlarının sisteme girişi genellikle İnternet üzerinde güvenilir olmayan kaynaklardan indirdiğiniz programlar aracılığıyla ya da tanımadığınız kişilerden aldığınız dosyalar yardımıyla olur.

Truva atının esas amacı, sisteminizin kontrolünü tümüyle ele geçirerek sisteminize uzaktan bağlanan başka bir kullanıcının ellerine onu teslim etmektir. Truva atı sisteminize bir kez yerleşerek çalışmaya başladıktan sonra, sisteminizde Truva atı olduğunu anlayan kötü niyetli bir kullanıcı, tüm şifrelerinizi kolayca ele geçirebilir, bilgisayarınızda neler yaptığınızı dakika dakika izleyebilir, istediği dosyaları ya da sabit diskinizdeki tüm verileri silebilir, bilgisayarınızı yeniden başlatabilir, bazı temel fonksiyonlara erişimizi engelleyebilir ya da kimliğini belli etmeden dilediği mesajı ekranınızda görüntüleyebilir. Kısacası sisteminize bir Truva atı aldıysanız başınız büyük dertte demektir.

Kötü niyetli kullanıcılar için sisteminize yerleştirilmiş bir Truva atı olup olmadığını anlamanın birkaç yolu vardır. Bunlardan ilki, rasgele kullanıcıların IP adreslerini tarayarak Truva atlarının oluşturduğu karakteristik sistem açıklarının olup olmadığını kontrol etmektir. İkincisi, Truva atlarının girdikleri sistemden yaydıkları işareti takip etmektir, çünkü çoğu Truva atı, uzak bir sistemde çalışmaya başladığı andan itibaren sahibine bir işaret yollayarak varlığını ve konumunu belli eder. Üçüncü ve en yaygın kullanılan yol ise kişinin İnternet'e bağlı olup olmadığının kolayca anlaşılabileceği platformları Truva atı tuzağı olarak kullanmaktır. Örneğin MSN Messenger ya da ICQ gibi platformlar, hedef kullanıcının İnternet hattına bağlı olup olmadığını anlamayı bir hayli kolaylaştırırlar. Bu nedenle çevrimiçi mesajlaşma platformları, Truva atı saldırılarının en yaygın yaşandığı platformların başında gelir.

Bir Truva atının kontrol arabiriminin görüntüsü. Tuzağa düşen kurbanı parmak ucunda oynatmak için hazırlanmış kontrolleri sol tarafta görebilirsiniz.

Truva Atı Saldırılarından Nasıl Korunursunuz?

Truva atı saldırılarından korunmanın en iyi yolu bilgisayarınıza bir antivirüs yazılımı kurmak ve sisteme herhangi bir yolla giriş yapan tüm dosyaların bu programın kontrolünden geçmesini sağlamaktır. Truva atları antivirüs programları tarafından zararlı programlar olarak bilinir ve kolayca tespit edilirler.

Eğer sisteminizde Truva atını çalıştırdıysanız ve saldırıya da maruz kaldıysanız, zaman kaybetmeden sisteminizin İnternet bağlantısını kesin. Aksi halde bu işten nasıl bir zarar göreceğiniz saldırganın inisiyatifine kalmış demektir. Sistemin İnternet bağlantısını kestikten sonra mümkünse bir başka kaynaktan sisteminize antivirüs programı yükleyin ve Truva atını temizlemeden asla İnternet'e bağlanmayın. Bu gibi durumlara karşı bir yerlere güncel bir antivirüs yazılımı yedeklemeniz bu ve benzeri durumlar için oldukça faydalı olacaktır.

Ayrıca kullanımı kolay bir güvenlik duvarı (firewall) programı edinmek de bu tarz saldırılardan etkilenmenizin önüne geçebilir. Güvenlik duvarı yazılımları, sisteminizin açık portlarını kapatarak dışarıdan içeri ve içeriden dışarı yöndeki bağlantı isteklerini denetim altına almanızı sağlarlar. Böylece içeride bir Truva atı olması durumunda bunun size hissettirmeden varlığını başkalarına haber vermesini önleyebilir, ayrıca sisteminizi Truva atlarının varlığına karşı denetlemek için gerçekleştirilen port taramalarından kurtulabilirsiniz. Windows XP işletim sistemi, SP2'den itibaren zaten dahili bir güvenlik duvarı uygulamasına sahip. Ayrıca her türden işletim sistemi için ücretsiz güvenlik duvarı uygulamalarını http://www.free-firewall.org ve http://www.iopus.com/guides/free-firewall.htm adreslerinde bulabilirsiniz.

rafından topluca mesaj göndermeye hazır hale getirilmiş zombi sistemlerin IP adreslerinin listesini kolayca satın aldıklarını ve aynı şeyi spamcıların da yapabileceğini yazdı (spam, bilgi ve istekleri dışında birçok kişiye eşzamanlı olarak gönderilen ve genellikle ticari içeriğe sahip olan mesajların bütününe verilen bir isim). Aynı dönemde doğrudan sistemdeki güvenlik yazılımlarına saldıran ve kendini yayarken sabit diskin de bir kısmını silen Witty solucanı ortaya çıktı.

Bu yıl içinde çıkan Sasser solucanı, LSASS Windows açığını kullanarak FTP kanalıyla yayılma yoluna giden ilk örnek oldu. Mayıs ayında çıkan Worm W64.Rugrat.3344, yalnızca 64-bit Windows dosyalarına saldırma özelliğiyle bir 64-bit virüsü olarak dikkat çekti. Aynı yıl, Bluetooth bağlantısını kullanarak civardaki telefonlara bulaşma özelliğine sahip ilk cep telefonu virüsü olan Symb/Cabir-A da (bilinen adıyla Cabir) boy gösterdi.

Hamsi adıyla bilinen W32/Amus-A da yine bu yıl içinde ortaya çıkan virüsler arasındaydı. Olasılıkla Türkiye'de yazılmış olan virüs, e-posta mesajlarıyla yayılıyor ve Windows'un metin seslendirme altyapısını kullanarak "hamsi. I am seeing you. Haaaaaaa. You must come to turkiye. I am cleaning your computer. 5. 4. 3. 2. 1. 0. Gule. Gule." metnini sesli biçimde okuyordu. Hamsi fazla yayılamadı ve büyük çaplı bir tehdit oluşturmadı.

2004 yılının sonlarına doğru, 20/21 Kasım tarihlerinde Bofra/IFrame, İnternet reklamlarına kendini saklayan ilk virüs olarak kronolojideki yerini aldı. MyDoom varyantı olan bu virüs, yayılmak için bir bilgisayar korsanı tarafından ele geçirilen AdSolution reklam dağıtım yazılımını kullanmış ve fark edilene kadar 12 saat boyunca yayılmayı başarmıştı. Yılın son sürpriziyse Santy solucanı oldu. Santy'i özel yapan yalnızca phpBB açığına sahip forum sitelerine saldırması değil, saldırıya uygun siteleri bulabilmek için Google arama motorunu kullanabiliyor olmasıydı.

2005: 2005 yılı, Ocak ayında ortaya çıkan ve yayılmak için MSN Messenger yazılımını kullanan Bropia solucanıyla yine özgün bir çıkışa sahne oldu. Şubat ayında bu kez Microsoft'un sistemdeki casus yazılımları temizlemek için Windows kullanıcılarına ücretsiz dağıttığı Microsoft Antispyware Beta sürümünü hedef alan Troj/BankAsh ortaya çıktı. Mart ve Nisan aylarının yıldızı hem e-posta, hem MSN Messenger aracılığıyla yayılan Chod oldu. Bunun en önemli özelliği virüs tarafından gönderilen postalara sanki bir antivirüs firmasından geliyormuş gibi güvenilir bir mesaj süsü verilmiş olmasıydı.

ÜCRETSİZ

cınızın ekranının ayrıntılı virüs taraması yapabilen güçlü bir arabirime dönüştüğüne şahit oluyorsunuz. İlk yükleme hem tarayıcı arabiriminin, hem de o anki güncel virüs veritabanının kurulumunu gerektirdiğinden, biraz uzun sürüyor. Arabirimin bir kez yüklenmesini beklediğinizde kullanılan arabirim ve antivirüs veritabanı, tarayıcınızın tampon belleğine kaydediliyor. Böylece siteye her bağlanışınızda yalnızca kayıtlı bilgilerin güncellemesi yapılıyor, bu da ilk yüklemeye oranla daha kısa sürüyor.

Arabirim yüklendiğinde karşınıza sürücülerinizin bir listesi çıkıyor, siz de kontrol edilmesini istediğiniz sürücülerinizi seçerek işlemi başlatıyorsunuz. Çözüm Web tabanlı olmasına karşın görünüm ve kullanım açısından tıpkı bir antivirüs yazılımı kullanır gibi kolay ve zahmetsiz. Üstelik Trend Micro'nun ücretli antivirüs çözümü olan PC-Cillin ile paralel olarak Web uygulamasına ait virüs tanıma dosyaları da sürekli güncelleniyor.

Trend Micro'nun HouseCall antivirüs sitesi, herhangi bir program yüklemenize gerek kalmadan tarayıcınız üzerinden sisteminizi kontrol etmenize olanak sağlıyor.

HouseCall, normal antivirüs uygulamalarında olduğu gibi sisteminizi kontrol ederken bir virüsle karşılaşırsa önce dosyayı tamir etmeyi deniyor, tamir edemezse size sorarak silme yoluna gidiyor.

Herhangi bir kurulum gerektirmemesi, ücretsiz oluşu, her yerden ulaşılabilir olması ve güncelleme işini otomatik gerçekleştirmesi servisin olumlu yönleri. Bununla birlikte Web tabanlı oluşundan dolayı bazı olumsuz yönleri mevcut. Örneğin bir tehdit anında virüs taraması için bu uygulamaya güvenmeyin.

Trend Micro HouseCall Online

PC-Cillin Antivirüs'ün üreticisi Trend Micro'nun Web sitesi, antivirüs uygulamalarında pek de karşılaşılmadık ve insanı şaşırtan bir çözümü barındırıyor: HouseCall. HouseCall, Trend Micro tarafından Web üzerinden antivirüs uygulamalarına dair kendi sunabilecekleri bir örnek olabilmek açısından herkese açık bir site. Üstelik kullanmak için özel yaşamınızı sorgulayan bir kayıt işlemi gerektirmiyor.

HouseCall'ın http://housecall.antivirus.com/housecall/start_corp.asp adresindeki Web sitesine girerek ülke seçimini yaptığınızda, yükleme, için geçen zamanın ardından İnternet tarayı-

Virüs Düşmanı Siteler

http://www.viruslist.com
Kaspersky tarafından hazırlanan bu sitede virüslerle ilgili bilmek istediğiniz hemen her şeye ulaşmanız mümkün.

http://www.antivirus.net
Birçok antivirüs sayfasına bağlantılarla dolu.

http://www.sherpasoft.org.uk/acvFAQ/
Usenet'teki alt.comp.virus grubunun sıkça sorulan sorular arşivi.

http://securityresponse.symantec.com/
Symantec'ten virüslere karşı detaylı bir başvuru kaynağı.

http://www.symantec.com/avcenter/hoax.html
Symantec'in Hoax listesi.

http://hoaxbusters.ciac.org/HoaxBustersHome.html
CIAC (Computer Incident Advisory Capacity) Hoax listesi. Hoax tanıma yöntemleri ve ayrıntılı bilgiler mevcut.

http://www.ravantivirus.com/scan/
RAV Antivirus online dosya tarama sayfası. Bir tür HouseCall alternatifi.

http://www.icsa.net/
ICSA (International Computer Security Association) Web sitesi.

Hangi Virüs, Ne Zaman Saldırıyor?

Geçtiğimiz son birkaç yılın, virüslerin dünya çapında verdikleri zararlar açısından oldukça parlak geçtiğini kimse inkar edemez. Özellikle sistemlere saatli bomba gibi yerleşerek 26 Nisan 1999 yılında aktif hale geçen Çernobil (CIH) virüsünün verdiği zarar, dünya çapında birçok bilgisayarı kullanılamaz hale getirerek sistem güvenliğine verilmesi gereken önem konusunda küresel bir ders oldu.

Aslında virüsleri belli tarihlerde saldırmak üzere programlama fikri, 1988'de ortaya çıkan ve olasılıkla "13. Cuma" (Friday the 13th, aslında buna "Cuma Ayın 13'ü" demek daha doğru) filmine atıfla aktif hale gelmek için ayın cuma gününe denk gelen 13. günlerini kollayan Jerusalem adlı virüse kadar uzanıyor.

Tabii yalnızca Jerusalem ve Çernobil değil, diğer birçok virüs de harekete geçmek için yılın belli günleri, her ayın ilk çarşambası gibi saldırı için önceden belirlenmiş tarihleri kolluyorlar. Bu şekilde zamana bağlı olarak aktif hale geçen virüslerle ilgili olarak bulunduğunuz ay içindeki olası tehditleri bir arada görmek isterseniz, http://securityresponse.symantec.com/avcenter/calendar/ adresindeki özel virüs takvimine göz atabilirsiniz.

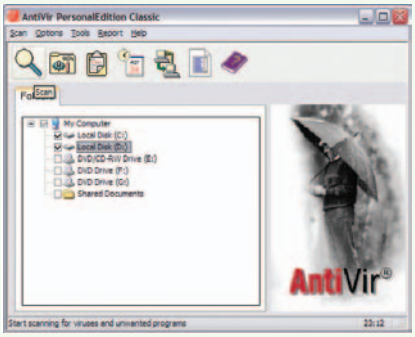
Symantec'in virüs takvimiyle, bulunduğunuz ay içindeki zaman ayarlı olası virüs tehditlerini öğrenebilirsiniz.

ANTİVİRÜS UYGULAMALARI

necekseniz, makinenizin en az İnternet'e bağlanabilecek ve bu sayfayı açabilecek ölçüde kendinde olması lazım. İkincisi, uygulama sürekli çalışır durumda kalamadığı için sizi e-posta kutunuzdan ya da indirdiğiniz dosyalardan giriş yapacak virüslere karşı koruma sağlayamıyor.

Birçok modern virüs, girdiği bilgisayarda çalışmaya başladığı anda bütün antivirüs programlarını kullanılamaz hale getiriyor ve bunlara ilişkin İnternet sitelerine de erişimi engelliyor. Yine de başınıza kötü bir şeyler geldiğinden şüpheleniyorsanız ve hazırlıksız yakalandıysanız, ilk yapmanız gereken şey, bu siteye bağlanmayı denemek olmalı.

AntiVir Personal Edition



AntiVir Personal Edition, etkili ve ücretsiz bir antivirüs yazılımı.

HouseCall gibi bir Web çözümü yerine sistemine normal bir antivirüs programı kurayım, icabında e-posta mesaj eklerinden bilgisayarıma indirdiğim dosyalara kadar giren çıkan her şeyi kontrol etsin, üstelik de ücretsiz olsun diyorsanız sizin için de çözüm mevcut: AntiVir Personal Edition. http://www.free-av.com/ adresinden indirebileceğiniz AntiVir Personal Edition, bilgisayarınıza kurup kullanabileceğiniz bir bedava antivirüs yazılımı. Yani kullanırken sizi para ödemeye zorlamıyor, belli bir süreden sonra çalışmamazlık ederim demiyor. Üstelik sisteminize virüs girişine engel olmak için sürekli çalışabilen tarayıcısından tutun da, İnternet üzerinden yeni virüslere karşı güncelleme yapabileceğiniz yardımcı araçlara kadar her fonksiyonu mevcut.

AntiVir Personal Edition, sunduğu zengin olanaklar ve sıkça güncellenmesi sayesinde ilgiyi hak eden bir ürün. Hatta ücretli bir antivirüs programı kullanıyor olsanız bile, ek bir önlem olarak bu yazılımı da indirip sisteminizde tutabilirsiniz.

AVG Free Edition

Tıpkı AntiVir Personal Edition gibi, bilgisayarınıza kurup tüm fonksiyonlarından faydalanabileceğiniz bir başka ücretsiz antivirüs aracı da AVG Free Edition. Bu yazılımı Grisoft'un http://www.grisoft.com adresindeki Web sitesinde bulunan AVG Free Edition bağlantısı altında bulabilirsiniz.

AVG Free Edition, firmanın profesyonel antivirüs çözümü olan AVG yazılımının ticari amaçlar dışında, yalnızca ev kullanıcılarına yönelik olarak sunduğu bir ürün. Ücretsiz bir ürün olmasından dolayı bazı gelişmiş özelliklere sahip değil ve ağ üzerinden çalışabilme özellikleri kısıtlanmış durumda. Bununla birlikte e-posta mesaj eklerinin kontrolünden otomatik güncellemeye kadar, ortalama bir kullanıcının gereksinim duyabileceği tüm korumayı sağlıyor.

AVG Free Edition, bilgisayarınızı virüslerden korumanız için gönüllü olarak katkıda bulunan bir diğer yazılım.

Virüsler İsimlerini Nereden Alıyorlar?

Bugün bilinen 60.000 civarı bilgisayar virüsü ve bunların da her birinin kendine özgü isimleri var. Doğal olarak bu isimlerin çoğu birbiriyle herhangi bir benzerlik göstermiyor: LoveBug, Goner, I-Worm.Klez-H, W95.CIH.V1.4, VBS.Pet_Tick.B@mm, HTML.Reality.B, O97M.Teocatl, Boza, Avalon yalnızca birkaç örnek. İnsanın da aklına haklı olarak şu iki soru geliyor: Virüsler hangi kurallara göre isimlendiriliyorlar ve isimlendirmedeki bu çeşitliliğin nedeni ne?

Antivirüs uzmanları, virüslerin isimlendirilmesi için bazı belirlenmiş kurallar dizisi olmasına karşın, her zaman bunu izlemek zorunda olmadıklarını belirtiyorlar. Bununla birlikte isimlendirmede istisnasız uygulanan tek bir kural var: Virüsler, asla sahibinin ona taktığı isimle çağrılmıyorlar. Örneğin bir virüs programcısı yaydığı virüse "kedi" ismini veriyorsa, antivirüs uzmanlarının ona vereceği isim asla "kedi" olmuyor. Ayrıca isimlendirmenin hatırlanabilir ve güncel olaylarla bir ilgisinin olmamasına da özen gösteriliyor. Başta Pentagon adıyla bilinen virüsün, yakın zamanlarda gerçekleşen Pentagon saldırısını hatırlatması nedeniyle adının Goner olarak değiştirilmesi buna bir örnek.

İsmin ne olmayacağı belli olduktan sonra, sıra ne olacağını belirlemeye geliyor. Antivirüs uzmanları, bu belirlemeyi yaparken virüsün yayılmak için kullandığı karakteristik mesajlardan alıntılar yapmaktan tutun da, virüsün kodundaki belirleyici ortak noktalara kadar birçok öğeyi isimlendirme konusunda karar vermek amacıyla kullanabiliyorlar. Ortalıkta birden fazla çeşidi dolaşan virüsler içinse kök isimlendirme sistemi kullanılıyor, I-Worm.Klez serisi gibi.

İsimlendirmede bazen de çok daha rastlantısal yollar izleniyor. Örneğin ünlü Code Red virüsü, adını kendisini keşfeden araştırmacının en sevdiği içecekten alıyor.

Karantinaya Alınan Dosyalara Ne Olur?

Antivirüs yazılımları, genellikle virüslü ya da virüslü olma olasılığı olan bir dosyayı tespit ettiklerinde, size virüslü dosyayı tamir etme ve silme seçeneklerinin yanında bir de karantina opsiyonu sunarlar. Peki karantinaya alma işleminin özelliği nedir?

Karantinaya alma işlemi, özetle bir dosyanın diğer dosyaların ve işletim sisteminin ulaşmayacağı güvenli bir alana kaydırılması işlemidir. Yani karantinaya alınan bir dosya diğer dosyalarla etkileşime giremeyeceği gibi, bilgisayarınızdaki dosya ve yazılımlar da bu alandaki dosyalarla herhangi bir iletişimde bulunamazlar. Bu sayede karantinaya alınan dosyadaki olası virüs yayılma imkanı bulamadan zararsızca bir köşede bekler. Antivirüs yazılımlarında, genellikle karantinaya alınmış dosyaların inceleme için merkeze gönderilmesi gibi bir seçenek bulunur. Bu seçenek sayesinde şüpheli ya da virüs enfeksiyonundan temizlenemeyen dosyaları antivirüs yazılımınızın ilgili araştırma birimine gönderebilirsiniz; ancak bunu yapmak istemiyorsanız karantinayı boşaltmanızda herhangi bir sakınca yok. Tamir edilemeyen bu dosyalar arasında çok önemli şeyler varsa da, artık bunlara tedbirsizliğin bedeli gözüyle bakmaktan başka yapacak pek bir şey yok.

MİLYARLIK TELEFON FATURAL

Modeminizle güle oynaya dolaştığınız yerin gerçekten kendi İnternet bağlantınız olduğuna emin misiniz? Saniyeler içinde bağlantınızı koparak sizi yurtdışı numaralara aktaran ve milyarlık telefon faturaları gelmesine neden olan küçük parazitlere dikkat! Nasıl bulaşırlar, nelere dikkat etmeli?

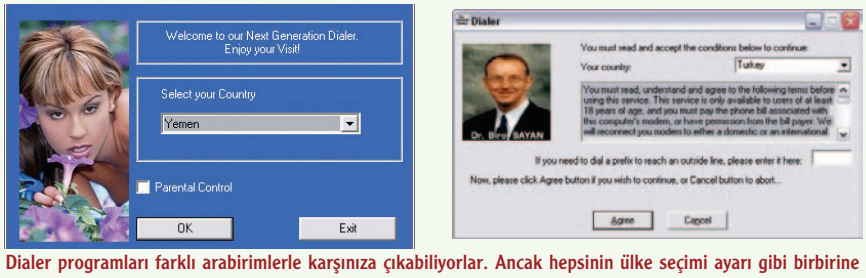
İnternet'te dolaşırken, sizin üzerinizden para kazanmayı kendine iş bilen birçok uyanığın kapınızı çaldığı olmuştur. Kimi e-posta adreslerinizi sizden habersiz olarak toplayarak bunları veri tabanı haline getirir ve satarak para kazanır, kimi bilgisayar kullanma alışkanlıklarınızı düzenli olarak bir merkeze raporlayan casus yazılımları allayıp pullayıp bilgisayarınıza sokar, kimi cep telefonu numaranız gibi kişisel bilgilerinizi reklam amaçlı kullanmak için allı pullu para kazanma sistemlerine sizi üye yapmaya çalışır, kimi de sizin izniniz olmadan e-posta adresinizi sürekli reklam bombardımanına tutar. Elbette bunların karşılığı olarak ödenen bedeller de kimi zaman hayli yüksek olabiliyor. Örneğin yıllarca kullandığınız ve herkese dağıttığınız e-posta adresinizin spam yüzünden kullanılamaz hale gelmesi, başınıza gelebilecek rahatsız edici sonuçlara güzel bir örnek.

Ancak bütün bu yöntem ve çabalar oldukça rahatsız edici olmakla birlikte, hiç olmazsa mali yönden sizi sıkıntıya sokma konusunda çok somut riskler taşımıyorlardı. Oysa bir süredir İnternet'te sizin sırtınızdan para kazanmak isteyenlerin kullandığı bir diğer yöntem var ki, maddi yönden getireceği külfet, cebi en sağlam olanlarınızı bile inim inim inletecek türden. Her şey "dialer" adlı küçük bir programı İnternet'ten indirip çalıştırmanızla başlıyor ve başınıza ne büyük bir bela aldığınızı ancak telefon faturanızı elinize aldığınızda farkediyorsunuz. Peki ama nedir bu dialer? Nerden gelirler, neye benzerler, nasıl anlaşılırlar, kendinizi bunlardan uzak tutmak için hangi tedbirleri alabilirsiniz?

Son zamanlarda çeşitli haber sitelerinde ve çeşitli yayın organlarında bahsi geçen ve kamuoyu tarafından merak edilen bu sorulara ayrıntılı olarak yanıt vermeye çalışalım.

Neden Dialer?

İnternet üzerinden ücretli servislere kayıt yaptırmak için kullanılan en yaygın ödeme aracı, bildiğiniz üzere kredi kartları. Bu ücretli servisler arasında yaygın kitleyiyse üyelerine yetişkinlere özel içerik sunan Web siteleri oluşturuyor. Ancak çoğu amatörce çalışan bu sitelerin hemen her biri kendilerine yeni üye çekebilmek için akıl almaz yöntemlere başvuruyor ve bir çoğu da ödemelerle ilgili olarak verdikleri taahhütlere uymuyorlar. Bütün bunların üzerine bir de amatör çalışan bu sitelerin kredi kartı veritabanlarının saldırılara açık olduğu, yani her an verdiğiniz kredi kartı numarasının kötü niyetli bir üçüncü kişi tarafından çalınma riski bulunduğu da göz önüne alındığında bu işe çekimser yaklaşanların sayısı bir hayli fazla. Bu ve benzer örneklerin çoğalması da birçok kişinin kredi kartını İnternet üzerinde, özellikle de yetişkinlere özel içerik sunan sitelere üye olurken kullanmak konusunda çekimser davranmasına neden oluyor.



Dialer programları farklı arabirimlerle karşınıza çıkabiliyorlar. Ancak hepsinin ülke seçimi ayarı gibi birbirine benzer yönleri var.

Dolayısıyla bu durum, kullanıcısını bir şekilde yolmaya çalışan sitelerin çoğunu ödeme konusunda alternatif arayışlarına yöneltiyor. İşte bu alternatiflerden biri, dialer adı verilen küçük programları, bir şekilde kullanıcının bilgisayarına sokarak çalıştırmasını sağlamak.

Nasıl Çalışıyorlar?

Dakikası insana oldukça pahalıya patlayan, bir zamanların popüler 900'lü hatlarını hepiniz bilirsiniz. Bu hatlar, belli firmalar tarafından işletilerek arayan kişi üzerinden gelir elde etmek üzere kullanılıyorlar. Dialer programlarının yaptığı şeyse, modeminizi ve telefon hattınızı kullanarak benzer şekilde sizi milletlerarası bir ücretli telefon servisine aktarmaktan başka bir şey değil.

Genelde senaryo şöyle gerçekleşiyor: Tuzak kurulmuş olan Web sitesine girdiğinizde, öncelikle şatafatlı görüntüler eşliğinde içeriği size öven görüntülerle karşılaşıyorsunuz. Ancak içeriğe erişmek için üzerine tıkladığınızda karşınıza gelen bir mesaj, bu içeriğe erişmek için küçük bir programı bilgisayarınıza indirmeniz gerektiğini belirtiyor. Bazen bu istek size masum bir rica yoluyla gelirken, çoğu zaman kandırma ya da zorlama yoluyla bu programı çalıştırmanızı sağlama yoluna gidiliyor.

Dialer programları, sizi sıkmadan ve bekletmeden bilgisayarınıza kolayca indirip çalıştırabilmenizi sağlamak için genellikle 30K ile 70K arasında bir büyüklüğü geçmeyecek biçimde tasarlanıyorlar. Bu da programın bilgisayarınıza indirilmesi için yaklaşık 10 saniyelik bir sürenin yeterli olması demek. Dialer programı, sistemde çalıştırıldığı zaman mevcut İnternet bağlantınızı keserek kodunda tanımlanmış olan yurtdışı ücretli bağlantı numarasıyla bağlantı kuruyor. Bu numaraları, yurtdışında yüksek ücretlendirme sistemiyle yapılandırılmış İnternet servis sağlayıcılara ait POP noktaları gibi düşünebilirsiniz. Yani gene İnternet'e bağlanıyorsunuz, ancak yurtdışı numarayı arayarak ve dakikası 10 milyon gibi bir ücretle... Bu durumun farkına varamadığınız taktirde bunun telefon faturanıza ne şekilde yansıyacağını sanırım kafanızda canlandırabiliyorsunuzdur.

Dialer programını çalıştırdığınız anda genellikle kendilerine ait birkaç kısayol simgesini belli yerlere eklemekten geri durmazlar.

Bu senaryoda olayın kaymağını yiyen taraf, bizzat yurtdışında yapılandırılmış olan dialer servisi. Ancak dialer programını bilgisayarınıza sokan Web sitesi de bu işten komisyon kazancı elde etme beklentisinde olduğundan, olayı şeker-bal kaynağı olarak gören ve sizi çeşitli tuzaklar içine çekerek bu programları çalıştırmanızı sağlamaya çalışan sitelerin içeriği yalnızca yetişkin içeriğiyle sınırlı kalmayabiliyor. Kısaca dialer yazılımlarıyla Web üzerinde her an karşılaşma riskiniz var.

Diğer yandan bu tarz sistemlerle kolay para kazanmayı hayal eden arkadaşlar da, başkalarına verdikleri maddi zarar şöyle dursun, kendileri de dolandırılıyorlar. Zira çoğu ya firmadan ödeme alamıyor, ya da firma çeşitli bahaneler öne sürüp Türkiye'ye ödeme yapmıyor.

Nasıl Anlaşılırlar?

Her ne kadar dialer programlarını ilk bakışta tanımlayabilmek bir miktar deneyim gerektirse de, bunları anlayabilmenin birkaç yolu var. Başlarken bilmeniz gereken en önemli husus, bunların çoğunun herhangi bir antivirüs programı tarafından virüs ya da trojan olarak algılanmıyor oluşu. Dolayısıyla bunlara karşı kendinizi korumak için en çok güvenmeniz gereken şey, olaya şüpheci yaklaşmak ve dikkatli bir gözlemci olmak. Bir dialerla karşılaştığınızda ancak bu ikisini bir araya getirerek bu parazitleri sisteminizden uzak tutmayı başarabilirsiniz.

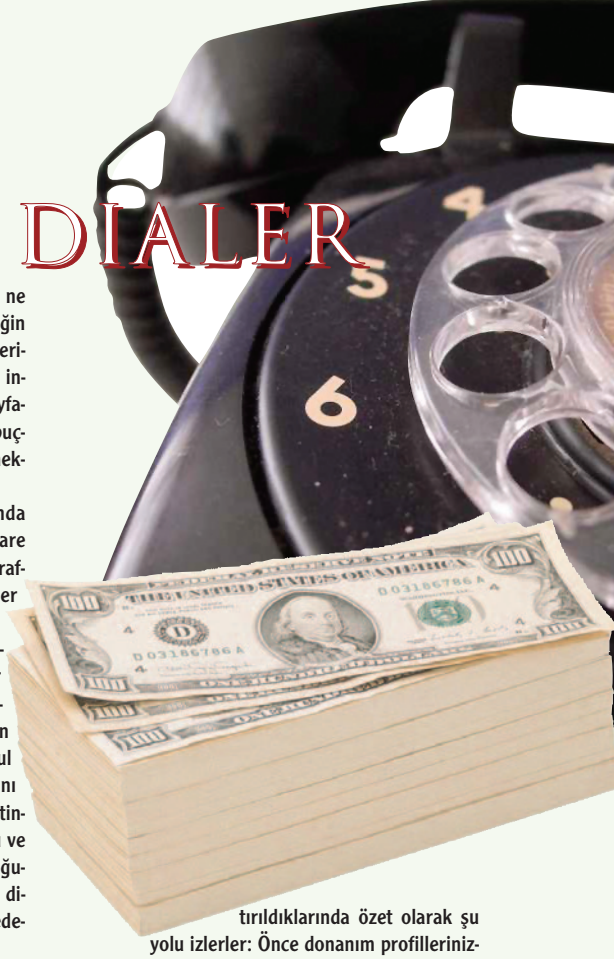
A- Şüpheci Yaklaşım: Dialer programını bilgisayarınıza indirmek için Web siteleri size çok çeşitli vaatlerle gelirler. Üstelik bu sitelerin yalnızca yetişkin içerikli sitelerden gelmesi gibi bir kural da yok. İşte size kurulan tuzaklara dair rastladığım örneklerden bir demet:

1- Girdiğiniz Web sitesi, bedava sundukları küçük bir program sayesinde İnternet üzerinde 10 kat daha hızlı dolaşabileceğinizi iddia etmektedir.

2- Web sitesi tarafından önünüze koyulan programın Napster'in Türkçe sürümü olduğu ve aradığınız her türlü MP3'ü bulabileceği iddiası vardır.

3- Yetişkin içerikli Web sitesi, içeriğinin tamamını görüntülemek için herhangi bir üyelik ya da

ARININ SORUMLUSU: DİALER



kredi kartı numarasını istemediğini belirtir. Bütün bunların yerine yalnızca ufak bir programın çalıştırılması, servislerine doğrudan erişim yapabilmeniz için yeterlidir.

4- Yine yetişkin içerikli Web sitesi, içeriğinde yüzbinlerce film, milyonlarca resim ve kamera karşısında söylediğiniz her şeyi yapmak için binlerce bekleyeniniz olduğu vaadindedir. Bütün bu servislere ulaşım için ihtiyacınız olan tek şey, ufacık bir programı bilgisayarınızda çalıştırmakta ibarettir.

5- Bolca MP3 içeren bir Web sitesine girip ana menüden istediğiniz MP3'ü bularak indirmek için tıkladığınızda, o anda sunucunun aşırı talep nedeniyle erişilemez olduğu uyarısı gelir. Ancak uyarı ekranı aynı zamanda bu tarz bir yoğunluktan etkilenmemek için küçük bir programı kullanarak servislerine doğrudan bağlantı kurabileceğinizi ve 10 kat daha hızlı MP3 indirebileceğinizi önermekten geri durmaz.

6- Ana sayfada, cinsel sorunlarınız için sizinle sorununuz hakkında konuşmak ve bilgi vermek üzere sohbet hattının öbür ucunda 7/24 bekleyen uzman doktorlar bulunduğu belirtilmektedir. İlgili konu ya da doktor ismine tıkladığınızda karşınıza çıkan bir uyarı, seçtiğiniz doktorla anında sohbet edebilmek için ufak bir programı bilgisayarınıza indirip çalıştırmanız gerektiğinden bahseder.

Yukarıdaki listede sunulanların hepsinin de dikkat ettiyseniz iki ortak özelliği var: Birincisi, neredeyse sunulan bütün vaatler abartılı ifadelerden oluşuyor. İkincisi de sunulan bütün bu ufak tefek mucizevi programların bir dialer oluşu.

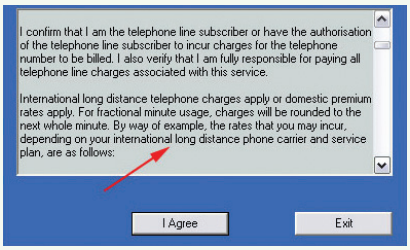
Şüpheci yaklaşımın gerekli olduğu bir diğer nokta da, sitelerin bu ufak programları indirip çalıştırmanız için inanılmaz derecede ısrarcı davranması. Bu işi yapan bütün sitelerde genelde bir ortak özellik daha bulunur: Sitedeki bağlantılar farklı yönleri ve farklı içerikleri de gösteriyor olsalar, takip ettiğinizde ya bütün bağlantıların size dialer programını indirtmeye çalışan tek bir sayfaya çıktığını, ya da biraz dolaştırıp eninde sonunda "hadi indir şunu" noktasına getirdiğini görürsünüz.

Özetlemek gerekirse, şu üç durumda olaylara şüpheyle yaklaşmak sizi zarar görmekten koruyabilir:

1. Web sitesi size olmadık vaatler sunuyorsa,

2. Web sitesi sizi ısrarla ufak bir programı indirmeye zorluyorsa,

3. Web sitesinin bütün tasarımı sizin tek bir programı indirmeniz ve çalıştırmanız üzerine odaklanmışsa.



Dialer programlarının lisans anlaşmalarında bulunan bazı ifadeler, size neyle karşı karşıya olduğunuz konusunda belirgin ipuçları verirler.

B- Dikkatli Gözlem: Dialer programları her ne kadar cebinizi boşaltmak için sınırsız bir isteğin ürünü olsalar da, yine de birtakım kuralları yerine getirmeyi ihmal etmezler. Programı es kaza indirseniz ya da program size doğrudan Web sayfasından script olarak merhaba dese bile bazı ipuçlarını değerlendirerek kendinizi tuzağa düşmekten koruyabilirsiniz.

Dialer programlarının bazılarında aslında "Dialer" yazan bir bölge bulunur, ama bu ibare programda mevcut değilse ipuçlarını başka taraflarda aramanız lazım. Bunlardan ilki, dialer programlarının bağlantıyı kurmadan önce size bir lisans anlaşması okutup kabul ettirdiği aşama. Bu lisans anlaşmaları, tıpkı şu hemen her yazılımda olduğu gibi en başta çıkan ve yüklemek üzere olduğunuz yazılımın kullanımının belli kurallara dahil olduğunu, anlaşmayı kabul etmeniz durumunda da bu kuralların tamamını okuduğunuzu ve onayladığınızı bildiren bir metinden ibaret. Tabii bu metinlerin İngilizce olması ve gerek yabancı dilin yetersizliği, gerekse bir çoğumuzun bu tarz metinleri hiç okumadan "Yes" diyerek onaylamaya kendini alıştırmış olması nedeniyle bu aşamanın geçilmesi kolay.

Ancak dikkatli bakanlar için o metinde programın sizi uluslararası bir telefon servisine bağlamak üzere olduğundan ve çalıştırdığınız zaman uluslararası telefon tarifesine dahil olacağınızdan tutun da, bağlandığınız servisin size sunacağı içeriğin kalitesinin ve doğruluğunun hiçbir şekilde garanti edilmiyor oluşuna kadar hemen her şey yazıyor. Dolayısıyla gözlem aşamasında dikkat edebileceğiniz ilk adım size gelen ufacık programın bir lisans sözleşmesini onaylatmaya çalışıyor olup olmadığı ve bu lisans anlaşması metninin içeriği. Hele de bu lisans anlaşması metninde "long distance telephone", "age 18", "international telephone charge" gibi ibareler varsa, çalıştırmak üzere olduğunuz programın bir dialer olduğundan adamakıllı şüphelenebilirsiniz.

Burada aynı zamanda dikkat edebileceğiniz bir diğer nokta da, dialer programı tarafından size ülke seçimi konusunda seçenek sunulması. Bu nedenle çektiğiniz ve çalıştırdığınız minik programın size bulunduğunuz ülkeyi sorması da şüphelenmenizi gerektirecek bir durum.

Tüm bu aşamaları atlayıp farkında olarak ya da olmayarak bu anlaşmayı da onaylarsanız, bu durumda programı çalıştırarak büyük bir mali risk altına girdiniz demektir. Bu tarz programlar çalıştırıldıklarında özet olarak şu yolu izlerler: Önce donanım profillerinizden modeminizi tespit eder, daha sonra mevcut bağlantıyı size sormadan doğrudan koparır ve modeminizle bağlı olduğu telefon hattını kullanarak programlanmış uluslararası numarayla bağlantı kurarlar. İşte bu bağlantı anında da sizden gizli birtakım işler karıştırmakta olduklarıyla ilgili anlık ipuçları verirler. Elinizdeki program çalıştırıldığında İnternet bağlantınızın bir anda kopması, modeminizden tekrar hat alma ve numara çevirme sesleri gelmesi, harici modem kullanıyorsanız bir anda üzerindeki ışıkların sönerek tekrar yanması gibi beklenmedik tepkilerle karşılaşıyorsanız, çalıştırdığınız program olasılıkla bir dialer programıdır. Bu ipuçlarını takip edebilmek için modem sesini açık tutmak ve varsa harici modeminizi gözünüzün göreceği bir yere almak faydalı olabilir.

Dialer Programları Kablo ya da ADSL Kullanıcılarını Etkiler mi?

Hayır. Dialer programlarının asıl amacı, modeminizi ve buna bağlı telefon hattınızı kullanarak tıpkı 900'lü numaraların aranması gibi yurtdışı ücretli bir servise bağlanmanızı sağlamaktan ibarettir. Kablo ve ADSL bağlantıya sahip bir bilgisayarınız varsa ve çalışan telefon hattının bağlı olduğu bir modeme sahip değilseniz, dialer programlarından etkilenmezsiniz. Ancak bu bağlantıların yanında bilgisayarınıza çalışan bir de modem ve telefon hattı mevcutsa, bu durumda dialer programlarıyla olası bir karşılaşmada siz de risk altındasınız demektir.

Korunma Yöntemleri

Başlangıçta dialer yazılımları virüs muamelesi görmediklerinden dolayı bunları tespit eden herhangi bir yazılım mevcut değildi. Oysa bugün bazı antivirüs uygulamaları, dialer temizleme özelliğine sahip olarak geliyor. Bunun yanında "Anti Dialer" ya da "Dialer Remover" gibi terimler üzerine yapılacak kısa bir araştırmayla, dialer engelleme ve temizleme üzerine uzmanlaşmış çok sayıda yazılım bulmak mümkün. http://yukle.superonline.com/detay.aspx?pid=741&kid=194 adresindeki SuperOnline Antidialer uygulaması bunlara güzel bir örnek.

Bunun yanında dialer tuzaklarından korunmak için yapabileceğiniz en iyi şeylerden biri de daima uyanık olmak. Bu amaçla da yapabileceğiniz ilk akıllıca adım, İnternet'ten indirdiğiniz her dosyayı çalıştırmamak ve her soruya "Evet" diyerek yanıt verme alışkanlığına son vermek olabilir.

Bu işe en kökten çözümse, telefonunuzu yurtdışını aramak için kullanmıyorsanız Telekom'a başvurarak numaranızı uluslararası aramalara kapatmaya yönelik bir dilekçe vermek olacaktır.

ELEKTRONİK POSTA KUTUNUZDAKİ MİLYON DOLARLIK MASALLAR

Geçmişi neredeyse yüz yıl öncesine dayanan bir dolandırıcılık sistemi, teknolojinin de yardımıyla evimizdeki ve işyerimizdeki bilgisayarlara, faks makinelerine kadar uzandı. Milyon dolarlık bu büyük vaatlerin ardında neler yatıyor?

Normal bir günde elektronik posta kutuma gelen mesajları kontrol ederken, aralarında ilginç olan bir tanesi dikkatimi çekti. Gönderilen mesajda yazanlara göre Kongo'dan Frank Langa isimli bir albay, isyancı birliklerle mücadele etmesi için kullanmak üzere hükümetin bilgisi haricinde devlet başkanı Laurant Kabila'dan 19,5 milyon dolarlık örtülü destek almış, ancak bu olaydan birkaç gün sonra Kabila bir suikaste kurban gitmişti. Langa, devlet görevlilerinin haberdar olmadığı bu parayı bir şekilde yurt dışına kaçırmak istiyor ve bunun için yurtdışında kendisine aracılık edecek güvenilir birini arıyordu. Mesajdaki talep, bu parayı sizin banka hesabınıza transfer ederek ülkeden kaçırma üzerindeydi. Söylenene göre tahmini olarak en fazla beş-altı gün sürecek bu basit transfer işlemi sonrasında bu hizmetin karşılığında bana birkaç milyon dolarlık yüklüce bir komisyon vaat ediliyordu. Mesaj, ilgilenmem dahilinde kontak kurabilmem için gerekli telefon numaraları ve e-posta adresleriyle sonlanıyordu.

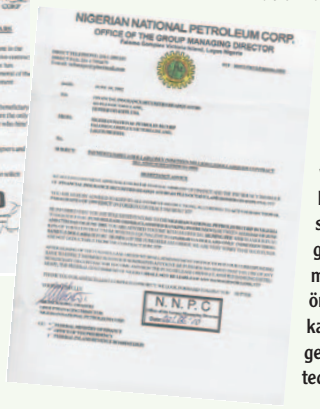

NIGERIAN NATIONAL PETROLEUM CORP.
OFFICE OF THE GROUP MANAGING DIRECTOR.
P.M.B.1090, LAGOS, NIGERIA

APPROVED FOR PAYMENT

DESPATCHED

N. N. P. C

İşte sahte bir para transferi onay belgesi. Oldukça detaylı ve gerçekçi görünüyor.


NIGERIAN NATIONAL PETROLEUM CORP.
OFFICE OF THE GROUP MANAGING DIRECTOR

N. N. P. C

19 Milyon doların transferi için tutarın yalnızca binde biri olan 19 bin "dolarcık" ödeme yapılması gerektiğini anlatan sahte belge


THE MASSES
CONSCIENCE, NURTURED BY TRUTH

Govt Release US$218M For Foreign Contractor's Payment

İşte bu da inandırıcılığı artırmak için para transferine dair örnek gazete sayfası. Elbette ki sahte.

Kuzu Postunun Altındaki Kurt

Aslında okudukça güzel bir anlaşma gibi görünüyor. Düşünsenize, yapmanız gereken şey yalnızca karşı tarafa paranın transfer edileceği bir banka hesap numarası vermekten ibaret. Karşı taraftaki kişiler oradan gerekli işlemleri halledecekler ve bir-iki hafta içinde, sizin payınıza düşecek olan birkaç milyon dolarlık komisyonla birlikte yüklüce miktarda parayı banka hesabınıza aktarılmış olarak bulacaksınız. Para gökten zembille inmediği ya da piyangodan vurmadığı sürece, herhalde ona ulaşmanın daha kolay bir yolu olmasa gerek.

Ancak kazın ayağı öyle değil. Bu olay tahmin edeceğiniz üzere bir dolandırıcılık yöntemi ve Nigerian Money Scam (elektronik ortamda ilk olarak Nijerya'dan yayıldığı için böyle deniyor), 4-1-9 ve Advance Fee Fraud gibi farklı isimlerle biliniyor. Daha çok paralı işletmeleri ağına düşürmeye yönelik bu yöntemin özünde, kolay para kazanma hayaliyle büyük vaatler peşinde koşan insanların bu zaaflarından faydalanmak yatıyor.

Dolandırıcıların oltaya takılmanız için sizden yapmanızı bekledikleri şey, bahsi geçen telefon numarasını aramanız ya da orada yazılı e-posta adresine bir mesaj göndermeniz. Verilen telefon numarasında ciddi ciddi size mesajda bahsi geçen konu hakkında yardımcı olmak üzere gerçek birileri bekliyor. Gelgelelim bunlarla bir kez iletişim kurmaya karar verdiğiniz anda, kendinizi güven duygusuyla pekiştirilmiş vaatlerden örülü bir örümcek ağının ortasında buluveriyorsunuz.

Dolandırıcılığın İşleyiş Mekanizması

Bu kişilerle iletişime geçtiğiniz zaman hemen ilk söylenen şey, bunun çok gizli bir operasyon olduğu ve bu olayın işleyiş sürecinden kimseye bahsetmemeniz gerektiği oluyor. Daha sonra karşı taraf sizden banka hesap numaralarınızı ve iletişim bilgilerinizi istiyor. Dikkat edin, banka hesap numaralarınızı istiyor, banka şifrelerinizi değil (banka hesap numaranızı oraya para yollamak isteyen birine göndermenin ne zararı olabilir ki?). Bu arada sizinle güven üzerine kurulu ilişkiyi ilerletmek üzere yapılan iletişim devam ediyor ve olayın gidişi hakkında yer yer bilgi veriliyor.

Bu aşamada, her şeyin yolunda gittiğini sanmanızı sağlamak ve içinizde varolan şüpheleri gidermek için sözde ilgili kurumların hazırladığı ve son derece gerçekçi görünümleri olan sahte belgeler e-posta adresinize ve faks numaranıza yollanıyor. Bu belgeler kimi zaman karşıdaki şirketin üst düzey yönetiminden çıkma para çıkış onayı, kimi zaman da sözde para transferi yapacak olan bankanın para transferiyle ilgili işlemleri başlattığına dair bilgiler içeren evrak oluyor. Bütün bunlar, evrak numarasından ve damgalarından tutun da, altlarındaki imzalara kadar oldukça gerçekçi görünüyorlar. Hatta bazıları, ilerleyen güven ortamını iyice pekiştirebilmek ve sizi iyice havaya sokabilmek için, aktarılacak parayla ilgili haberlerin çıktığı gerçek görünümlü sahte gazete kupürleri bile hazırlayıp gönderiyorlar. Amaç, konu üzerindeki olası şüphelerinizi son derece gerçekçi hazırlanmış birkaç belgeyle ortadan kaldırmak.

Ancak artık her şeyin yolunda gittiğini düşündüğünüz bir anda, arkanıza yaslanmış paranın hesabınıza girmesini beklerken karşı tarafta bazı şeyler ters gitmeye başlıyor. Banka görevlilerinden biri, bu kadar yüklü bir miktarın çıkışına onay vermek için birkaç bin dolar rüşvet istiyor. Derken bankadan gelen sözde bir resmi belge, bu paranın transferiyle ilgili işlemlerin başlatılabilmesi için ana paranın binde biri oranında bir işlem vergisi ödenmesi gerektiğini ve bunun ana paradan kesilmesinin mümkün olmadığından bahsediyor. Arada bu gizli işten bir başkasının haberi oluyor ve sus payı istiyor. Sonu gelmeyen bu aksiliklerin yoluna koyulması için gereken yardımlarsa daima sizden talep ediliyor. Öyle ya, birkaç gün içinde gelecek milyon dolarlara kavuşabilmek için bugün verilecek birkaç bin doların ne önemi olabilir? Üstelik elinizde transferlerin birkaç gün içinde gerçekleşeceğine dair resmi belgeler, paranın ülke dışına çıkacağıyla ilgili gazetede yayınlanmış güncel haberler var.

Ancak sonu gelmeyen bu aksiliklerden iyice sıkılıp karşı tarafı sıkıştırmaya başladığınızda, dostlarınız bir anda ortadan kayboluyor ve bir daha ne onlardan, ne de verdiğiniz paralardan asla haber alamıyorsunuz.

Yeni Bir Yöntem mi?

Hayır. Söylenenlere göre bu tür olayların ilk ortaya çıkışı ve yayılma süreci 1900'lü yılların başlarına kadar uzanıyor. O zamanların en popüler hikayesi de Spanish Prisoner, yani İspanyol mahkum adını taşıyormuş. Buradaki olay, varlıklı bir mahkumun hapishaneden çıkarılması için yardımcı olacak kişiye bu çabası karşılığında verilecek yüklüce bir ödülle ilgili. Ancak yüklü bir maliyetle girişilen kurtarma çabaları sürekli bir engele takılıyor ve gardiyanlara ödenecek son bir rüşvet, imzalanacak son bir kağıdın arasına sıkıştırılması gereken para derken, gerçekte varolmayan mahkum, hayali hapishanesinden hiç bir zaman çıkamıyor.

Peki bu durum ne kadar ciddi olabilir? Birçoğunuz olayın baştan itibaren bir düzmece olduğunu ve böyle bir şeye asla para vermeyeceğinizi düşünebilirsiniz. Ancak bu işin arkasındaki ikna düzenekleri öyle güzel tasarlanıyor ki, yalnızca ABD'de 15 aylık bir zaman içinde bu yolla dolandırıcılara kaptırıldığı rapor edilen paraların 100 milyon doları bulduğu tahmin ediliyor. Üstelik bu yöntemle dolandırıldığı halde şikayetçi olmayan birçok kişinin bulunduğu ve asıl kaybın çok daha yüksek olabileceği söyleniyor.

Sonuç

20. yüzyılın başlarında mektuplarla başlayıp, teknolojinin açtığı yoldan ilerleyerek faks makineleri ve e-posta mesajlarını da yayılma aracı olarak kullanılan bu dolandırıcılık türünün günümüzde rastlayabileceğiniz binlerce farklı çeşidi mevcut. Gönderenler değişiyor, hikayeler değişiyor, transfer edilecek rakamlar ve komisyonlar değişiyor, vaatler de değişiyor ama amaç her zaman aynı: Kolay yoldan zengin olma hayaliyle döndürülen başınızın durmasına fırsat vermeden sizden mümkün olduğunca para koparmak ve gözünüz açılmaya başladığında ortalıktan sonsuza dek kaybolmak. Tıpkı güzel başlayan, ama sonu iyi bitmeyen bir masal gibi.

Korunmak için uygulayacağınız tek yolsa bu tarz vaatlere içeriği her ne olursa olsun hiçbir şekilde yüz vermemek, iletişim kurmaya çalışamamak ve mesajı silmekten ibaret.

Konuyla İlgili Bağlantılar

http://www.geocities.com/jaccountinfo/AbbasBunduScam.html
Kendisine Abbas Bundu adını veren bir dolandırıcının evire çevire işletilmesine dair mesajlaşma kayıtları. İşleyişin nasıl yürüdüğünü öğrenmek açısından oldukça faydalı.

http://www.snopes2.com/inboxer/scams/nigeria.htm
Advance Fee Fraud hakkında detaylı bilgi ve bağlantılar.

http://www.secretservice.gov/alert419.shtml
Amerikan gizli servisinin konu hakkındaki bilgilendirme ve uyarı sayfası.

SANAL DOLANDIRICILIĞIN YÜKSELEN YILDIZI: PHISHING

Gerçek süsü verilmiş sahte mesajlar eşliğinde kurumsal güveni kötüye kullanarak başınıza musallat olan dolandırıcılar, paranızın ve kimliğinizin peşinde.

Son dönemlerde bilgisayar kullanımı konusunda fazla deneyimi olmayan kullanıcıları hedef alan, maddi ve manevi anlamda ciddi zararlara neden olan yeni bir dolandırıcılık türü hızla yayılmaya başladı. Hatta henüz geçtiğimiz ay, bu tarz bir dolandırıcılık örneğini ülkemizde gerçekleştiren ve bu yolla 3.000 kullanıcının bankacılık işlem şifrelerini, kredi kart numaralarını ve özel bilgilerini ele geçirerek kendilerine çıkar sağlayan ve bu amaçla 17 yaşındaki bilgisayar korsanı B.B.'den yardım alan organize bir suç şebekesi çökertildi. İnternet üzerinden dolandırıcılık konusunda yıldızı giderek parlayan bu yönteme phishing adı veriliyor.

Peki nedir bu phishing denen? Phishing sözcüğü, eskiden telefon sistemlerinden ücretsiz görüşme yapmak için kullanılan bir aldatmaca sistemi olan "phreaking" ve balık avlama anlamına gelen "fishing" sözcüklerinin birleşmesinden oluşuyor. Tanım olarak phishing, genellikle e-posta ya da Web sitelerindeki açılır pencereler yoluyla karşınıza çıkan ve hem kişisel, hem finansal anlamda zararla sonuçlanabilme potansiyeli yüksek bir nevi bilgi hırsızlığı yöntemi.

Sistem Nasıl Çalışıyor?

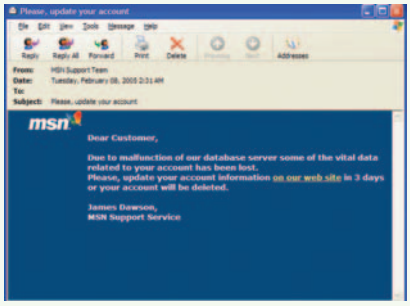
Phishing dolandırıcıları sizden kişisel bilgilerinizi ya da finansal şifrelerinizi çalmak için, hizmet aldığınız kurumların kurumsal kimliğini taklit eden mesajlarla karşınıza çıkıyorlar. Taklit edilen organizasyonlar arasında çalıştığınız banka, hizmet aldığınız servis sağlayıcı, hatta devlet kurumları bile olabiliyor.

Tüm bu mesajların ortak amacı, bir nedenle hesabınızla ilgili bilgilerin güncellenmesi gerektiği konusunda sizi ikna edebilmek. Genellikle söyleneni yapmadığınız takdirde sizi dezavantajlı konuma getirecek bir durumun varlığı da mesaja eklenerek bir an önce harekete geçmeniz teşvik ediliyor. Örneğin sürekli çalıştığınız bankadan geliyor süsü verilmiş bir mesaj size çevrimiçi bankacılık hesabınıza ait şifre bilgilerinizin değiştirilmesi gerektiğini söylerken, bunu bir hafta içinde yapmadığınız taktirde tüm hesaplarınızın güvenlik nedeniyle bloke edileceğine benzer bir blöf yaparak sizi bir an önce işlem yapmaya zorluyor. Bu yalana inanıp mesajda yer alan sahte bağlantıya tıklarsanız, bu kez her zaman kullandığınız güvenilir kurumsal sitenin başarıyla taklit edilmiş bir kopyası sizi karşılıyor. Ancak yönlendirildiğiniz sahte sitedeki ilgili boşluklara kişisel bilgilerinizi girdiğiniz anda tüm bilgileriniz karşı tarafın eline geçmiş oluyor. Bundan sonra bankacılık şifrelerinizi kullanarak banka ve kredi kartı hesaplarınızı boşaltmak, ya da bankadan edinilecek detaylı kişisel bilgiler yardımıyla işlenen bazı suçları sizin üzerinize yıkmak tümüyle hırsızın inisiyatifine kalıyor.

Tuzağa Düşmemek İçin Ne Yapmalı?

Phishing bu aralar gelişmiş teknoloji ve yaygınlaşan bilgisayar kullanımına bağlı olarak popülerlik kazanan ve her geçen gün daha fazla kişiyi tehdit eden bir dolandırıcılık yöntemi. Diğer yandan size gönderilen mesajlar ne kadar gerçekçi olursa olsun, mesajlardaki bazı özel işaretlere dikkat ettiğiniz ve bazı prensipleri uygulamaya koyduğunuz sürece bu işten zarar görmeden sıyrılabilirsiniz.

1- Kimlerle çalıştığınızı bilin. Size gelen bilgi doğrulama mesajı, çalıştığınız kurumlardan birine ait



İşte klasik phishing yaklaşımlarına basit bir örnek. Mesaj gerçekten MSN tarafından gönderilmiş gibi görünmekle birlikte, sisteme giriş yapmanız için sizi bir an önce harekete geçmeye zorlama çabası içinde ve mesaj içindeki bağlantı adresi (en alt satırda görebilirsiniz) sizi MSN'e ait olmayan tuzak siteye yönlendiriyor.

değilse silin.

2- Size gönderilen mesaj doğrudan kişisel ve finansal bilgilerinizi istemeye yönelikse, üstelik bu bilgileri sağlamanız için sizi acele etmeye yönlendirecek blöfler içeriyorsa olasılıkla bir tuzakla karşı karşıyasınız demektir. Unutmayın ki hiçbir düzgün banka ya da kurum, sizden e-posta yoluyla şifre ve kimlik bilgilerinizi göndermenizi istemez.

3- Asla sizden istenen bilgileri girmek için e-posta mesajları içinde yer alan bağlantıları kullanmayın. Mesajda yazılanların doğruluğunu teyit etmek istiyorsanız, önce yeni bir tarayıcı penceresi açın ve bankanızın/kurumunuzun Web adresi kendiniz elle yazarak girişinizi yapın. Unutmayın ki dolandırıcılar, tarayıcı açıklarını kullanarak, site içindeki bir JavaScript kodu yardımıyla siz tuzak sitede gezinirken adres satırını gerçekten kuruma ait Web sitesinde geziyormuşsunuz gibi gösterebilirler. Gezdiğiniz sitelerin bu yolla gizlenmediğinden emin olmak için http://www.corestreet.com/ adresindeki SpoofStick aracını kullanabilirsiniz.

4- Mesajların sizi yönlendirdiği adreslere dikkat edin. Bu yönlendirme adresleri çoğu zaman kurumun kendisiyle ilintisiz bir site olabileceği gibi, yönlendirme adreslerinde yalnızca gözü aldatmaya yönelik işaretler de bulunabilir (http://www.te1eweb.com gibi, l harfinin yerine 1 rakamının yerleştirildiğine dikkat edin). Bazen de dolandırıcılar mesaj içine gerçek firmaya ait Web sitesi üzerinde çalışmadığını bildikleri bir bağlantı koyarlar, altına da "eğer yukarıdaki adrese ulaşamıyorsanız aşağıdaki adresi de kullanabilirsiniz" diyerek tuzak kurulu adresi yerleştirirler. Bu oyuna gelmemenin yolu 3 numaralı maddeyi istisnasız uygulamaya koymaktan geçer.

5- Kişisel ve finansal bilgilerinizi doğrulamaya yönelik olarak e-posta yoluyla size gönderilen formları asla doldurup geri göndermeyin. Bu bilgilerin güncellenmesini, kurumunuzun çağrı merkezini telefonla arayarak gerçekleştirin.

6- Yazım ve cümle hatalarına dikkat edin. Phishing mesajları ne kadar profesyonel görünürlerse görünsünler, genellikle yazım ve cümle kurulumunda bolca hata barındırırlar. Elbette ki gerçek kurumlardan gelen mesajlar da bu tarz hataları barındırıyor olabilir, ancak hata sayısı birden fazlaysa şüphelenmeye başlayabilirsiniz.

7- Güvenli Web siteleri http:// değil, https:// ön ekiyle başlarlar ve siteye girdiğinizde işlemin güvenli olduğunu belirten bir simge, tarayıcınızın alt kısmına belirir. Bu aslında tam olarak ayırıcı bir özellik değildir, ancak çoğu sahte site henüz bu özelliğe sahip olmadığından kontrol etmenizde fayda var.

8- Bazı antivirüs yazılımları ve tarayıcı eklentileri, phishing amacıyla kullanılan Web sitelerinin listelerine ulaşma ve böyle bir siteye yönlendirildiğinizde sizi uyarma özelliğine sahiptir. Bu özellik için satın aldığınız antivirüs programının üreticisine danışabilir, ya da bu amaçla kullanabileceğiniz ücretsiz bir program olan EarthLink Toolbar yazılımını bilgisayarınıza yükleyebilirsiniz (http://www.earthlink.net/software/free/toolbar).

9- Banka hesaplarınızı ve kullandığınız diğer servisleri düzenli olarak ziyaret edip bilginiz dışınızda bir işlemin gerçekleştirilip gerçekleştirilmediğini kontrol edin. Bazı durumlarda sizden alınan bilgiler hemen o an değil, şüphe çekmemesi için aradan belli bir süre geçtikten sonra kullanılabilir. Şüpheli bir hareket gördüğünüz anda hemen bankanızı ya da servisinizi arayın.

10- Kullandığınız İnternet tarayıcısını ve e-posta yazılımını güncellemeyi unutmayın. Yeni güncellemeler, bu tarz saldırıların önlenmesi konusunda yeni özellikler içeriyor olabilir.

Konuyla İlgili Bağlantılar

http://www.olympos.org/article/articleview/1347/1/2/
Phishing konusunda oldukça ayrıntılı açıklamalara yer veren çok güzel bir Türkçe kaynak.
http://www.olympos.org/article/articleview/1403/1/2/
Türkiye'deki phishing girişimlerine ait örnekler.
http://www.hsbc.com.tr/OnlineServisler/Guvenlik/Phishing.asp
HSBC Bank'ın phishing hakkındaki Türkçe bilgilendirme sayfası.
http://www.innova.com.tr/08Arsiv/makaleler.htm
İnnova'nın Türkçe bilgilendirme sayfası.
http://www.antiphishing.org/
Phishing konusunda bilgiler ve bilinen phishing yöntemleri üzerine geniş bir veritabanı.
http://survey.mailfrontier.com/survey/quiztest.html
Size gösterilecek mesajlardaki ipuçlarını gözden geçirerek hangilerinin gerçek, hangilerinin dolandırıcılık teşebbüsü olduğunu anlayabilme konusundaki becerinizi ölçen bir test.
http://survey.mailfrontier.com/survey/phishing_uk.html
Yukarıdaki testin İngiltere sürümü.
http://www.hmaus.com/signal/topstories/documents/phishing101.html
Zor anlaşılan türden bazı phishing girişimlerinin ortaya çıkarılmasına dair yararlı bir makale.

Bilgilerinizi Verdiyseniz Ne Olacak?

Diyelim ki bir şekilde dolandırıcıların tuzağına düştünüz ve kredi kartı bilgilerinizi, banka hesabı şifrelerinizi kaptırdınız. Bu durumda yapmanız gereken ilk şey hemen çalıştığınız kurumlara güvenilir bir yoldan ulaşarak tüm şifrelerinizi ve kart numaralarınızı değiştirmek olmalı. Daha sonra bu bilgiler kullanılarak şüpheli hesap hareketleri gerçekleştirilip gerçekleştirilmediğini kontrol edin. Eğer böyle bir durum varsa hemen gerekli kanuni işlemlerin başlatılmasını sağlayın.

Çalıştığınız banka kanunlar ve kendilerine özgü sigorta sistemleri dahilinde karşı karşıya olduğunuz zararın tazmini ya da zararın yalnızca belli bir kısmından sorumlu tutulabilmeniz konusunda size seçenek sunabilirler. Eğer bu tarz bir dolandırıcılığın kurbanı olduğunuzu düşünüyorsanız, konu hakkında bankanızdan detaylı bilgi edinin ve bu bilgileri avukatınızla paylaşın.

Eğer sizden çalınan bilgilerle sizinle iletişime geçmeye çalışan birileri olursa, konuyu hemen bir avukat eşliğinde ilgili makamlara iletin ve böyle kişilerle asla kendiniz muhatap olmayın.

AYLIK POPÜLER BİLİM DER

BİLİM ve TEKNİK

TÜBİTAK

İsteyen okurlarımız 1,5 YTL. (1.500.000 TL) ve posta ücreti karşılığında 2004 yılı indeksini satın alabilirler.
TÜBİTAK Kitap Satış Bürosu:
Atatürk Bulvarı No:221
Kavaklıdere / Ankara
Sipariş için:
(312) 467 32 46

434 (OCAK) 2004 - 445 (ARALIK) 2004

2004 İndeksi

ÇIKTI