Tahammül Sınırlarımızı Zorlayan Bilgisayar Virüsleri

Günümüzde "bilgisayar virüsü" tanımlaması artık "bela" ile eş anlamlı tutuluyor. Bilgisayarınız açılmıyor mu? Belki de bilgisayarınıza virüs bulaşmıştır. Ancak şunu da unutmamak gerekir; bilgisayar ile ilgili sorunlara neden olan herzaman virüs değil, donanım, CONFIG.SYS veya AUTOEXEC.BAT dosyalarındaki değişiklikler ya da kullanıcı hatalarıdır. "Virüs"ler, "Solucanlar" (worm), "Truva Atları" (trojan horse) ve "mantık bombaları" (logic bomb), istenmeyen zararlı yazılım sınıflarıdır.

BİLGİSAYAR virüslerinin ve istenmeyen zararlı yazılımların da aralarında önemli farklar vardır. Bu farkların temelinde, bu sınıfların bir "konağa" ihtiyaç duyup duymadığı ve kopyasını çıkarıp çıkarmadığı gibi durumlar vardır. Elbette bu dört sınıf da zarar verir, ancak tanımları farklıdır. Tablo'da hepsinin tanımı verilmiştir.

Günümüzde bilinen virüslerin çoğu eski Sovyetler Birliği, Bulgaristan, Almanya ve Amerika'da yazılmıştır. Bunların yazarları da genellikle gençler ve üniversite öğrencilerdir.

Virüs Nedir?

Hayatımızı zehir etmek için virüsler dosyalara ve "boot" sektörlere bulaşabilir. Bunlar boyut olarak küçük, hatta bilgisayarımızdaki en küçük programlardır diyebiliriz. Boyutlarının küçük olmasının nedeni, fazla dikkat çekici olmamaları için makine dilinde yazılmasıdır. Bir incelemede 3551 tane virüs temel alındığında, virüslerin ortalama boylarının 1198 bayt olduğu görülmüş.

Birçok kimse virüs problemini, virüsleri saldıran ve kendi bilgisayarlarını da savunan tarafın olduğu bir mücadele olarak görürler. Peki insanlar neden virüs yazar? Bunun nedeni belki de, virüs yazanların kullanıcıya zarar vermekten çok antivirüs geliştiricilerini hedef almasıdır.

Virüsler Nasıl Yayılır?

Dünyadaki yaklaşık 100-200 milyon kişisel bilgisayar ve Mac kullanıcısının milyonlarcası en az bir kere virüs saldırılarına maruz kalmıştır. Ancak ortalıkta ne kadar virüsün bulunduğu konusunda kimsenin kesin bir bilgisi yok. Çünkü virüsler hakkında hazırlanan raporlar hiçbir zaman tam değildir. Bunun en önemli nedenlerinden biri, virüse maruz kalan insanların karşılaştıkları sorunların kendilerinin yaptığı hatalardan meydana geldiğini düşünmesi, bu yüzden de çoğu virüs problemi gerekli kişilere bildirilmemesi.

Daha 3-4 yıl öncesine kadar işyerlerinde karşılaşılan virüs problemleri evden getirilen disketlerden kaynaklanıyordu. Ancak günümüzde virüslerin daha çok İnternet'ten bulaştığını görüyoruz. Virüslerin sadece küçük bir kısmı gerçekten zararlı. Geri kalanı kötü yazılmış, iyi test edilmemiş, "bug"lı küçük yazılımlardır. Yine de bunları teşhis etmek zaman alır. Dataquest'in bir araştırmasına

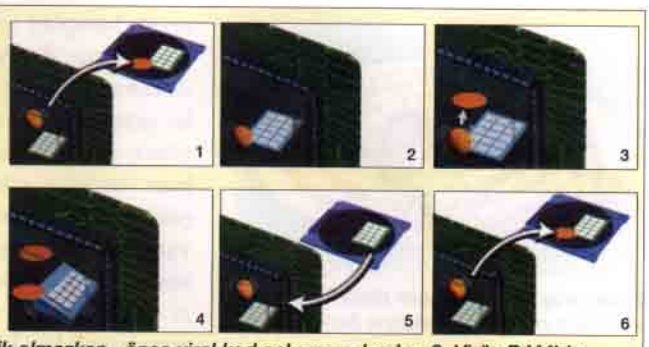
ve değişik birkaç sigorta şirketinin sözcüsünün aktardıklarına göre, bir şirketin kişisel bilgisayarları arasında çoğalan bir virüs, ortalama bir kaç bin dolara ve veri kaybına neden oluyor. Dataquest'in raporuna göre, örneğin bir şirket sadece bir olaydan dolayı 2 milyon dolar kaybetti. En az bir sigorta şirketi, bilgisayar virüsleri yüzünden meydana gelen zararlara karşı, yılda 100 000 dolarlık sigorta poliçesi veriyor.

Son yıllarda bilgisayar virüsleri o kadar önem kazandı ki, büyük bir anti-virüs endüstrisinin doğmasına neden oldu. Dünya çapında bu işle uğraşan düzinelerce şirket, yüzlerce araştırmacı var. Sadece anti-virüs yazılımlarıyla uğraşan bazılarının hisse senetleri Amerikan Borsası'nda el değiştiriyor.

Şu anda virüs ve anti-virüs geliştiricileri arasındaki savaş neredeyse başabaş görünüyor. Ancak yine de özellikle iki olgu var ki, durumu virüs yazanlar lehine çeviriyor. Birincisi, yeni yazılan virüs sayısındaki artış karşısında, artık bu virüsleri inceleyip çözüm bulan anti-virüs uzmanlarının gittikçe daha da zor durumda kalmaları. İkincisi, dünyadaki bilgisayarlararası iletişimin hızla artması. Güncel anti-virüş yazılımlarının bir tek merkezden periyodik bir şekilde dağıtılması da, virüslerin günümüzdeki yayılma hızına göre çok yavaş kalıyor.

Yakın bir gelecekte, bilgisayarlar bilinmeyen virüslerin farkedilmesi durumunda, bunları otomatik olarak tanıyıp ortadan kaldıracak bir sisteme ihtiyaç duyacaktır. Bilgisayar virüslerinin biyolojik isim babalarına karşı doğa böyle bir şeye çare olacak (bu davetsiz misafirleri tanıyıp hatta tanımasa bile hemen tepki verebilecek) bir mekanizmaya sahip: omurgalıların bağışıklık sistemi. İşte bu bağışıklık sistemi mekanizmasını model alarak, anti-virüs yazılım şirketleri kendi yazılımlarını geliştiriyorlar.

Dosya Virüsünün Yaşam Döngüsü



1. Kullanıcı, virüsün bulaştığı bir program çalıştırdığında, bilgisayar başta diskten virüsün hareketsiz bulunduğu programı, çalıştırabileceği yer olan ana belleğe (RAM) kopyalar. 2. Virüsün bulaştığı programda bir değişiklik olmazken, önce viral kod çalışmaya başlar. 3. Virüs RAM'de, programdan ayrı bir yere kendini kopyalar. Bu şekilde kullanıcı sonradan başka programları çalıştırdığında da, çalışmaya devam edebilir. 4. Başlangıç işi bittiğinde, virüs kontrolü tekrardan virüslü programa bırakır. 5. Kullanıcı başka bir program çalıştırdığında, uyuyan virüs tekrar çalışmaya başlar. 6. Kendi kopyasını virüs bulaşmamış yeni programa yerleştirir. Bu şekilde bulaştırma döngüsü kendini tekrarlar.

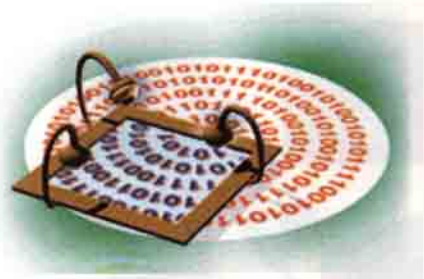
Günümüzde Ulaşılan Nokta

Günümüzde tam bir bilimsel inceleme konusu olarak ele alınmasa da, bilgisayar virüslerinin önemi bilgisayar dünyasında gitgide artmaktadır. Bu kadar yaygın ve önemli olmasının nedeni biyolojik benzerliklerle verilebilir: Bilgisayar virüsleri kendilerini bir yere bulaştırıp (bu bir program ya da bir bilgisayar olabilir), bilgisayar kaynaklarından yararlanarak kendilerini çoğaltabilir. Bunun belirtileri zararlı, hatta yıkıcı olabilir. Biyolojik virüsler nasıl bir toplumda kişiden kişiye yayılıyorsa, bilgisayar virüsleri de bir programdan diğer bir programa, bir bilgisayardan bir başka bilgisayara atlayarak bulaşabilir.

IBM'deki araştırmacılar bilgisayar virüslerine karşı yapılan çalışmaların geliştirilmesinde, virüslerin yayılışının biyolojik virüslere olan benzerliklerinden yararlanıyorlar; virüs yazılımlarına karşı yapılan çalışmalarda, omurgalıların bağışıklık sisteminden ve onun hastalık bulaştırıcıları itici ya da öldürücü yeteneğinden esinlendiklerini belirtiyorlar.

Her ne kadar bir programın bir bilgisayara bulaşması fikri 1970'lere kadar gitse de, 1987 yılında Delaware Üniversitesi'nde birkaç düzine diskette çıkan "Brain" (beyin) adlı virüs ilk virüs olarak kabul edilir. Günümüzdeyse bilgisayar virüsleri yılda milyonlarca bilgisayarı zor durumda bırakıyor. Kullanıcılar da, anti-virüs ürün ve servislerine her yıl yüzlerce milyon dolar harcama yapıyorlar. Bu miktar hızla daha da yükseliyor. Çoğu bilgisayar virüsü kişisel bilgisayarlara saldırıyor. Bugüne kadar 1000'den fazla virüsün ortaya çıktığı biliniyor. Hergün de 6 yeni virüs yaratılıyor. Sınıflandırma yapacak olursak 3 çeşit kişisel bilgisayar virüsü var: dosyalara

	Konağa ihtiyaç duyuyor mu?	Kendini kopyalayarak çoğalıyor mu?
Virüs:	Evet. Virüsler konağa ihtiyaç duyarlar. Mevcut çalıştırılabilir programların içlerine kendini yerleştirerek daha zor saptanabilir ve zaman zaman çalışacak şekilde kendini garantiye alır.	Evet. Bütün virüsler kendi kopyalarını çıkartırlar. Fırsat arttıkça da başka boot sektörlere, master boot kayıtlarına bulaşırlar.
Solucan:	Hayır. Bir konağa ihtiyaç duymazlar. Çünkü solucan tipik bir anaçatı bilgisayar (mainframe) problemi ve kullanıcılardan da gizlenmesine gerek yok.	Evet. Solucanlar fırsat buldukça kendilerini kopyalarlar.
Truva Atı:	Hayır. Her ne kadar "Truva Atı" adı yıkıcı kodlara sahip programları çağrıştırsa da, genellikle tüm COM veya EXE uzantılı dosyalarla çalışıyorlar.	Hayır. Çoğu truva atı, çalıştırıldıkları zaman aktif hale geçirilir. Genellikle hali hazırdaki sürücünün yapısını (FAT'ları, dizinleri) bozar ve bu işlem içerisinde kendini de siler.
Mantık Bombası, Zaman Bombası, Hatalar	Evet. Programcılar diğer kodları yazmadan "hata" (bug) yazamazlar. Aslında şunu da söylemek gerekir ki, çoğu programcı bu hataları isteyerek yazmıyor. Mantık bombaları ve zaman bombaları ise programcılar tarafından, iyi kodların içine yerleştiriliyorlar.	Hayır. Bu kod genellikle kendini kopyalamaktan daha iyi şeyler yapar. Mantık bombaları ve zaman bombaları yaptıkları görünürken, kendilerinin gizli kalmalarını yeğler. "Hatalar" daha fazla hata yapmak dışında herşeyi yaparlar.



İmza tarayıcıları, kullanıcı diskinde bilinen virüslerin program kodlarına benzeyen parçalara bakarlar.

bulaşan virüsler, "boot"-sektör virüsü ve makro virüsleri. Bilinen virüslerin yaklaşık %85'i elektronik tablolama, oyun gibi uygulamaları içeren .EXE ve .COM uzantılı dosyalara bulaşıyor. Ne zaman bir kullanıcı, virüs bulaşmış bir uygulamayı çalıştırsa, ilk önce virüs kodu çalışır ve kendini bilgisayarın ana belleğine kopyalar ve bu şekilde kullanıcının sonradan çalıştırdığı diğer temiz uygulamaları içeren öteki dosyalara bulaşır. Yerleştikten sonra virüs, denetimi yine bulaşmış uygulamalara devreder; kullanıcı bunun varlığından habersiz işlerine devam edecektir. Doğal olarak virüslü program bir şekilde başka bir bilgisayara bulaşacaktır. Bu ya elden ele dolaşan disketle ya da bilgisayar ağlarından olabilir. Bir döngü bu şekilde başlar.

Virüslerin yaklaşık %5'ini oluşturan boot-sektör virüsleri, disketlerin ya da sabit disklerin, bilgisayarınızı ilk açtığınızda okunup belleğe yüklenecek özel bir bölgesine yerleşir. Normalde "boot" sektör, bilgisayar işletim sisteminin geri kalan kısmının yüklenmesi için gerekli bilgilerinin bulunduğu bölgedir. Bir kere bu bölgeye virüs bulaşırsa, sürücüye takılan her türlü diskete ve aynı zamanda sabit diskinize de bulaşır. Bu şekilde virüsler bilgisayarınızı her açtığınızda belleğe yerleşir. "Boot" sektör virüsleri dosyalara bulaşanlardan çok daha etkilidir.

Üçüncü sınıfa giren makro virüsler işletim sistemlerinden bağımsız çalışırlar. Bunlar klasik programlardan farklıdırlar. Birçok elektronik tablolama, veritabanı ve kelime işlemci programları, bir dokümanın içine yerleştirilmiş belli komutları içeren küçük programcıklar çalıştırırlar. Bu programcıklar (ya da makrolar) kullanıcıyı, yinelenecek bir dizi komutu tekrar tekrar girmekten, örneğin bir sürü uzun kelimeyi yazmaktan ya da uzun karmaşık hesapları tekrar tekrar yapmaktan kurtarır. Bu, virüs programcılarını dokümanlar içine kopyalanan makrolar yazmaya yönlendirmiştir. Makro virüsler diğer virüslere göre çok daha hızlı yayılırlar, çünkü birçok kişi pek çok veriyi ortak kullanır. Örneğin bir iş yerindeki bir dosyanın ya da verinin hemen herkes tarafından kullanıldığını düşünün. Bu şekilde bu dosyayı açan birçok kişi kendi bilgisayarına bu virüsü bulaştırmış olacaktır. 1995 yılının sonunda çıkan "Concept" adlı virüs rastlanılan ilk makro virüsüydü ve şu anda dünyada en yaygın olan virüstür. Günümüzdeyse 1000'den fazla makro virüsü bulunmaktadır.

Virüsler, kopyaladıkları temel kodları dışında, onu yazan programcının isteğine göre başka kodlar da içerebilirler. Kimi virüsler ekranınıza sadece mesaj gönderir ya da görüntü yollarken, diğerleri verilere ya da bütün bir programa zarar verebilir.

Antivirüs Teknolojisi

İlk virüslerin belirmesiyle antivirüs yazılımları da piyasaya çıktı. Virüs tarama programları, bilgisayar sistemlerinin virüs bulaşmış bir şekilde hareket edip etmediğini ve düzenli olarak programların kuşku yaratacak değişikliklere uğrayıp uğramadığını kontrol eder.

Virüs tarama programları ise bunun aksine, dosyaları, "boot" kayıtlarını ve belleği, bilinen virüslerin belli yapıdaki birkaç baytlık veri dizisine (virüs örüntüsü) göre tararlar ve nadiren yanlış alarm verirler. Bu tarama programlarının değişik yapılı virüslerin ortaya çıkmasından dolayı, belli aralıklarla güncellenmeleri gerekir. Bu programların tanıdıkları virüs imzaları genellikle kısa, 16 ila 30 bayttır. Buna karşın, bir virüsün tamamı birkaç bin bayttır. Benzer olarak, biyolojik bağışıklık tanıyıcıları da 8 ila 15 amino dizisine bağlanır. Oysa bir viral protein binlerce amino asitten oluşur. Bütün bir virüsü incelemektense küçük bir parçasını incelemek elbette daha elverişlidir. Çoğu bilgisayar virüs tarayıcısı, binlerce virüs imzasını kontrol edebilecekleri, örüntü eşleme algoritmasını kullanır. En iyi algoritmalar 10 dakikadan kısa sürede 10 000 programı, 10 000 virüs örüntüsüne göre tarar.

Antivirüs "Snapshot"ları (enstantane fotoğraflar) çok önemli program ve verilerin matematiksel "parmak iz"lerini alırlar. Bunda sonradan meydana gelen değişiklikler bir virüs bulaştığının işaretidir. İleri algoritmalar, orjinal parmak izlerini kullanarak, programı virüslü durumdan ilk ve bozulmamış duruma geri getirir.

Bir virüs bulunduğu zaman yokedilmelidir. Bunun en kolay ve temiz yolu bulaşmış programı silmektir. Bu tıpkı bir bağışıklık hücresinin hastalıklı hücreyi yok etmesine benzetilebilir. Vücut hücreleri genellikle yenilenebilir, ancak bilgisayar programları ve dokümanlar o kadar kolay gözden çıkarılamayabilir. Sonuç olarak, bilgisayar programları hastalıklı dosyaları silmekten çok, onları mümkün olduğunca onarmaya çalışır. Eğer belli bir virüse ait özel tarama programı, virüs bulaşmış bir dosya bulursa, genellikle programcı tarafından hazırlanan ayrıntılı bir güdüm zincirini izleyerek, sadece virüs kodunu silip dosyayı onarmaya çalışır. Bu "virüse özel" tarama programları, her bulunan yeni virüs için ayrıntılı bir inceleme gerektirir. Program yazarlarına yeni bir virüs gönderildiğinde, yazdıkları yazılımlar virüsün bayt dizilerini istatistiksel olarak inceler.

Kullanılan başka bir biyolojik benzerlik de, programcıların bilinen virüslerin yapılarını kullanarak başka virüsler geliştirmeleri. Virüs tarayıcı programları yazanlar da bundan yararlanarak, kendi programlarında bir tek virüs yapısı örneğiyle düzinelerce virüs tanıyacak programlar yazmaktadır.

Günümüzde makro virüsleri daha çok önem kazanmaktadır. Gelişmiş posta ve dosya aktarım işlevleri sayesinde, kullanıcı eskiye göre daha hızlı ve kolay doküman ve program paylaşabiliyor. Bu da virüs probleminin daha da çabuk yaygınlaşmasına neden oluyor.

Makro virüsleri aynı zamanda bilgisayarların birbiriyle bağlantısından

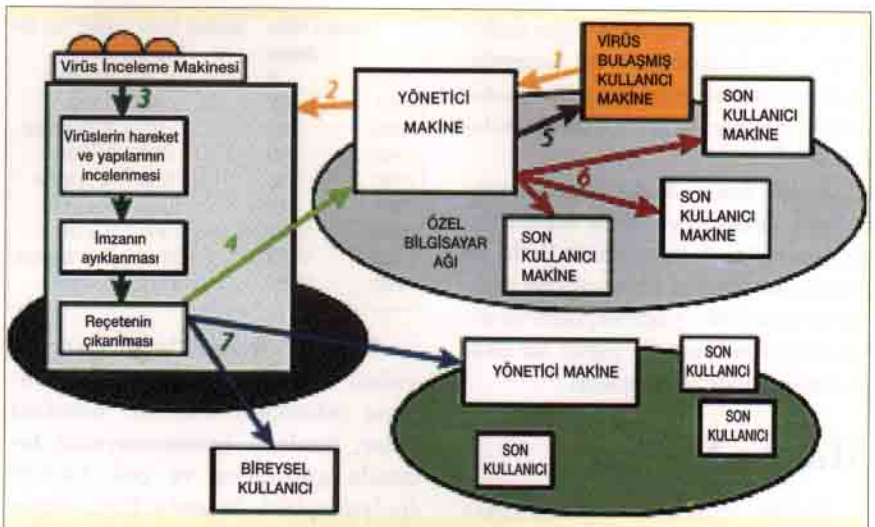
yararlanan ilk virüsler. DOS işletim sisteminin dosyalarına bulaşan eski virüsler hiçbir zaman bir Macintosh'a zarar veremezdi. Ancak makro virüsleri bilgisayarlara her zaman zarar verebilirler. Örneğin Microsoft Word uygulamasını çalıştıran herhangi bir bilgisayar, Concept ya da başka makro virüslerinin geleneksel işletim sistemi sınırlarının ötesine geçmesini sağlayabilir.

Virüs Avı

1990 yılından beri IBM firması, birkaç yüzbin kişisel bilgisayar kullanıcısı topluluğundan virüs istatistikleri topluyor. Şirket kişisel bilgisayar veya disketlere bulaşan virüslerin, kimliği, nerede ve hangi tarihte ne kadar kişisel bilgisayar ya da diskete bulaştığı gibi bilgileri bir araya getirmiş. Bu, şirkete virüslerin davranışları konusunda çok önemli ipuçları veriyor. Virüslerin sadece küçük bir kısmı gerçekten problem çıkarıyordu. Bilinen tüm virüsler, incelenen kullanıcı topluluğunun yalnızca yüzde beşinde; ve bunların çoğunda da sadece bir kere görülmüş. En fazla görülen 10 virüs ise meydana gelen olayların üçte ikisini oluşturuyordu. Buna ek olarak, bu virüslerin yaşam süreci belli bir yapıdaydı. Bir virüs, bir sene ya da daha fazla bir zamanda çoğalıp sayısını doğrusal bir şekilde artırdıktan sonra belli bir düzlüğe ulaşıyor. Bundan sonra, bilgisayarlarda görülmeye devam ediyorsa da, bazen yok olma derecesine bile düşebiliyor.

Virüslerin bu özelliklerini anlamak amacıyla IBM biyolojik salgın hastalıklarının matematiksel modellerinden yararlandı. En basit modele göre yapılan tahminlerde birkaç parametreden yola çıkılıyor. Buna göre en belirgin parametreler; hastaların birbirlerine bulaştırdıkları dönemdeki doğum hızı ve ölecek ya da tedavi edilebilecek hastadaki ölüm hızı. Eğer bu iki hız arasındaki oran belli bir kritik değerin altındaysa o zaman herhangi bir bulaşıcı hastalık yok olacaktır. Bu oran ne kadar büyükse, o zaman bir salgının tek seferde bulaşacağı topluluk kesiminin büyüklüğü de aynı şekilde daha fazla olacaktır.

Ancak yapılan gözlemler böyle basit bir bakış açısının yetersiz olduğunu gösterdi. Buna göre, doğum-ölüm oranı kritik değere yaklaşmadıkça, virüs ya yok olmalı ya da büyük bir hızla artarak evrensel hale gelmelidir. Oysa birçok virüs toplam popülasyonun küçük bir kısmında varolacak şekilde dayanıyor. Bu basit modelde önemli bir hata da, popülasyondaki "birey"ler arasında sabit bir temas şansı olduğunu kabul etmektir. Daha gelişmiş modeller, yazılım değiş-tokuşunda meydana gelen olağandışı farklılıkları hesaba katıyorlar. Genel olarak her birey yazılım ve verileri sadece birkaç kişiyle paylaşıyor ve bu paylaşım çoğunlukla grup içerisinde meydana geliyor. Örneğin, Ayşe Mehmet'le, Mehmet Ali'yle, Ali de Ayşe'yle üçlü bir grup oluşturarak paylaşıyor olabilir.



Siberuzaydaki Sayısal Bağışıklık Sistemi'nin çalışması burada gösterildiği şekilde planlanmıştır. Bilinmeyen bir antivirüs, yönetici makinaya bir örnek göndermesi için kullanıcı makinayı harekete geçirir. (1) Bu da merkez virüs inceleyici makinaya şifrelenmiş bir örnek gönderir (2). Bu makina bu virüsün bir kopyasını çıkarır ve bunun hareketlerini ve yapısını inceler (3). Sonuçta çıkan reçete tekrar yönetici makinaya gönderilir (4). O da bunu, ilk olarak virüsün bulaştığı makinaya iletir (5) ve sonradan ağ üzerindeki diğer makinalara (6). Bütün dünyadaki diğer aboneler de bu yeni virüsten kendilerini koruyacak güncel antivirüs ürünlerini alır.

Sayısal Bağışıklık Sistemi

"Sayısal ekosistem"de hızla gelişen bu virüs trafiğine artık dur diyebilecek tekniklere ihtiyaç duyar. IBM, McAfee Associates gibi firmalar, yeni virüslere karşı hızlı ve otomatik olarak cevap verecek yeni teknolojiler gelistirmeye çalışan firmalar arasında. Şu anda IBM siberuzayda "bağışıklık sistemi" olarak adlandırılabilecek bir teknoloji geliştirmekte. Örneğin IBM AntiVirus programını çalıştıran kişisel bilgisayarlar, bir bilgisayar ağı aracılığıyla virüsleri inceleyen bir merkez bilgisayara bağlı olacaklar. Her kişisel bilgisayardaki inceleme programı, sistemdeki ya da programdaki kuşku veren değişikliklere göre, virüs bulaşmış olan programların bir kopyasını bilgisayar ağı aracılığıyla virüs inceleme makinesine gönderebilecek.

Bu kuşkulu örneği alan makine, bunu virüs inceleme makinesine gönderir. Makinedeki yazılım bu örnekteki virüsleri harekete geçirecek şekilde ona yem atar. Aktif hale geçen virüs kodu bu yemlere bulaşır. Bu evre içinde virüsün diğer özellikleri de ortaya çıkar. Artık virüsün bulaştığı bu yemler bağışıklık sisteminin diğer parçaları tarafından incelenmeye hazırdır. Burada kodlar açığa çıkar ve sistem, virüsü temizleme yöntemini belirler. İnceleme makinesi bu yöntemi virüsün bulaştığı kişisel bilgisayara ulaştırır. Virüsün bulaştığı makine, kendi tarama aracının altında bulunan, bilinen virüsleri içeren veritabanına bu yöntemi ekler. Bundan sonra makine virüsü temizler ve daha sonra meydana gelebilecek aynı virüsün saldırılarına karşı bağışıklık kazanmış olur.

Eğer virüsün bulaştığı bilgisayar bir yerel bilgisayar ağına bağlıysa, bü-

yük bir olasılıkla bu virüs diğer makinelere de bulaşmıştır. Bu sistemle, virüs temizleme yöntemi diğer makinelere de otomatik olarak dağıtılacaktır.

Ancak, her ne kadar antivirüs teknolojisi gelişse de, virüs teknolojisi de buna göre ilerleyecektir. Belki de bilgisayar virüsleri ve bilgisayar bağışıklık sistemleri, yaşayan, ölen ve avlananların bulunduğu yapay bir ekosistemin habercileri sadece.

Makro Virüsleri

Makro virüsleri öteki virüslere birçok yönden benzer. Bunlar belli koşullarda kendi kopyasını çıkartarak çoğalabilen kodlardan ibarettir. Bunlar, öteki virüsler gibi zarar verecek, ekrana mesaj yazdıracak ya da diğer programların yapabildiklerini yapabilecek biçimde yazılabilir.

Makro Virüsleriyle Öteki Virüslerin Arasındaki Fark

Makro virüsleriyle öteki virüs çeşitleri arasında birtakım farklar vardır.

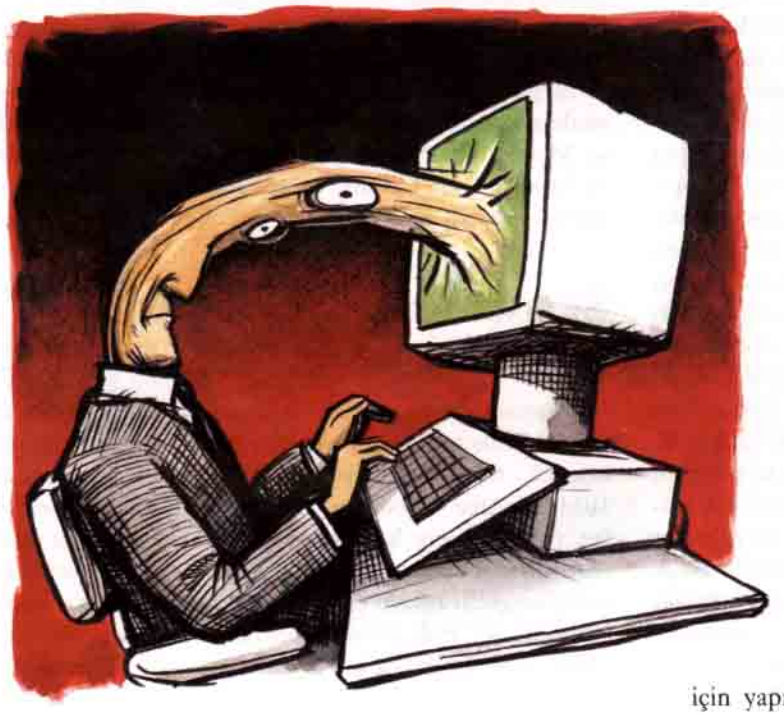
* "Boot" virüsleri her zaman makine dilinde yazılır, seyrek olarak da C gibi üst düzeyli dilde yazılır. Makro virüsleriyse her zaman makro dilinde yazılır.

* Bilgisayara boot virüsünün bulaşması için bilgisayarın, boot virüsü bulaşmış bir disketle açılması gerekir. Dosya virüsü bulaşması için de virüsün bulaştığı bir dosyanın kopyasını çalıştırmalıdır. Makro virüsünün bulaşması için, virüsün bulaştığı bir dokümanı çift tıklamayla açmak yeterlidir. Dosya yüklenirken, program makroları da bir yandan çalışır ve bilgisayara virüs bulaştırır.

Yıl	Yazılan Virüs Sayısı	Toplam Virüs Sayısı	1997'nin En Yaygın Virüsleri
1986	8	8	1.Cap
1987	32	40	2. Concept
1988	33	73	3. Wazzu
1989	150	223	4. Antiexe
1990	333	556	5. FORM
1991	746	1302	6. Laroux
1992	1260	2562	7. Anticmos
1993	1082	3644	8. Junkie
1994	2730	6374	

* Birçok modern "boot" ve dosya virüsü, son derece gelişmiş programlama teknikleri kullanır. Bundaki amaç, bunların saptanamayacak biçimde görünmez ve çok biçimli (polymorphic) olmasıdır. Buna karşın günümüzde makro virüsleri hâlâ, basittir. Çok azı, gizli (stealth) niteliktedir (Hot, Nuclear, Xenixos) bazıları da (Atom, Colors, Divina, FormatC, Hot ve Nuclear vb.) ne yaptıkları belli olmasın diye, şifrelenmiş, sadece çalıştırılabilir (execute only) makrolar kullanır.

Makro virüsleri ve Makro truvalar arasında fark vardır. Truvalar kendi kopyalarını çıkarmaz. Her ikisi de zarar verir. "Auf Wiederöffnen" ve "FormatC" truvadır, virüs değil. Bazı makro virüsleri çok büyük zararlar verir. Örneğin, "Hot" virüsü, belgelerin silinmesinde çok etkilidir. "MDMA" ise Macintosh, Windows 3.x, Windows NT ve Windows 95'e zarar vermek için kodlanmıştır.



Makro Virüslerin Çalıştıkları Platformlar

Makro virüsleri makro dilinde yazılır. Bu nedenle bunlar, makro komutlarının anlaşılıp, uygulanacağı herhangi bir ortamda çalışabilir. Bu yüzden WordBasic'te yazılmış Word.Concept adlı virüs, Word'ün İngilizce sürümünü kullananların belgelerine bulaşabilir. Çünkü sadece Word'ün İngilizce sürümünün anlayabileceği iki makro (AutoOpen ve FileSaveAs) kullanır. Ancak, Macintosh, DOS, Windows NT'de çalışacağından bu virüs bu platformlarda bulaşabilir.

Bazı makro virüs çeşitleri, belli tabanların özel olanaklarından yararlanır. Bunlar yalnızca o tabanda çalışır. Bu yüzden "Hot" Windows API'lerini kullanır ve Macintosh ya da Windows 95'lere bulaşmaz. Bir uygulamanın farklı işletim sistemlerinde çalışabilir olması farklı platformlarda çalışan virüslerin yazılmasına olanak verdi (bu çalıştırılabilir dosyalara bulaşan virüslerle mümkün olmayan bir durumdu).

Makro virüsleri her zaman uygulamaya özeldir. Örneğin "Laroux" isimli bir virüs, sadece Excel uygulaması kullanıcılarına bulaşır, "Green Stripe" ise yalnızca AmiPro uygulaması kullanıcılarının bilgisayarına bulaşır. Bu aynı tip ancak farklı uygulamalarda bir sorun çıkaramıyor. Örneğin Word Perfect kullanıcılarına Word makro virüsü, ya da 1-2-3 kullanıcısına Excel makro virüsü bulaşamaz.

Kimi makro virüsleri de dile özeldir. Örneğin, "Friendly, LBNYJ, NOP ve Xenixos" Microsoft Word'un Almanca sürümünü, "Concept.B.FR" ise Word'ün Fransızca sürümünü gerektirir. Her dilde çalışan makrolar kullanan virüsler, her dil için yapılmış uygulama sürümle-

rinde çalışabilirler. "Wazzu" yazılan ilk çok dilli makro virüsü olarak kabul edilir. Bu Word'ün her dilindeki sürümde olan "AutoOpen" makrosunu kullanır. Öteki virüsler ve truvalar ("Anti-DMV, FormatC, Guess" gibi) benzer şekilde bir çok dildeki sürümlerde çalışabilir.

Bütün makro virüsleri her zaman otomatik olarak bulaşmazlar. Ancak makro başlangıcında "Auto" bulunduran makro virüsleri genellikle otomatik olarak bulaşır. Bu yüzden "Concept" AutoOpen makrolarını çalıştırır. "Colors" gibi öteki virüs çeşitleri de kullanıcının belirli hareketleri yapmasını bekler (Colors, kullanıcı, Dosya/Yeni ile yeni bir dosya yarattığı zaman bulaşır, Dosya/Kaydet ile bulaşmış dosyayı kapatır, Autosave ile dosyayı kaydeder ya da Araçlar/Makro ile makroları listeler).

Şablonlar

Makro virüsleri sadece birkaç makro kümesinden oluşur.. Makrolar, uygulamanın makroları sakladığı yerde bulunur. Microsoft Word'de ise, makrolar belgeler yerine şablonların içinde saklanır. Word .DOT uzantılı herhangi bir belgeyi şablon belge ve öteki uzantılara sahip olanları normal belge olarak algılar. Ancak, şablon yapısındaki ve makro bulunduran bir dosyada yazı bulundurabilir ve ekranda standart bir belgeymiş gibi görünür. Böyle bir şablon belgede herhangi bir uzantıya sahip olarak saklanabilir. Bu yüzden Word makro virüsleri bilgisayara .DOC uzantısıyla şablon belge olarak gelir. Böyle bir dosya yüklendiğinde, hem şablon belge olarak (makrolar çalıştıran), hem de belge olarak (içindeki yazı okunabilen) hareket eder.

Bütün makro virüsleri "genel şablon"a (NORMAL.DOT) bulaşır. Çoğu, belgeleri şablonlara .DOC uzantısıyla dönüştürür. İşte bu dosyaların kendilerine makro virüsleri bulaşmıştır. Kullanıcılar .DOC uzantılı bir dosyanın, içinde yazının bulunduğu şablon belge mi, yoksa gerçek belge mi olduğunu bilmez. Bu nedenle virüs bir kullanıcının haberi olmadan bir sisteme girebilir.

Bulaşma Olasılığı

Bir makro virüsünün bulaşması, her gün açıp baktığınız yeni, bilinmeyen belge sayısıyla orantılıdır. Eğer dışarıya yeterince kapalı bir sisteminiz varsa, virüslerin bilgisayarınıza bulaşma oranı çok düşüktür. Diğer yandan her gün düzinelerce yeni belgeyle çalışıyorsanız bu oran çok yükselir.

Virüslerin size bulaşma oranı, aynı zamanda çalıştığınız yeni belgeleri virüs taramasından geçirmenize de bağlıdır. Buna göre şimdiye değin sadece iki site "Laroux" virüsüne yakalandığını bildirmiştir. Bu iki sitede (biri Alaska'da, bir diğeri ise Afrika'da) çalışmıyorsanız, bugün bu virüslere yakalanma ihtimaliniz de sıfırdır.

Elbette, böyle bir virüs yeterince yaygınsa, yeni bir elektronik tablo (spreadsheet) belgesine çift tıklamak riskli hale gelir.

Makro Virüs Olgusu

Makro virüslerini herhalde şu iki olay en iyi biçimde tanımlar:

1. Bunlar ortaya çıkan diğer virüs çeşitlerinden çok daha hızlı yayılıyor. Örneğin Word.Concept virüsü, ilk çıktığı 1995 Temmuz ayından 1996 Nisan ayına değin tüm dünyada bildirilen virüs olaylarının % 25'ini oluşturuyordu. Bu olaylar Amerika, İngiltere, Finlandiya, İsveç, Rusya, Fransa, Almanya, Hollanda, Türkiye ve Kanada'dan bildirilmiştir. O zamana değin hiç bir virüs bu kadar hızlı yayılmamıştır.

2. Değişik makro virüs çeşitleri büyük bir hızla artıyor. Bu engellenemez bir durum. Çünkü makro virüslerini yazmak, makine dilinde yazılan diğer virüslere göre, çok daha kolay. Üstelik dünyada makro yazabilecek insan sayısı, makine dilinde yazabilen insan sayısının çok üzerinde. Bundan başka, birçok makro virüsü şifreleme kullanmıyor (örneğin: Nuclear.B), makroları da "yeni" makro virüs yazarlarınca daha kolay inceleniyor.

Savunma İçin Yeni Kurallar

Makro virüsleri, virüslere karşı kullanılan birçok savunma kuralını değiştirmiştir.

1. Daha önceleri bir virüsü yazıp okuyabileceğiniz bir program kullanarak makinenize bulaştırmıyordunuz. Oysa şimdi makro virüslerinde, kullandığınız program, makroları yorumlayıp çalıştırırsa o zaman bilgisayarınıza virüsü bulaştırmış oluyorsunuz.

2. Eskiden e-posta yoluyla virüs bulaştırmıyordunuz. Ancak şimdi e-postanıza eklenmiş olan makro virüsünün bulaştığı bir belgeye sadece bakmak, virüsü bulaştırmanız için yeterli (e-posta mesajlarının kendisine virüs bulaşmıyor, bu yüzden de bunlar tehlike kaynağı değiller).

3. Eskiden tüm belge ve veri tabanlarını virüs bulaşmış mı diye taramanıza gerek yoktu. Günümüzdeyse her türlü uzantıya sahip dosyada bulunabiliyor (Word, belgelerin her türlü uzantıya sahip olmasına olanak veriyor).

4. Eskiden kullanıcılara kaynakları güvenilir olan programları çalıştırması tavsiye edilirdi. Bu durumda şimdi, sadece daha önceden açmış olduğumuz belgeleri açmalıyız, bu da çok kısıtlayıcı bir durum.

İnternet makro virüsleri için farkına varılmayan bir araçtır. Birçoğu İnternet aracılığıyla genellikle de haber grupları aracılığıyla dağıtılmıştır. Unutmamak gerekir ki, ilk makro virüsü, İnternet'e bir belgenin içinde yollanmıştı (bu belgede de bu tip virüslerin nasıl yazıldığı anlatılıyordu!).

Alkım Özaygen

Konu Danışmanı: Ali Saatçi
Prof. Dr., Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü

Kaynaklar:
www.av.ibm.com
www.sevenlocks.com/quarc/VirusHandbookhtm
www.sciam.com/1197issue/1197kephart.html
kumiti.com/myths
www.stiller.com
www.ncsa.com/virus