

## VİRÜSLER

Virüsler, genellikle bilgisayara zarar vermek amacıyla yazılmaktadır.

**Virüslerin Yayılışı:** Virüslerin bir başka programa yapışarak yayılmaktadır. Bir virüs, kelime işlemci, tablolar programı, e-posta programınıza, dosyalarına, boot (hard disk veya disketinizin başlangıç adresine) yerleşerek sürekli çoğalır ve yayılır. Virüsü kapmış olan dosya ya da disket, bilgisayara takılıp içindeki dosya açıldığında virüs çalışmaya başlar. Genellikle belleğe gider ve orada diğer dosyalara bulaşmak için fırsat bekler. Bir sonraki çalışan program ya da dosya veya diskete bulaşır. Virüslerden bazıları, belli tarihlerde çalışıp ekrana resim, mesaj çıkarır (etkisi az olan virüsler). Bazıları ekran ayarlarını değiştirir ya da sisteminizin yavaşlamasına neden olur (orta şiddette etkili virüsler). Bazıları da veri kaybı, sistem çökmesi, dosyaların hasar görmesine neden olur (çok zararlı virüsler).

**1. Dosyalara bulaşan virüsler:** Genellikle COM, EXE uzantılı dosyaların kaynak koduna kendilerinin bir kopyasını eklerler. SYS, DRV, BIN, OVL, OVY uzantılı dosyalara da bulaşan virüsler de vardır. Bazı virüsler dosyaların açılmasını beklemeden de çoğalabilir. Örneğin DOS'da DIR çekildiğinde diğer dosyalara bulaşan virüsler de vardır.

Dosyalara bulaşan virüslerin büyük bir kısmı, EXE dosyanın başlangıç kodunu alarak başka bir yere yazar. Dosya çalıştırıldığında önce virüs harekete geçer, başlangıç kodunu çalıştırır. Her şey yolunda gidiyormuş görünür. Bazıları da COM uzantılı ikinci bir dosya yaratarak içine kendi kodunu kopyalar. DOS tabanlı işletim sistemleri önce COM uzantılı dosyaya bakacağından farkında olmadan virüsü çalıştırır.

**2. Boot sektörü virüsleri:** Disk ve disketlerde (A, C, D, E, ...) olarak bilinen mantıksal bölümlerin her birinde boot sektörü vardır. Boot sektörde diskin formatı ve depolanmış verilerin bilgileriyle DOS'un sistem dosyalarını yükleyen boot programları bulunur. Bir boot virüsü boot dosyalarına bulaştığında, bu disk veya disketten bilgisayar açılmaya çalışıldığında "Non-system Disk or Disk Error" mesajı verilerek bilgisayar açılmaz. 1996 yılına kadar en yaygın virüsler bu cins virüslerdir. Boot virüs, belleğe yerleştikten sonra takılan her diskete bulaşır.

**Master Boot Record Virüsleri:** Sabit diskin ilk fiziksel sektörlerinde diskin Master Boot Record'u ve Partition Tablosu vardır. Sabit Diskin Master Boot Record'unun içindeki Master Boot Programı partition tablosundaki değerleri okur ve boot edilebilir partition'ın başlangıç yerini öğrenir. Sisteme o adrese git ve bulunduğu ilk program kodunu çalıştır komutunu gönderir. Bu virüsler de boot sektör virüsleri gibi bulaşır.

**Multi-Partite Virüsler:** Boot Sektörü virüsleri ile Master Boot Record virüslerinin bileşimidir. Hem MBR'a hem boot sektörü ve çalıştırılabilir dosyaları bozarak yayılma şanslarını bir hayli artırmış olurlar.

**3. Macro Virüsleri:** Microsoft Word ve Microsoft Excel gibi popüler uygulama programlarının macro dillerini kullanılarak yazılıyorlar. Macro'lar veri dosyalarında kaydedildiği için virüslü belge

açıldığında virüsün makro kodu çalışmaya başlar.

#### 4. Script Virüsler:

**Trojan Horse (Truva Atı):** Bilgisayarınızda arka planda çalışan ve zamanı geldiğinde aktif hale gelerek sisteminize zarar veren yazılım. Sabit diski formatlamak, dosyaları silmek ya da çökertmek gibi çok zararlı işler yapar. Kötü amaçlı program olmalarından dolayı virüslere benzetilebilir. Benzemeyen yönleri ise, Truva atlarının zararsız bir programmış gibi gözle görülür olmaları ve kendi kendilerini çoğaltarak başka bilgisayarlara yayılmamalarıdır. Windows 95/98 veya Nt kullanıyorsanız trojanlara ( casus yazılım diyebiliriz.) çok dikkat etmelisiniz. Bu tip bir trojan size nasıl ulaşabilir ?

1 ) Elektronik posta yolu ile kötü niyetli veya şakacı bir arkadaşınız tarafından yollanabilir.

2) IRC kanallarında chat yaparken size birisi bakın bu çok hoş bir program mutlaka al diyerek sizin trojan yazılımı bilgisayarınızda çalıştırmanıza sebep olabilir.

3) CD-ROM veya disket yolu ile başka bir kullanıcıdan gelebilir. Eğer bilgisayarınızda trojan yazılımı engelleyen bir koruma programınız ( yani iyi bir anti - virus yazılımınız ) yoksa başınıza gelebilecek olaylar şunlar olabilir ..Tabii bunlar sadece İnternet bağlantınız varken geçerli olabilir.

#### Trojanın sizde aktif olduğunu bilen kişi ;

- Sabit disklerinize cd rom veya diğer disket sürücülerinize sizin ulaştığınız rahatlıkla ulaşabilir.

- Sabit veya taşınabilir disklerinize her türlü işlemi yapabilir. - İnternet şifrenizi öğrenebilir.

- İsteddiği dosyayı okuyabilir, silebilir.

- İsteddiği dosyayı kendi bilgisayarına indirebilir.

- İsteddiği dosyayı sizin bilgisayarınıza yükleyebilir.

- Sizin yazdıklarınızı izleyebilir. Eğer kamera takılıysa sizi canlı olarak izleyebilir.

-Bilgisayarınızda çalışan herhangi bir programı kapatabilir.

- Eğer bir bilgisayar ağına sahipseniz sizin sayenizde tüm ağ üzerinde işlem yapabilir.

-Bilgisayarınızı kapatabilir veya yeniden başlatabilir.

Bu yukarıdaki özellikleri Netbus ve BO adlı trojan yazılımlar çok rahat gerçekleştiriyor. Bu yüzden siz siz olun mutlaka trojanlardan korunun.

**Worm:** Bellekteki ve diskette eriştiği bölgelerin verilerini bozar. İçine gömülüp saklanacağı bir ev

sahibi programa gereksinimi olmadığından virüslerden ayrılır.

Virüsler, bilgisayarın işleyişinin kesilmesine, dosyaların silinmesine, sistemin yavaşlamasına yol açar. Virüsler, disketlerde bulunan programların içinde gizlenmiş olarak bulunur. Disket, disket sürücüyeye takılıp, virüslü dosya veya disket okutulduktan ya da içindeki programlar çalıştırıldıktan sonra bilgisayara geçer.

**Spam:** bir mesajın arka arkaya gönderilmesi. Spam ağı tıkar, pdsta dağıtımını yavaşlatır. Bir tür virüs olarak nitelenebilir. Ardarda gelen gereksiz elektronik postalar yüzünden bilgisayarda çalışamaz hale gelebilirsiniz.

Sabit Diskleri virüslerden korumak gereklidir.

#### **Virüslerden korunmak için ipuçları:**

- Antivirüs programı kullanın. Virüs tarama programınızı internette **bir kaç günde bir güncelleyin.**
- Birden fazla virüs programı kullanın. Her virüs programı bütün virüsleri tanımaz.
- Temiz açma disketi bulundurun.
- Disketleri ve elektronik postaları virüs tarama programından geçirmeden açmayın.
- Bilmediğiniz dosyaları açmayın.
- Tanımadığınız birisi tarafından gönderilen dosyaları açmayın.
- Virüs uyarılarını dikkate alın.
- Her zaman dosyalarınızın yedeğini alın.
- BIOS setup'ından Boot sırasını C:, A: yapın. Böylelikle disket sürücüde unutulmuş olan virüslü disketten Sabit diske açılış sırasında virüs geçmesi önlenmiş olur.

·Virüsler ayrıca modemle iletişim sırasında da geçebilir. Ayrıca kopya programlarda da virüs bulunabilir. antivirus programlarının bulunduğu siteler:

<http://www.avg.com> [AVG75free.zip](http://www.avg.com)

<http://www.mcafee.com>

<http://www.symantec.com>

<http://www.antivirus.com>