D.E.Ü. İ.İ.B.F. Dergisi
Cilt: 11, Sayı: II, 1996, ss.239- 248

BİLGİSAYAR VİRÜSLERİ

Mustafa GÜNEŞ (*) **Ahmet ALABACAK (**)**

ÖZET

Bilgisayar virüsleri, son 7-8 yıldır bilgisayar kullanıcılarını rahatsız eden bir konudur. Virüs, özel amaçla hazırlanmış 5-10 KB. uzunluğunda bir tür bilgisayar programıdır. Bu programlar, bilgisayarın disk disket gibi yan bellek birimlerinin boot sektörlerine veya COM ve EXE tipi programlarına bulaşırlar. Bulaşmaları elden ele dolaşan disketler yada networkler yolu ile olur. Bulaştığı yerlerde yada programların üzerinde tahribat yaparlar.

Varlıkları ekranda beklenmeyen görüntü ve mesajların görünmesi, klavyenin kilitlenmesi, bilgisayarın çalışma hızının düşmesi, COM ve EXE tipi programların uzunluklarının değişmesi ile anlaşılır.

Virüsler, veri dosyalarını bozar, sistemin açılışını kilitler, programları çalıştırmazlar. Bu çlışmada virüsler hakkında ganal bir bilgi verildikten sonra tipleri üzerinde durulmuş ve korunma yolları anlatılmıştır.

1. GİRİŞ

1988 yılının 2 Kasım günü ABD' de İnternet ağı içindeki 6000 bilgisayar terminalinde, içlerinde çok sayıda önemli bilim adamı ile araştırmacılarının da bulunduğu kullanıcılar grubu garip bir süprizle karşılaştılar. Bilgisayar terminallerini kullanamıyorlar ve sistemleri de iş yapamaz duruma gelmişti.

Olay, araştırıldığında Robert Morris Jr. adlı bir kişinin sisteme yerleştirdiği virüs programının etkisi ile olduğu anlaşılır. Bu kişi kendini başkalarına kanıtlamak istediğini ve biraz da eğlenmek için bu işi yaptığını söylemiştir. Ancak gözden kaçan ufak bir hata programın kontrolden çıkmasına ve İnternet ağının çökmesine, sonuçta da 98 milyon dolarlık bir zarara sebep olmuştur.

1991 yılı sonuna kadar 700' den fazla bilgisayar virüsünün ortaya çıktığı görülmüştür. Bugün ABD' de virüs araştırma kuruluşu olarak faaliyet gösteren MCAfee firmasına göre virüs problemi ile ilgili olarak günde ortalam 42 başvurunun yapıldığı belirtilmiştir. Şu anda 500 farklı bilgisayar virüsü ve 3000' den fazla virüs olduğu, 1995 yılı sonuna kadar ise 40.000 virüs çeşidine ulaşılacağı tahmin edilmektedir.

(*) Doç.Dr. D.E.Ü. İ.İ.B.F. Ekonometri Bölümü.

(**) Öğr. Gör. D.E.Ü. İ.İ.B.F. Ekonometri Bölümü.

Virüs programlarının, ekonomik ve kültürel olarak geri kalmış yada kendini kanıtlamak isteyen Bulgaristan, Pakistan, İsrail gibi ülkelerde üretildiği söylense de ortaya çıkışlarının bir başka sebebi de ticaridir.

AT&T Bell Laboratuvarları araştırmacılarından M. Douglas Mcilroy 1972' de Darwin adını verdiği bir bilgisayar oyunu yazmıştır. Bu oyunda program aktif hale geldiğinde diğer programların yerlerini alarak onları tyok etmeye çalışıyordu.

Sonraki yıllarda çeşitli bilim adamları, bilgisayarcılar benzeri programlar üzerinde çalışarak bu tür programların bilgisayara zarar verebileceğini işaret etmişlerdir.

Son 7-8 yılda bilgisayar dünyasında sıkça konuşulan ve özellikle mikro bilgisayarlar üzerinde etkili olan, kısaca virüs diye adlandırılan zararlı yazılımlar hakkında neler biliyoruz? Zararlı yazılım nedir? Virüs denilen bu yazılımların yapısı nasıldır? Çeşitleri nelerdir? Nasıl bulaşırlar? Zararları nedir? Korunma ve temizleme yöntemleri nelerdir?

Yukarıda sıralanan bu sorular çok kimselerce ya hiç bilinmemekte ya da kulaktan dolma yarım bilgilerle cevap bulmaktadır. İşte bu yazı içerisinde bu verilecek, daha sonra virüslerin bulaşma şekilleri, korunma yolları ve daha sonra da temizleme yöntemleri açıklanacaktır. Bu arada bilinen bazı virüsler ile bunları temizleyen programlar hakkında da bilgi verilecektir.

2. ZARARLI YAZILIMLAR

2. 1. Zararlı Yazılım Nedir?

Zararlı yazılım bilgisayarın kendisine ya da işletilen programına öyle ya da böyle herhangi bir şekilede olumsuz etkisi olan bilgisayar programlarıdır. Zararlı yazılımlar yıkıcı olan ve yıkıcı olmayanlar olmak üzere iki gruba ayrılır.

2. 1. 1. Yıkıcı Olan Yazılımlar

Bu yazılımların yaptıkları zararlar aşağıdaki gibi sınıflandırılmaktadır.

a) Toplu Yıkım: Disketi alçak düzey formatlayarak verinin yok olmasına neden olan yıkımdır.

b) Bölümsel Yıkım: Diskin bir bölümünün silinmesi veya değiştirilmesine neden olan yıkımdır.

c) Seçimli Yıkım: Belirgin kütükler üzerinde silme yada değişiklik yapan yıkımdır.

d) Rastgele Yıkım: En tehlikeli yıkım sınıfıdır. Disk veya RAM (Read Only Memory) Ana bellekte verilerin rastgele değiştirilmesine neden olan yıkımdır.

2. 1. 2. Yıkıcı Olmayan Yazılımlar

Bu tip yazılımlar disk veya kütüklere zarar vermeyen, sadece yaratıcısının dikkat çekmek amacı ile yarattığı ve ekranda mesaj görüntüleme, çeşitli renkler oluşturma, harflerin bir kısmını veya tamamını büyük veya küçük harf yapma gibi klasikleşmiş işler yapan yazılımlardır.

Zararlı yazılımlar yapılarına göre Varm (Solucan), Trojen Horse (Truva Atı), Virüs olmak üzere üç ana gruba ayrılırlar. Bunlar sırasıyla aşağıdaki özellikleri taşımaktadırlar.

Varm (Solucan): Çalıştırıldığında kendi kendini kopyalayarak büyüyebilen, kendini, iletişim ağları ile diğer bölümlere aktarabilen yazılım türüdür.

Trojen Horse (Truva Atı): Çalıştırılmadığı sürece zararsız olup, Varm gibi kendini kopyalayarak çoğalan yazılım türüdür.Memory ya da ikinci bellekteki yazılımları yok edebilirler. Bu tür yazılımların iki tUr ıslevi vardır.

1- Kullanıcıya, kendini kulllanması için Cekici özellikler sunarlar (Oyun programı, özgün formatlama gibi...).

2- Çalıştırıldığında üzerinde bulunduğu sisteme mutlaka zarar veren oğeler taşırlar.

Bunlar, işlevlerini yerine getirebilmek için ayrı bir yazılıma (ev sahibi yazılım) ihtiyaç duymazlar.

Virüs: Tek başına çalışmayıp işlevlerini yapabilmek için başka bir yazılıma ihtiyaç duyan kötü amaçlı özel yazılım türüdür.

Virüs Nedir?

Virüs sözcüğü Ana Britannica Ansiklopedisinin 22. cilt 23. sayfasında "Yalnız, canlı bakteri hayvan ya da bitki hücrelerinde çoğalabilen küçük ve basit yapılı enfeksiyon (hastalık) etkeni" olarak tanımlanmaktadır. Gelişim Larouse da ise "Organik virüs, optik mikroskopla görülmeyen, genellikle bakteri geçirmez süzgeçlerden geçen ve özellikle tek tip nükleik asit içermekle önanyot hücrelerde zorunlu asalak olmakla bakterilerden ayrılan mikroorganizma" olarak tanımlanmaktadır. Görüldüğü gibi biyolojik olarak tanımı bulunan virüsün, bilgisayar virüsü olarak tanımı nasıl yapılabilir? Bu tanım;

Ana belleğe yerleşerek kendini kopyalama yöntemi ile çoğaltan ve belli

bir koşulla karşılaştığında da aktif hale gelen, çeşitli zararları olan yazılımlara virüs denilir diyerek yapılabilir.

Bilgisayar virüsleri ile biyolojik virüsler arasında bir çok yönden benzerlik bulunmaktadır. Bu benzerlikler;

1- Yerleştikleri iyi ortamlarda ürüyor ve çoğalıyorlar.

2- Üremek için yerleştikleri yerin imkanını kullanıyorlar.

3- Belirtiler ortaya çıkmadan önce bir suskunluk devresi (kuluçka dönemi) geçiriyorlar.

4- Kontrol edilmediklerinde ölümcül olabiliyorlar.

5- Bir taşıyıcı vasıtası ile yeni sistemlere transfer olabiliyorlar.

6- Ev sahibini işgal ettikleri için imhaları güç oluyor.

Bu benzerliklerin yanında;

Telefon hatları ile diğer ülkelereseyahat edebilme gibi bilgisayar virüslerinin ayırıcı özellikleri de bulunmaktadır.

3. VİRÜS PROGRAMLARI

3. 1. Virüs Programlarının Sınıflandırılması

Virüsler çalışma biçimi ve yerleştikleri yere göre 4 gruba ayrılır.

3. 1. 1. Kabuk (Shell) Virüsler

Bu virüsler, kendilerini bir ana programın çevresine sarar ve özgün programı bozmazlar. Ana program çalışmadan önce bu virüs programı çalışır. Sonra denetimi ana programa bırakır. Bu çalışma şöyle olur; Virüs programı belleğe yerleştiği anda kendi adresini sisteme programın işletilebilir ilk komutunun adresi olarak tanıtır. Böylece ana program işlemeden kendi çalışmış olur. Kabuk virüsler, programın boyunu uzattıklarından yakalanmaları kolay olur.

3. 1. 2. Sığıntı (Intrusive) Virüsler

Bu virüsler, kendilerinin var olan bir programın içine yamarlar. Amaçları ya programı bozmak, ya da programla birlikte varolmaktır. Eğer programı bozmak istiyorsa programın kullandığı adresleri ve göstergelewri değiştirmesi amacına ulaşmak için yeterli olur.

3. 1. 3. İşletim Sistemi Virüsleri

Bu virüsler işletim sisteminin bir parçasını kendi kodu ile değiştirirler ve işletim sistemi ile birlikte diskin az erişilen bir adresine yerleşirler.

3. 1. 4. Kaynak Kod Virüsleri

En az tanınan türleridir. Çünkü program geliştirici bir kimsenin kendisi, bu virüsü kaynak programın içine yerleştirmiştir. Belirli tarihlerde çalışmayan ya da kendini kilitleyen bilgisayarlarda bu tür bir virüs var demektir.

3. 2. Virüsün Bulaşması

PC (Personal Computer) lerde iki tür virüs bulunur. Bunlar boot sector virüsleri ve program virüsleridir.

3. 2. 1. Boot Sector Virüsleri (Önyükleme bölümü virüsleri)

Bu virüsler TSR (Terminate and Stay Resident) Sonlan ve yerleş yapısındaki virüslerdir. İşletim sisteminin boot sector (işletim sistemini çalıştıran bölüm) kendisi ile değiştirir ve orjinalini disketin bir başka yerine kopyalar. Bilgisayar bu disket ile boot edildiğinde sistem çalıştırıldığında Virüs programı kontrolü ele geçirir ve RAM da saklanır. Orjinal boot sector yükler sonra sistemi çalıştırır. Herşey olması gerektiği gibi olur. Bundan sonra sisteme takılan her diskete bir DOS servisi çağrısı ile bulaşırlar.

3. 2. 2. Program Virüsleri

Bu virüsler çoğunlukla COM ve EXE tipi çalıştırılan dosyalara bulaşırlar. Virüs taşıyan bir program bu virüsün bir kopyasını genellikle dosyanın sonuna taşır. Program çalıştırıldığında virüs bellekte kalır ve daha sonra çalışan diğer programlara bulaşarak onları etkiler. Bu virüsler kalıcı virüslerdir. Programın normalde ilk çalıştığı adresteki byte' ları kendi içinde bir yere kopyalar ve bu bölgelere de kendi kaynak kodlarının, giriş adresine girilmesini sağlayan bir komut girerler. Bu şekilde belleğe yüklenen her programa bulaşırlar.

Virüsler bir PC (Personal Computer) microbilgisayarın 3 bölgesine bulaşabilirler.

1- Disketin ve diskin sisteme özel olan boot sector

2- Sistem tarafından kullanılan sabit disklerin partitation table (ayırma tablosu) na

3- Sistem ve kullanıcı tarafından kullanılan dosyaların bulunduğu yerlere

3. 3. Virüs Programlarının Yapısı

Tipik bir virüs programı şu komutları içerir.

- Ev sahibi yazılımın işlemesini geçici olarak durdur.

- Bellekte, sana ev sahibi olacak yazılımları ara (COM ve EXE tipi dosyaları).

- Bulduysan bu komutların aynısını ona kopyala.

- Denetimi ev sahibi yazılıma geri döndür.

Bu işlerin tamamı en fazla bir saniye sürer. Virüs programları genellikle 200-300 Byte ile 5-10 KB arasında uzunluğu olan Assember dili ile yazılmış bilgisayar programlarıdır.

3. 4. Virüslerin Bulaşma Belirtileri

Eğer bilgisayarınızda aşağıda sıralanan davranışlar görülürse virüsün varlığından şüphelenilir.

- Beklenmedik anda ekranda acaip hata mesajları görünüyorsa,

- Bellek alanı azalmış görünüyorsa,

- Disk lambası normalden daha uzun süre yanık kalıyorsa,

- Dosyalar aniden yok oluyorsa,

- Sistem tarihi belirli bir tarihi gösteriyorsa,

- Sistem hoperlöründen değişik sesler çıkıyorsa,

- Ekrandaki karakterlerden aşağıya doğru düşme oluyorsa,

- Program işlemesinde yavaşlama gözleniyorsa,

- Bazı dosyaların uzunlukları değişmişse,

3. 5. Virüslerin Yayılması

Virüsler bir yazılımla birlikte gelmiş olabilir. çeşitli yollarla elde edilen programlara daha önce bulaşmış iselerbu şekilde başka sistemlere de bulaşırlar. Bilerek kullanılmak üzere ortaya bırakılan ve doğrudan çalıştırılan programlar vasıtasıyla bulaşırlar. Özellikle belleğe yerleşen virüsler DOS komutlarının kullanılması sırasında COMMAND. COM dosyasına kendisini kopyalar. Bundan sonra da bu dosyanın bulunduğu her ortamda diğer dosyalara kendi-

ni kopyalayarak yayılırlar.

Virüsler sabit diski bulunan bilgisayarlar üzerinde daha çabuk yayılırlar. Tek ya da çift disket sürücu bulunan bilgisayarlarda RAM' a yerleşen virüsler bilgisayar kapatılınca yok olacağından bu tip bilgisayarlarda virüs bulaşması daha az olur. Eğer virüs RAM' da iken başka disketlerde takılıp kullanılırsa bu takdirde bulaşma olur.

Bir V2P6 virüsü kendini kopyaladığında kaynak kodunu her kopyalamasında değiştirir. Aynı kodu yeniden üretme olasılığı ise üçyüz milyarda birdir.

3. 6. Virüslerin Zararları

Virüsler bilgisayar ve programları üzerinde şu zararları yapabilirler.

- Verileri silebilirler,
- Veriler üzerinde oynayarak metinlerin içine yazılım hataları eklerler,
- Bellek alanını azaltırlar,
- Sistemi yavaşlatırlar,
- Sistemi kilitlerler,

Virüsler bu zararları yaptıklarında bunların telafisi için bir zaman ve emek harcamak gerekir. Dolayısıyla daha çok zararı zaman kaybı biçiminde görülür.

Virüsler bu zararlarının yanında bir de yapamadığı işleri sıraladığımızda bu virüsler hakkında daha iyi bilgiye sahip oluruz. Virüslerin yapamayacakları işler;

- Bir virüs bir bilgisayar tipinden diğerine geçemez (örneğin MAC için tasarlanmış bir virüs IBM ve uyumlularını etkilemez),
- Bir virüs kendi kendine doğmaz,
- Her virüs saldırgan ve yıkıcı değildir,
- Bir virüs bilgisayara hastalıklı bir disket boot edilmedikçe ya da hastalıklı bir disket çalıştırılmadıkça bulaşmaz,
- Hastalıklı disketten okuma yapmakla virüs bulaşmaz,
- Yazma korumalı diskete virüs bulaşmaz,

- Veri dosyalarına eklenerek çoğalamazlar,

3. 7. Bazı Örnek Virüsler (Özellikleri, zararları, kurtulma yolları)

Microbilgisayarlar içinde MAC bilgisayarlarına ilk defa 1988 yılında SCORES virüsü, AMIGA bilgisayarlarına SCA virüsü, IBM bilgisayarlarının 350.000 terminaline CHRISTMAS virüsü bulaşmıştır. 1993 yılında yapılan bir ankete göre en popüler boot virüsü olarak SİGALİT virüsü, en popüler dosya virüsü de DIR2 seçilmiştir. 1994 yılında yapılan bir başka değerlendirmeye göre de en büyük 10 virüs aşağıdaki gibi sıralanmıştır. (*) (Computer World Monitör Gazetesi sayı 245).

Virüs Adı	Takma Adi
1- Form	Yok
2- Stoned, Standart	New Zealand
3- Stoned Michelangelo	Yok
4- V-Sign	Cansu ve Sigalit
5- Kampana 3700-boot	Anti-tel
6- Joshi-A	Telecom ve Telephonica
7- Stoned Emprie Monkey	Yok
8- Green-Caterpiller	1575, 1591 ve Find
9- Tequila	Yok
10- Jerusale 1808 Standart	1801, Israel ve Friday 15

En yaygın olarak IBM ve uyumlu bilgisayarlarda görülen virüsler 170x (1701-1704), Stoned-Marijuana, Key-Keypress, Dark Avenger, Pakistan-ı Brain Asher, Cansu, Mumcu, From virüsleridir.

Dark Avenger: EXE ve COM dosyalara yerleşir. Boot sector değişiklik yapar, programları bozar, dosyaları yok eder. RAM tarayacak bir virüs temizleme programı ile yok edilebilir.

Stoned-Marijuana: Disk partition table ve boot sector yerleşir. Command. Com'.u bozar. Kendini şifreleyebilir. Floppy disketten boot edildiğinde bulaşır. 7. sector 0 sector kopyalayarak yok edilebilir.

170x: Boot sector yerleşir, OVL (Overley) dosyalara bulaşır. Disk bölümleme tablosunu bozar. Virüs temizleme programları ile temizlenebilir.

Key Press: Klavyeyi etkileyerek kullanıcının yazı yazmasını engeller, tuşların görevini değiştirir. Virüs temizleme programları ile temizlenebilir.

Disk Killer: Ön yükleme sector bulaşır. Kendini harddisk ya da disketin boş blokları içine kopyalayarak çoğalır. Bulunduğu bölgeyi "bad" saha olarak FAT da işaretlendiğinden üzerine birşey yazdırmaz.

4. VİRÜSLERDEN KORUNMA VE KURTULMA

4. 1. Virüslerden Korunma

Virüslerden korunmak için bazı yol ve yöntemler vardır. Bunlar şöyle sıralayabiliriz;

- Ana kütüklerin, farklı isim ve ekli olarak kopyalarını almak,

- DOS' un ATTRIB komutunu kullanarak tüm dosyaları yalnız okunabilir yapmak,

Formatı: >ATTRIB *.* +R

- Bazı virüs temizleme programları temin etmek, bu tur programları bilgisayar açılışında aktif hale getirmek,

Anti-virüs adı verilen bu programlardan koruma ve kontrol amaçlı VSTOP, VSHILD, VSAFE programları ile tarama ve temizleme amaçlı SCAN-CLEAN, TNT, CPAV, F-PROT programları sayılabilir.

Virüs tarama programları üzerinde bir araştırma yapan InfoWord dergisi, araştırma sonuçlarına göre;

MCAfee Pro. scan	V. 20.01	% 73
F-Prot	V. 114a	% 92
Norton anti-virüs	V. 1. 0. 0	% 72
tool-kit	V. 4. 25	% 89
IBM Virscan	V. 1. 0	% 25

oranında güvenilir olduğunu yayınlamıştır.

Virüslerden korunma konusunda şu uyarılara da uymak gerekir;

- Bilgisayarınızı başkalarından alınan disketlerle açmayınız,

- Eğer sadece disket sürücülü bilgisayarınız varsa her bilgisayarın ayrı bir sistem disketi olması gerçeğini unutmayınız,

- Sabit diskli bilgisayarınız mecbur olmadıkça (virüs tarama aracı veya sistemin açılmaması durumu dışında) asla disket sürücüden açmayınız,

- Çevreden edineceğiniz programları diske kaydetmeden önce muhakkak tarayınız,

- Formatlama anında disketinize anlamlı isimler veriniz ve bunları ara sıra kontrol ediniz,

- Disketlerin yazma korumalı kapağını kapalı tutnuz,

- Disketinizin izinsiz olarak başkaları tarafından kullanılmasına engel olunuz,

- Çok sistemli ortamlarda sadece veri dosyalarının aktarılmasına izin veriniz,

- Eğer bir iletişim ağında çalışyorsanız, kaynağını bilmediğiniz yazılımları File Server (ortak dosya hizmet) rehberine almayınız,

- İletişim ağının dosya hizmet birimi "node" unda sistem yöneticisinden başkasının çalışmasına izin vermeyiniz,

- Mainframe bağlantıları için emülatör yazılım kullanıyorsanız bunları ayrı bir alt dizine alın ve buraya başka yazılım koymayınız,

- Sistemdeki olası değişiklikleri gözleyiniz.

1991 yılında İngiltere' de bir virüs yazarı, 20 yıl hapse mahkum edilmiştir. İngiliz polisi bilgisayar suçları ile ilgilenen ayrı bir birim kurmuştur. Amerika' da ise polis bilgisayarına 2.000.000 $ lık zarar veren bir kişi hapse girmiş ve ömür boyu bilgisayar klavyesine dokunmama cezası almıştır.

4. 2. Virüs Temizleme Yolları

Virüs bulaşmış bir bilgisayarı, bu zararlı yazılımdan temizlemek için önce virüsün varlığından emin olmak gerekir. Ayrıca virüslü olduğu tahmin edilen programlar kullanılmamalıdır. Muhakkak temiz bir sistem disketi hazırlanmalı ve korumalı hale getirilmelidir. Güvenilir yerden virüs tarama ve temizleme programları edinilmelidir. Eğer bilgisayarınızda virüs olduğundan şüpheleniyorsanız aşağıdaki yolu izleyiniz;

1- Bilgisayarınızı ana güç düğmesinden kapatınız.

2- Yeni ye yazma korumalı bir sistem disketi ile bilgisayarınızı A sürücüsünden açınız.

3- Virüs tarama programı ile Memory' i ve diski tarayınız.

4- Virüs temizleme programı ile tespit ettiğiniz virüsleri, formatına uygun yazarak temizleyiniz.

5- Şüphelendiğiniz diğer disketleri ve yedek dosyaları da tarama yapınız.

6- Tarama ve temizleme işleminden emin olmak için ilk adımdan itibaren

işlemleri tekrarlayınız.

7- Eğer problemden kurtulamadınız ise bir ustaya başvurunuz.

4. 3. Virüs Tarama ve Temizleme Programları

CPAV (Central Point Anti-Virüs)

Menü arabirimi yada komut satırından çalışabilir. Bilinen virüsler için sistem belleğini ve kütükleri hızlıca tarar ve aynı zamanda temizleme yapar. Geri plan virüs koruması için iki tane TSR (VSafe ve VWatch) içerir. Kolay kullanılır.

Pro-Scan (Scan ve Clean)

Virüs tarama ve temizleme için iyi bir programdır. Ancak bu işleri yaparken virüs bulaşmasını önleyecek bir imkan sunmuyor.

F-prot

Hem tarama hem temizleme yapan ve birçok seçenekle çalışan bir programdır. Tek disket sürücülü ve harddiski olmayan bilgisayarlarda kullanılamıyor.

toolkit

Virüsleri kolayca yakalayıp temizleyemiyor.

Norton Anti-Virüs

Program menüleri basit ve temel işlevleri yerine getirmek için herşeyi sağlar. Ancak diğer anti-virüs programların da bulunan kütükleri inceleyen, üzerine yazan, belleği kendiliğinden kontrol eden yardımcı araçları yoktur.

5. SONUÇ

Yukarıda birçok yönüyle anlatılan virüsler özellikle yeni kullanıcıları çok güç durumda bırakmaktadırlar. Ancak öyle anlaşılıyor ki virüsler bir yönüyle de ticari amaçlar taşımaktadırlar. Bu sayede, geliştirilen antivirüş programları piyasada talep bulmakta ve önemli bir gelir kaynağı olmaktadır. Sonuç ne olursa olsun, bilgisayar virüsleri kullanıcıları usandıran ve teknolojiden soğutan, bilim ahlakına aykırı geliştirilmiş yapılardır diyebiliriz. Ancak şunu da söyleyebiliriz ki bu virüsler sanıldığı kadar korkulacak bir olgu da değildirler. Öncelikle tedbirli olmak gerekmektedir. Hele hele yeni kullanıcıların başkalarının disketlerinden dosya transfer etmeleri durumlarında daha bir dikkatli davranmaları ve mutlaka kontrol yapmaları gerekir. Eğer virüs bulaşmış ise bilinçli bir şekilde hareket edildiğinde bunlardan kolayca

korunabilirler.

KAYNAKÇA

EREN, Şaban, KOLTUKSUZ,Ahmet; "Bilgisayar Virüsleri". Bilgisayar Dergisi sayı 94-95-96-97

ERSOY, Kerem; Virüslere Bulaşmamak". PC World Dergisi sayı 2: sayfa 76-78

KÜÇÜKARAS, Hülya ve v. d. "Virüsler". PC World Dergisi sayı 6: sayfa 40-67

Computer World Monitör Gazetesi sayı 245