

## BÖLÜM 4: BİLGİSAYAR VİRÜSLERİ



### A. VİRÜSÜN TANIMI

Virüs, kullanıcının isteği dışında bilgisayarın belleğine yerleşen, programlara ve dosyalara kendini ekleyen, virüs programını hazırlayan kişinin isteğine bağlı olarak, yerleştiği programların yapısını değiştiren ve kendisini çoğaltabilen programdır.

Virüs programlarının büyüklüğü bir kaç bayt (byte) olmasına karşın bilgisayara verdiği zararlar büyüktür.

Virüsler EXE, COM, SYS, DLL, LIB, DOC ve benzeri gibi uzantılı dosyalara bulaşabilirler. Bunlar küçük programlar olduğundan aktif hâle gelebilmeleri için virüs taşıyan bir yazılımın çalıştırılması ya da virüslü sistem dosyalarıyla bilgisayarın açılmış olması gerekir.

Disketteki bir ya da daha çok dosya virüslüyse disket, disket sürücüyü takıldığında virüs yazılımı önce RAM belleğe, oradan da sabit diske bulaşır.

Sabit diskte virüs programı varsa diskete kayıt yapıldığı zaman virüsler diskete de bulaşır. Sabit diskte bulunan virüs programlarının diskete geçmesini önlemek için disketin koruması (protect) kapatılır.

İnternet sayfalarından indirilen dosyalarda virüs varsa bunlar sabit diske bulaşır. Ayrıca e-posta yoluyla gönderilen dosyaların açılmasıyla sisteme virüs bulaşması mümkündür.

Virüsler, bilgisayar ve programcılık bilgisi olan kişiler tarafından yazılmaktadır. Bunların yazılmasının amacı bilgisayarlara ve kullanıcılara zarar vermektir.

Virüsler çoğunlukla üç alanı kullanırlar. Bunlar:

**I.** Sabit diskin bölümleri,

**II.** Diskin BOOT sektörü,

**III.** COM ve EXE uzantılı sistem ve kullanıcı dosyalarıdır.

### B. VİRÜS ÇEŞİTLERİ

Bilgisayar virüslerinin verebileceği zararlar çok çeşitlidir. Bazıları yazılımları çalışmaz hâle getirir. Bazıları belgeleri bozar, bazıları ise donanım parçalarına (BIOS yongası, sabit disk) zarar verir.

Virüsleri genel olarak şu gruplar altında toplayabiliriz:

#### 1. Boot sektör (memory resident) virüsleri

*Boot* sektör virüs programları sistem alanlarına bulaşrlar. Bu tür virüslerin bulaşma şeklini anlayabilmek için işletim sisteminin çalışma ilkesini bilmek gerekir.

Bilgisayarın içinde test programları, ekran, yazıcı, sürücü, klavye denetim programları gibi sistemle ilgili temel bilgilerin bulunduğu BIOS adı verilen bölüm vardır. BIOS, ROM bellek üzerinde yer alır ve bilgisayar açıldığında sistemin işlevlerini yerine getirip getirmediğini denetler.

Sistem doğru çalışıyorsa, sabit disk belirlenir. Bu işlemden sonra sabit diskin ilk sektörü olan *Master Boot Record (MBR)* yüklenir ve sistemin kontrolü bu yükleyici programa aktarılır. Yükleyici program, diskin üzerinde bulunan *boot* sektörü okur. *Boot* sektörde ya da MBR'de virüs varsa, sistemin her açılışında virüs, bilgisayara takılan bütün disketlerin *boot* sektörüne kendini kopyalar. Bulaşan virüsler, *boot* sektörde yer alan bilgileri diskte herhangi bir alana yazar ve *bad* (kötü, bozuk) sektör olarak işaretler. Çünkü DOS, kötü alanlara bilgi yazamaz.

Yükleyici program, disk ya da diskette ilk okunan IO.SYS ve MSDOS.SYS dosyalarını araştırır. Bulursa ilk önce IO.SYS dosyasını belleğe yükler ve sistemin kontrolünü bu dosyaya aktarır. Bu dosya belleğe MSDOS.SYS dosyasını yükleyerek sistemin normal olarak çalışmasını sağlar.

#### 2. Program (COM ve EXE) virüsleri

Bu tür virüsler çalışılabilir programlara (COM, EXE) bulaşrlar. Program virüsleri genellikle kendilerini programın sonuna eklerler.

Virüs içeren program çalıştırıldığında virüs belleğe yerleşmiş olur ve her çalışan programa bulaşır. Bulaşma yöntemi bu şekilde olan virüslere **yerleşik virüs** denir.

Virüs, programın ilk çalışacağı adresteki bilgileri kendine kopyalar ve bu alana kendi kodlarını yerleştirir. Böylece programın kontrolü virüs programına geçmiş olur. Virüs, kendisini DOS sistem dosyalarına ekledikten sonra, programın kodlarını tekrar yazar ve kontrolü programa devreder.

DOS işletim sistemine yerleşen virüs, bilgisayarın her açılışında belleğe yüklenir ve bellekte çalışan tüm yazılımlara bulaşır. Bulaşma yöntemi bu şekilde olan virüslere direkt hareket virüsleri adı verilir. Bazı virüs programları bu iki yöntemi de kullanabilir.

### 3. Diğer virüsler

Hem *boot sektör (memory resident)* hem de program (çalışabilir dosya) virüslerinin özelliklerini bir arada taşıyan virüsler de vardır. Bu tür virüsler diğerlerine göre daha tehlikelidir. Çünkü bilgisayarın açılışından itibaren aktif (etkin) duruma geçer ve her çalışabilir dosyaya bulaşarak kısa sürede yayılırlar. Bu virüsler bilgisayara kayıtlı olan her tür program ve veri dosyasına bulaşarak bu dosyaların içeriğine zarar verebilirler. Kendi kendilerine çoğalma yeteneğine sahiptirler. Temizlenmeleri de diğer virüslere göre daha güçtür. Temizlenme sırasında bazı dosya ve verilerin zarar görmesine de neden olabilirler.

## C. VİRÜSLERE KARŞI YAPILACAK İŞLEMLER

Bilgisayarda virüs olup olmadığını öğrenmenin en kesin yolu, iyi bir virüs tarama yazılımı kullanmaktır.

Antivirüs programları, virüsten korunmak için tarama ve temizleme işlemlerini gerçekleştiren paket yazılımlardır. Bilgisayarla ilgili olan herkesin yaygın ve güvenilir bir antivirüs yazılımını kullanabilmesi gerekir.

### 1. Virüslerle ilgili olarak bilinmesi gereken önemli hususlar

- Virüs kendiliğinden oluşmaz, bir programcı tarafından yazılması gerekir.
- Zararsız virüsler de vardır.
- Virüs bulaşmış bir disket ya da program bilgisayarda çalıştırılmadığı sürece virüs yayılmaz.
- Koruma yuvası kapalı disketlere virüs bulaşması mümkün değildir.

### 2. Virüs programının kodlarının kısımları

- Virüsün çoğalmasını sağlayan kopya kısmı,
- Virüsü temizleme programlarına karşı gizleme kısmı,
- Virüsün zarar verme komutlarının yer aldığı bomba kısmıdır.

### 3. Virüslerden korunma yolları

- Bilgisayara her disket, CD-ROM, sabit disk ya da DVD-ROM takılmamalıdır.
- Güvenilir olduğundan emin olunmayan veri depolama birimleri kullanılmamalı ya da antivirüs programlarıyla virüs taraması yapıldıktan sonra kullanılmalıdır.
- Tanınmayan kişilerden gelen e-postalara ekli dosyalar açılmadan silinmelidir.
- İnternetteki her siteden dosya indirilmemelidir.
- Virüsten kuşkulandığında bilgisayar hemen kapatılmalıdır. Çünkü, virüs bulaştıktan sonra makinenin her açılıp kapatılışında daha da ilerlemektedir. (Örneğin Çernobil virüsü böyledir.)
- Önemli program ve dosyaların disket, CD-ROM, ikinci sabit disk gibi ortamlara yedeği alınmalıdır.

### 4. Antivirüs programlarının çalışma şekli açısından sınıflandırılması

Antivirüs yazılımlarının çalışma şekli;

- Belleğe kalıcı olarak yerleşen
- Belleğe yerleşmeyen olmak üzere iki şekildedir.

Belleğe kalıcı olarak yerleşen antivirüs programları bilgisayarın ilk açılışında genellikle AUTOEXEC.BAT dosyası yardımıyla çalıştırılır. Bilgisayar kapatılıncaya ya da program çalışması iptal edilinceye kadar bellekte çalışırlar. Bilgisayarın çalışması anında herhangi bir virüse karşılaştıklarında kullanıcıyı sesli ya da yazılı olarak uyarırlar.

Piyasada NORTON ANTIVIRUS, PANDA, F-PROT, SCAN, CLEAN, TOOLKIT, CPAV, MSAV, CRAZY ve benzeri gibi değişik isimlerde antivirüs programları bulunmaktadır.

Her virüsün belirli bir kodu vardır. Bu koda **virüs imzası** adı verilir. Antivirüs programları her dosyada virüs kodu olup olmadığına bakar ve bulursa temizler.

Antivirüs programlarının bazıları aşılama (*immunize, infect*) işlemi yaparak çalışır. Bu işlemde disk ya da diskette bulunan tüm dosyaların uzunlukları, oluşturulan yeni bir dosyaya kaydedilir. Antivirüs programı, kaydettiği uzunluklarda bir değişiklik olup olmadığını kontrol eder. Değişiklik varsa kullanıcıyı uyarır.

Antivirüs programlarının en önemli sakıncası yeni virüs kodunu tanınamaları, yani kütüphanelerinde (library) virüse ait kodların yer almamasıdır.

Bazen kullanılan antivirüs yazılımı bilgisayarda virüs olduğu hâlde tanımayabilir ve temizleyemez. Bundan dolayı farklı virüs temizleme programları kullanmakta yarar vardır.

Bir bilgisayarda virüs olduğunu gösteren belirtilerden bazıları şunlardır:

- I. Yazılımın çalışma süresi normalden uzun sürer.
- II. Beklenmedik hata mesajları ekranda görüntülenir.
- III. RAM bellek kapasitesi normalden daha az görülür.
- IV. Ekranda değişik (anlamsız) karakterler görüntülenir.
- V. Normalde çalışan programlar çalışmaz.
- VI. Çalışabilir program dosyalarının uzunlukları, tarihi ya da zamanı değişir.
- VII. Programlar çalıştığı anda bilgisayar ekranı uzun süre hareketsiz kalır.
- VIII. Bilgisayar işleme açılmaz.

Her gün yeni virüs programları üretildiğinden, antivirüs programlarının sürekli olarak yeni sürümleri çıkarılmaktadır.

Bir antivirüs programı yalnızca üretildiği tarihten önce varolan virüsleri temizleyecek bilgilere sahiptir. Antivirüs programı yazıldıktan sonra çıkan virüsleri temizleyebilmek için de, sürekli yeni sürüm programları takip ederek bilgisayara yüklemek gerekir.

Kullanılmak istenilen antivirüs yazılımı bilgisayar firmalarından ya da internet aracılığıyla da satın alınabilir.

Eğer deneme (*trial*) sürümünü alarak bir süre kullanmak isterseniz, bunlara ücret ödemeniz gerekmez. Çünkü bu programlar ücretsizdir. Periyodik olarak internetdeki indirme (*download*) sitelerinden sürekli olarak yeni sürüm antivirüs programları yüklenip tarama yapılmalıdır. Ancak *trial* (deneme) versiyonu olan virüs programlarının bilgisayarı tam olarak koruduğu söylenemez.

Bilgisayarın her açılışında RAM belleği kontrol ederek virüsleri bulması ve bizi uyarması için antivirüs programı kendisini başlangıca atar ve bilgisayar her açıldığında antivirüs yazılımı otomatik olarak kendisini çalıştırdıktan sonra aktif hâle gelip RAM belleği test eder. Virüslü bir disket ya da CD-ROM çalıştırıldığında ise uyarı verir. Böylece virüs uyarısından (*alert*) sonra kullanıcı da virüsü temizleyebilir ya da virüslü dosyayı açmaktan vazgeçebilir.

Virüslerle ilgili olarak sık olarak karşımıza çıkan terimlerin anlamları şunlardır:

- |  |   |
|--|---|
| <b>Warning:</b> Uyarı.                     | <b>Infected:</b> Bulaşmış.                            |
| <b>Checking:</b> Kontrol.                  | <b>Repair:</b> Tamir.                                 |
| <b>Remove:</b> Virüs silme.                | <b>Find:</b> Bul.                                     |
| <b>Clean:</b> Virüs temizleme.             | <b>Exit, quit:</b> Çıkış.                             |
| <b>Scan:</b> Tarama.                       | <b>Wait:</b> Beklemek.                                |
| <b>No viruses found:</b> Virüs bulunamadı. | <b>2 files appear to have virus:</b> 2 dosya virüslü. |

## Ç. YAYGIN BİR ANTI-VİRÜS PROGRAMININ KULLANIMI

### 1. Norton antivirüs programı

Virüslere karşı oldukça etkili ve yaygın olarak kullanılan bir antivirüs programı olan Norton, geniş tarama seçenekleri, etkili temizleme ve koruma yapabilmesi, fiyatının emsallerine göre ucuz oluşu, güncelleme işlemlerinin internet üzerinden yapılabilmesi tercih edilmesini sağlayan özellikleri olarak göze çarpmaktadır.



Şekil 1: Norton antivirüs programının kısa yol simgesi



Şekil 2: Norton antivirüs programının başlangıç menüsü (arayüzü)

Norton antivirüs programının *System Status* (sistem durumu) iletişim kutusunda ilk göze çarpan *Protect* (otomatik koruma) durumudur. *Auto Protect*'in yanındaki buton, programı *Enable* (aktif) ya da *Disable* (pasif) durumuna getirmenizi sağlayacaktır (şekil 2).

Antivirüs programı bellekte *resident* (saklı) olarak kalmalıdır. Böylece farkına

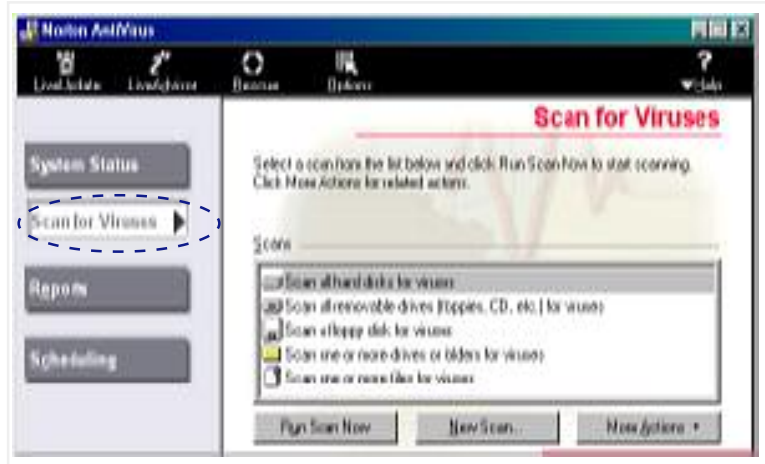
varmadan tanımlı bir virüsün saldırısının olması hâlinde ya da virüs davranışı gösteren bir uygulamanın etkisinin görülmesi hâlinde kullanıcı uyarılarak duruma müdahale edilir.

Şekil 3'te görülen *Scan for Viruses* (virüs tarama) iletişim kutusuna geçildiğinde beş ayrı tarama seçeneği görülür. Ayrıca üç ayrı komut düğmesine bağlı işlevler gerçekleştirilebilir. Bu düğmelerin işlevleri şunlardır:

**Run Scan Now (taramayı şimdi çalıştır):** Belirlenen taramayı başlatır.

**New Scan (yeni tarama):** Ekrandaki standart tarama biçimleri dışında kendi belirleyeceğimiz tarama grubunu oluşturmamızı sağlar. *New Scan* düğmesine basıldığında yol gösterici (sihirbaz programı) çalışmaya başlar.

İlk penceredeki *İleri* düğmesine basılırsa ekranda şekil 4'te verilen iletişim kutusu görüntülenir.



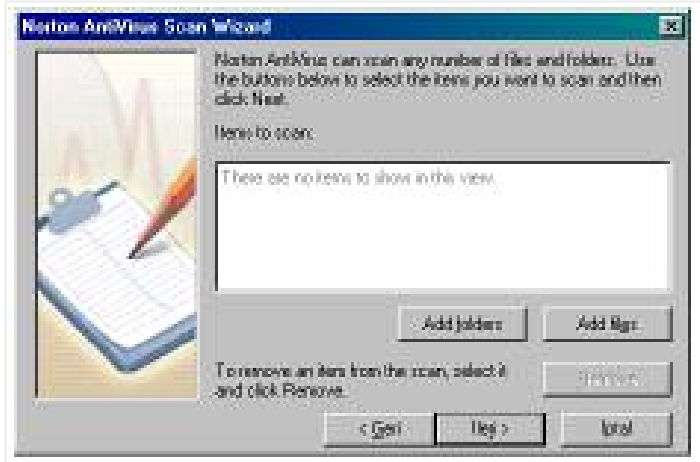
Şekil 3: *Scan for Viruses* butonuna basıldığında iletişim penceresinde görülen seçenekler

Şekil 4'teki iletişim kutusunda klâsör ya da dosya belirlemeyi sağlayacak iki buton (*Add folders ve Add files*) vardır.

*Add Folders* (klâsörler ekle) düğmesine basılırsa açılan iletişim kutusundan taranacak sürücü ve klâsörler işaretlenip *Add* (ekle) düğmesine tıklanır (şekil 5).

Tanımlanan yeni tarama grubuna bir isim (örneğin *tarama1*) verilir ve *Finish* (son) düğmesini tıklanır.

Tanımlanan taramanın hemen başlatılması isteniyorsa *Yes* (evet) düğmesi, istenmiyorsa *No* (hayır) düğmesine tıklanır.



Şekil 4: *New Scan* düğmesine basıldığında açılan iletişim penceresi



Şekil 5: *Add Folders* düğmesine basıldığında açılan *Scan Folders* adlı iletişim kutusu



Şekil 6: Norton antivirüs programının *Scan for Viruses/ More Actions* adlı düğmenin alt komutları

*Norton antivirüs* programının şekil 6'da görülen *Scan for Viruses* menüsündeki *More Actions* (diğer işler) butonu altındaki menüde bulunan komutların görevleri şunlardır:

**Edit Scan:** Tanımlanan tarama içerisine yeni klâsör ya da dosyalar eklenmesini sağlar.

**Delete Scan:** Tanımlanan tarama işlerini silmeyi sağlar.

**Rename Scan:** Tanımlanan tarama işlerinin adlarını değiştirmeyi sağlar.

**View:** Tarama biçimlerinden hangilerinin listeleneceğini belirler. *All* (tümü), *Build in Scan* (kurulu taramalar), *Custom Scans* (düzenlenmiş taramalar) olmak üzere üç ayrı biçim sunulur.

**Scan Properties (tarama özellikleri):** Seçilen tarama şeklinin tanımlı tarama ayarlarını gösterir.

Şekil 3'te görülen *Scan for Viruses* menüsündeki hazır tarama biçimleri şunlardır:

**Scan All Hard Disks For Viruses (tüm sabit disklerdeki virüsleri tara):** Bilgisayarın tüm sabit diskleri virüs taramasından geçirilir.

**Scan All Removable Drives (Floppies, CD, Etc.) For Viruses:** Çıkarılabilir olan tüm disk, disket ve CD-ROM sürücülerinde virüs taraması yapar.

**Scan A Floppy Disk For Viruses:** Yalnızca disket sürücüsündeki diskette virüs taraması yapar.

**Scan One or More Drives or Folders For Viruses:** Belirleyeceğiniz sürücü ya da sürücülerle, klâsörler üzerinde tarama yapar. Seçim ekranı sürücülerini ve ağ komşularını da içerir.

**Scan One or More Files For Viruses:** Bu komuta fareyle çift tıkladığı zaman seçilen dosya ya da dosyalar üzerinde tarama yapar. Şekil 7'deki iletişim kutusunda yalnızca dosya ya da dosyalar seçilebilir.

Norton antivirüs programı bilgisayarda virüs taraması yaparken şekil 8'de verilen iletişim kutusu ekranda görüntülenir.

Şekil 8'deki iletişim kutusunda bulunan sözcüklerin anlamları şunlardır:

**Scanned:** Taranan dosya sayısı,

**Infected:** Virüslü dosya ya da bölüm sayısı,

**Repaired:** Temizlenen dosya sayısı,

**Deleted:** Silinen dosya sayısı,

**Quarantined:** Karantina klâsörüne taşınan dosya sayısıdır.

*Quarantine* (karantina) sözcüğünün görevini şöyle açıklayabiliriz: Tanımlanan ancak güvenli şekilde silinemeyen ya da temizlenemeyen virüslerin bulaştığı dosyaların uzantıları değiştirilerek ayrı bir klâsörde muhafaza edilirler. Böylece bu dosyalar el altından kaldırılmış olur. İleride bu virüsleri güvenli bir şekilde temizleyecek program hazırlandığında temizlenip tekrar kullanılması sağlanmış olur.

Norton antivirüs programının *Reports* (raporlar) menüsü (şekil 9) üç komuttan oluşmaktadır. Şimdi bunların özelliklerini inceleyelim.

a.  View and manage the items in Quarantine.

Karantinaya alınmış olan virüslü dosyalar ve yapısal nitelikleri hakkında rapor sunma dışında pencere üzerindeki işlem butonlarıyla ya da *Action* menüsüyle:



Şekil 7: *Scan One or More Files For Viruses* adlı seçeneğe tıkladığımızda açılan iletişim kutusu



Şekil 8: Norton antivirüs programı çalışırken ekranda görülen açıklamalar penceresi



Şekil 9: Norton antivirüs programının başlangıç menüsündeki Reports düğmesine bastığımızda ekranda görülen iletişim kutusu

- I. Yeni bir dosyanın karantinaya eklenmesi sağlanabilir.
- II. Seçilen bir öğenin özellikleri görülebilir.
- III. Seçili dosya onarılabilir. Bu durumda dosyaya bulaşan virüsü temizleyen algoritmanın programa eklenmiş olması gereklidir.
- IV. Seçili dosya, alınmış olduğu konuma geri gönderilebilir. (Bu işlem dosyaya bulaşan virüs başarıyla temizlendikten sonra yapılmalıdır.)
- V. Seçili dosya diskten silinebilir.
- VI. Dosya internet aracılığıyla SARC (*Symantec Antivirus Research Center*)'a gönderilebilir.
- VII. Virüs veri tabanı dosyası güncellenebilir. Bu güncelleme işlemi bilgisayarda internet erişimi varsa mümkün olur.

b.  View the log of Norton AntiVirus activities.

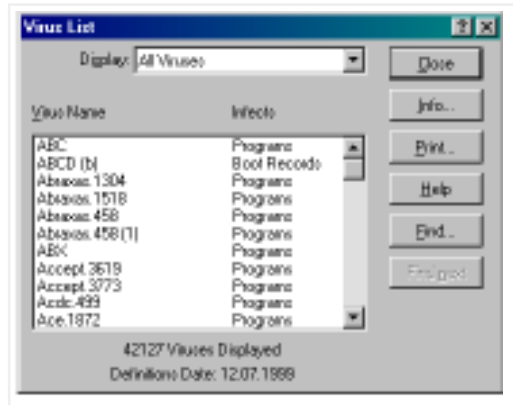
Faaliyet raporu kısmında yapılan tarama işlemleri hakkında bilgiler yer alır. Bu raporla ne zaman hangi bölümler üzerinde tarama yapıldığı ve sonuçları hakkında fikir edinmek mümkün olur.

*Print* (yazdır) düğmesiyle rapor yazıcıya gönderilebilir. *Clear* (temizle) düğmesiyle rapor dosyası boşaltılabilir.

*Filter* düğmesiyle rapor bilgisinin süzme esasları belirlenebilir.

c.  View the list of viruses that Norton AntiVirus is protecting you against.

Bu kısımda Norton antivirüs yazılımının sisteminizi hangi virüslere karşı koruyabildiği gösterilmektedir. Şekil 10'da verilen pencerede tanımlanmış virüslere ait liste görülmektedir.



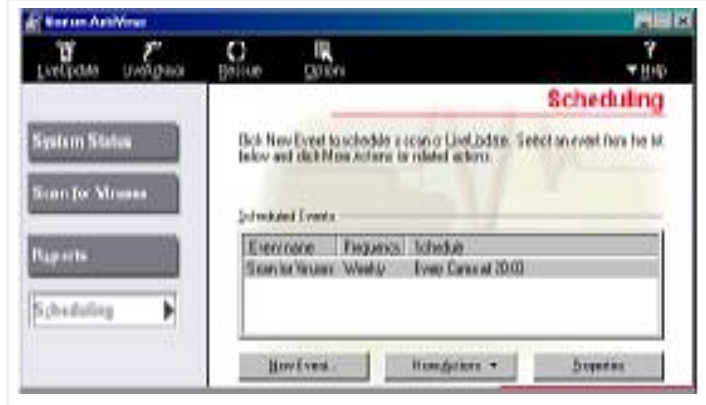
Şekil 10: View the list of viruses that Norton AntiVirus is protecting you against adlı komut çalıştırıldığında ekranda görülen virüs listesi

Şekil 10'da verilen pencerede,

- I. *Display* bölümüyle listelenecek virüsler kategorilere ayrılabilir.

- II. *Find* düğmesiyle listeden herhangi bir virüsü arama işlemi yapılabilir.
- III. *Print* düğmesiyle liste yazıcıya gönderilebilir.
- IV. *Info* düğmesiyle virüsler hakkında daha ayrıntılı bilgi içeren yeni bir pencereye geçilebilir.

Norton Antivirüs yazılımının başlangıç menüsündeki *Scheduling* (plânlama) düğmesine basıldığında şekil 11'de verilen iletişim kutusu ekranda görüntülenir. *Schedule* bölümüyle ileri tarihler için belirlenen tarama biçimleri durum raporu alınabilir. Bunun dışında *New Event* (yeni eylem) seçeneğiyle bu plânların arasına yeni bir plân eklenebilir. Bu işlemde bir sihirbaz programı yol gösterir. Yapılacak plânlama, virüs tarama işlemi, virüs veri tabanının güncellenmesi, bir başka programı başlatma ya da herhangi bir mesajın görünülmesi için olabilir.



Şekil 11: Norton antivirüs yazılımının başlangıç menüsündeki *Scheduling* düğmesine basıldığında ekranda görülen iletişim kutusu

#### D. TRUVA ATLARI (TROJAN HORSE)

Truva atları, virüslerden oldukça farklı bir yapıya sahiptir. Asla başka programlara bulaşmazlar. Belli olaylara bağlı olarak tetiklenme (çalışma) özellikleri vardır. Kendilerini kopyalayamadıkları için bazı programların içine bilinçli olarak yerleştirilirler. Trojan kodu, trojanın içine gizlendiği programın yazarı tarafından yazılmış olabileceği gibi sonradan da programa eklenmiş olabilir.

Truva atı programı bir bilgisayara yerleştiği zaman bu makinedeki şifre ve dosyaları kötü amaçlı kullanıcıya bildirirler. Ayrıca kötü amaçlı kişi (*hacker*) truva atı programıyla kontrol altına aldığı bilgisayara zarar verebilir.

Truva atlarından korunmak için şunlar yapılmalıdır:

- I. Güvenilir olmayan sitelerden program indirilmemelidir.
- II. Tanınmayan kişilerin elektronik posta yoluyla gönderdiği **EXE, COM, INI** uzantılı dosyalar açılmamalıdır.
- III. Bilgisayarda bulunan önemli verilerin yedeği alınmalıdır.
- IV. İnternet erişimi, elektronik posta, kredi kartı ve benzeri gibi şifreler bilgisayarda kayıtlı olarak tutulmamalıdır.
- V. Sohbet programları (MIRC, ICQ ve benzeri) ile gönderilen dosyalar açılmamalıdır.
- VI. Bilgisayara, truva atı belirleyen yazılımlar (Jammer, Cleaner ve benzeri) kurulmalıdır.

#### Sorular

1. Virüs nedir? Açıklayınız.
2. Virüslerden korunma yollarını yazınız.
3. Virüsler ne gibi zararlar verirler? Açıklayınız.
4. Truva atı nedir? Açıklayınız.