O. VİRÜSLER

a) VİRÜS NEDİR?

Bildiğiniz gibi virüsler gerçekte insanlarda çok çeşitli hastalıklara sebep olan mikro-organizmalardır. Bilgisayar dünyasında da buna benzer bir durum mevcuttur, ancak burada söz konusu olan "virüsler" canlı varlıklar değil, bilgisay ara zarar verm ek amacıyla hazırlanmış küçük programlardır.

Bir "virüsün" bilgisayar üzerindeki etkileri hemen hemen gerçek virüslerin insanlar üzerindeki etkilerine benzer. Bilgisayar normal çalışma düzenini sürdüremez, verilen komutları uygulayamaz bir hale gelir. Virüsler kendilerini benzer programlar ve veri dosyalan arasında bulaştırarak yayılırlar, genellikle bir virüsten etkilenmiş olan herhangi bir uygulama çalıştırıldığında o virüs de çalıştırılmış olur. Harekete geçen virüs çoğunlukla esas işi olan sisteme zarar verme faaliyetini sürdürürken, bir yandan da olasılıkları değerlendirip kendini başka programların içine kopyalar. Böylece virüs gittikçe çoğalır ve her defasında daha fazla uygulamayı etkiler, daha çok dosyaya bulaşır.

Günümüzde ortaya çıkan virüslerin çoğu kendini gizleyecek ve sistemdeki basit savunmaları aşabilecek özelliklere sahiptirler. Internet gibi geniş kitlelere hitap eden iletişim yollarını kullanarak hızlı bir biçimde çok sayıda bilgisayar sistemini etkilemeyi başarabilirler, özellikle de hiçbir savunma önlemi alınmamışsa çok etkili olabilirler. Bilgisayar virüsleri hakkında unutulmaması gereken bir diğer önemli özellik de, etkiledikleri sistemlerin onlara karşı herhangi bir bağışıklık kazanmadığıdır. Yani eğer bir sistem belli bir virüsten etkilenmiş ancak sonradan arındırılmışsa, bu o sistemin ileride tekrar aynı virüsten etkilenmeyeceği anlamına gelmez, o yüzden güvenlik önlemlerinin alınması ihmal edilmemelidir.

b) VİRÜSLER NEREDEN GELİR?

Dünya üzerinde bilgisayar sistemlerini etkileyen onbinlerce farklı virüs tipi bulunmaktadır, ayrıca her geçen gün bunlara yenileri eklenmektedir. Peki bu virüslerin kaynağı nedir, nereden gelmektedirler? Virüslerin aslında küçük bilgisayar programları olduğunu söylemiştik, yani onları yaratanlar bilgisayar programcılarıdır. Bir insanın oturup virüs yazmasının arkasında çok farklı sebepler bulunabilir. Mesela genç bir programcı ne denli yetenekli olduğunu göstermek için oldukça gelişmiş bir virüs yazabilir, fakat maalesef bu kişiler genellikle yetenekli oldukları oranda sorumluluk sahibi değildirler, bu yüzden yaptıkları işin diğer insanlara ne denli çok zarar verebileceğini genellikle göz ardı ederler.

Bazıları ise virüsleri bir intikam aracı olarak kullanmayı seçerler. Bu kişiler genellikle sorunlu insanlardır, mesela eski çalıştıkları firmayı ya da belki tüm toplumu başlarına gelenlerden ötürü sorumlu tutar ve intikam almak için virüslerden faydalanmaya kalkarlar. Ancak başlangıçtaki amaç ne olursa olsun, bir kez yayılmaya başlayan bir virüsü kontrol etmenin imkanı pek yoktur, bu yüzden genellikle dünyanın dört bir yanındaki insanlar aynı şekilde etkilenebilirler.

Bazen virüsleri gerçekte anti-virüs yazılımları hazırlayan firmaların yarattığı ve yaydığı söylenir. Ancak bu pek olası değildir, çünkü bu tür yazılımlar üreten firmalar genellikle böyle yasadışı bir iş yapmaya cesaret edemeyecek kadar göz önündedirler. Ayrıca hemen hepsi kişisel kullanıcılara yönelik anti-virüs yazılımlarını Shareware (Kısıtlı kullanım) ya da Freeware (Ücretsiz kullanım) olarak piyasaya sürmekte, genellikle bundan pek fazla para kazanmamaktadırlar. Bu gibi firmaların esas gelir kaynağını büyük kuruluşlara sundukları yazılımsal güvenlik hizmetleri oluşturmaktadır, o yüzden bu "komplo teorisi" pek akılcı değildir.

c) VİRÜS TÜRLERİ

Daha önce de belirttiğimiz gibi virüsler küçük programlardır ve girdikleri sisteme yapılarına uygun bir biçimde zarar vermeye çalışırlar. Genel olarak bir virüsün ne yaptığı ve nasıl bulaştığı bilinirse ona göre önlem alınabilir. Virüsler çoğunlukla kendilerini çalıştırılabilen bir programın ya da bir veri dosyasının içine gizlerler, bu yüzden özel yazılımlar kullanılmadan bulunmaları ve imha edilmeleri pek mümkün değildir. Bunun dışında nasıl saldırıya geçtikleri, ne gibi hasarlar verdikleri ya da kendilerini ne tür dosyaların içine gizlemeyi tercih ettiklerini basit bir sınışandırmayla anlatmak pek mümkün değildir, çünkü sayıları ve çeşitleri gerçekten oldukça fazladır.

```
                What does F-PROT detect ?

Using the current virus signatures (SIGN.DEF and MACRO.DEF),
this program identifies the following:

     44230 different DOS/Windows viruses
     8283 different Word/Excel viruses and Trojans
     245 Java viruses and Trojans
     2903 .BAT viruses
     1516 IRC viruses
     5874 Script viruses (mostly JavaScript and VBScript)

The program also detects at least 55735 different destructive
programs, many of which have been distributed as Trojans in
the past.  Finally, over 15750 viruses are generically
identified, so the total number of viruses and Trojans known
to F-PROT is over 134500.

Additionally the heuristics of F-PROT will detect many viruses
that have not yet been written.
```

d) BİR VİRÜSÜN VARLIĞINI ANLAMAK

Virüsler çok farklı yapılara sahip olduklarından bilgisayarınıza bulaştıklarında değişik belirtiler gösterebilirler. Bu belirtileri her zaman anlamanız mümkün olmayabilir, çünkü bazı virüsler harekete geçen kadar kendilerini gizlemeyi çok iyi başarırlar. Mesela bazıları belirli bir tarihte harekete geçerken, bir başka virüs tipi çalışmak için bilgisayarın birkaç kere yeniden başlatılmasını ya da belirli bir uygulamanın birkaç defa çalıştırılmasını bekleyebilir. Bu gibi virüsleri onlar saldırıya geçmeden tespit etmek genellikle pek mümkün değildir, ancak iyi bir anti-virüs yazılımı kullanılarak ortaya çıkarılabilirler.

Bazı virüsler ise çeşitli şekillerde varlıklarını açığa çıkaran ipuçları verebilirler, mesela kendini yaymaya çalışan bir virüs sabit disk üzerindeki boş alanın şüpheli bir biçimde azalmasına yol açabilir. Başka bir tür virüs ise bulaştığı dosyaların isimlerinde ya da büyüklüklerinde değişiklik yaparak kendini belli edebilir. Eğer hiçbir yeni veri kaydetmediğiniz halde sabit disk alanı gittikçe azalıyorsa ya da günlük tutmak amacıyla açtığınız bir metin belgesinin boyutu şüpheli bir biçimde artmışsa, yolunda gitmeyen bir şeyler olduğunu düşünme zamanı gelmiş demektir.

Virüsler verdikleri zarar açısından da çok çeşitlidirler, bazı virüsler bu açıdan oldukça masum sayılabilecek işler yaparlar, mesela belirli bir olayın yıldönümünde ekranda bir mesaj göstermek gibi. Ancak hepsi bu kadar tehlikesiz değildir, birçoğu program ve veri dosyalarını kurtarılamayacak şekilde bozarlar, hatta tüm sabit disk üzerindeki verinin bozulmasına sebep olarak bilgisayarın açılmasını dahi imkansız hale getirebilirler. Eğer bilgisayarı sadece oyun oynamak için kullanıyorsanız bu büyük bir tehdit gibi gelmeyebilir, ama işyerinizdeki bilgisayarı açıp da tüm müşterilerinizin verilerini içeren dosyanın ortadan kaybolduğunu görmek oldukça can sıkıcı bir deneyim olabilir.

Bazı virüsler çalışırken bilgisayarın performansını oldukça yavaşlatabilirler, ancak günümüzde kullanılan yüksek hızlı bilgisayarlarda bunu fark edebilmek gerçekten güç olacaktır, o yüzden bu tek başına bir belirti olamaz. Çok sık bahsedilen ve korkulan olasılıklardan biri de virüslerin bilgisayar parçalarına fiziksel hasar vermesi olasılığıdır. Ne var ki bu pek ciddi bir olasılık değildir, henüz sabit disk motorunu yakan ya da monitörü patlatabilen bir virüse rastlanmamıştır, çünkü bir programın tek başına bunu yapabilmesi mümkün değildir. Bilgisayarın anakartı üzerindeki Bios chip'inin içindeki programı bozabilen bir virüsün varlığı iyi bilinmektedir, ancak burada da donanımsal değil yazılımsal bir hasar söz konusudur ve chip yeniden programlanarak çalışır hale getirilebilir. Sonuç olarak ne yaparlarsa yapsınlar virüsler pek faydalı programlar değildirler ve onlara karşı önlem alınmalıdır. İyi bir anti-virüs yazılımı kullanmak, kaynağı şüpheli dosyalara dikkatli yaklaşmak ve önemli dosyaların yedeklerini alarak bunları güvenli bir ortamda korumak izlenecek en iyi yoldur. Eğer herşeye rağmen virüs saldırısına uğrarsanız o zaman bu konuda daha bilgili bir uzmanın yardımını istemekten kaçınmayın.

e) VİRÜSLERLE SAVAŞMAK

Virüsler bilgisayarınıza zarar verebilen yazılımlardır, ve onların ortaya koyduğu tehlikeyi gözardı etmek akıllıca değildir.

Virüslerle mücadele ederken kullanacağınız iki temel yöntem mevcuttur, bunların birlikte kullanılması karşı karşıya olduğunuz tehlikeyi küçültecektir. Uygulamanız gereken ilk yöntem virüs bulaşmasına karşı pasif korunma uygulamaktır, bunun için biraz dikkat göstermeniz yeterlidir. İkinci yöntem ise bilgisayarınızı sık sık anti-virüs yazılımlarıyla kontrol etmektir, burada her iki yöntemi de gözden geçireceğiz.

f) PASİF KORUNMA - DİKKAT VE TEDBİR

1. Bir insanın sağlıklı kalabilmek için çeşitli temizlik kurallarına uyması ve böylece hastalıklardan korunması gereklidir. İşte bilgisayarınızı virüslerden korurken de benzer biçimde uymanız gereken bazı temel kurallar vardır, bunları şöyle maddeleyebiliriz:
2. Kaynağını ve içeriğini bilmediğiniz şüpheli disket ve CD'leri asla önlem almadan kullanmayın. Bunları içeriklerine erişmeden önce anti-virüs yazılımlarıyla kontrol etmeyi ihmal etmeyin.
3. Adını daha önce duymadığınız programları çalıştırırken dikkatli olun, özellikle EXE ve BAT ekli çalıştırılabilir dosyalara karşı tetikte olun. Bunların çeşitli disketler dışında Internet gibi kaynaklardan da gelebileceğini unutmayın.
4. Her zaman için anti-virüs programlarının en güncel sürümlerini kullanın, ayrıca en az iki farklı anti-virüs yazılımdan faydalanmaya gayret edin. Böylece bilgisayarınıza virüs bulaşma ihtimalini bir hayli azaltmış olacaksınız.
5. Sadece program ve veri dosyalarını değil, aynı zamanda çeşitli dokümanları kopyalarken de dikkatli olun, özellikle "makro" türü virüsler bu şekilde basit metin dokümanlarını kullanarak bulaşırlar.
6. Asla disket sürücünün içinde disket bırakmayın. Eğer bilgisayar açılışta disket sürücüde sistem disketi arayacak şekilde ayarlanmışsa, o zaman bu disketin üzerinde bulunması muhtemel bir virüs rahatlıkla bilgisayara bulaşabilir.

g) AKTİF KORUNMA - ANTİ-VİRÜS YAZILIMLARI

Virüsleri bulmak, bulaşmalarını önlemek ve onları yok etmek amacıyla hazırlanmış programlara genel olarak anti-virüs yazılımları denir. Yazılım piyasasında bu tür pek çok program mevcuttur, bunlar farklı firmalar tarafından üretilirler. Ve hemen tüm firmalar da kullanıcıları en iyisinin kendi yazılımları olduğu konusunda ikna etmeye çalışırlar. Ancak farklı anti-virüs yazılımları değişik çalışma prensiplerine göre tasarlanırlar, bu yüzden hepsinin güçlü ve zayıf yanları vardır. Şimdi size bir anti-virüs programının içerebileceği değişik kontrol yöntemlerini tanıtacağız, seçiminizi yaparken bunları göz önünde bulundurarak karar vermenizde fayda vardır.

h) BOYUT KONTROLÜ (CHECK SUM)

İngilizce hazırlanmış anti-virüs yazılımlarında "Check Sum" adıyla geçen bu yöntemde, program bilgisayarınızda bulunan dosyaların oluşturulma tarihleri, boyutları ve benzer özelliklerini gözden geçirerek çalışır. Pek çok virüs türü "bulaşma" işlemi esnasında dosya boyutunda ya da oluşturulma tarihinde değişikliğe yol açtıklarından, bu yöntemle tespit edilebilirler. Bu yöntemin en iyi tarafın bir hayli süratli uygulanabilmesidir, ne var ki her tür virüsü tespit edemeyebilir. Çünkü bazı virüsler bu yönteme karşı korumalıdırlar ve kontrol işlemi esnasında programa bulaştıkları dosyanın tahrif edilmemiş haline uygun verileri sunarak kendilerini gizlemeyi başarırlar.

i) BİLİNEN VERİ DİZİLERİNİ ARAMA (STRING SEARCH)

Her canlının farklı bir genetik kodunun olduğu bilinen bir gerçektir, tıpkı canlılar gibi bilgisayar yazılımları da farklı kalıplarda düzenlenmiş veri kodlarına sahiptirler. Anti-virüs firmaları her zaman için yeni ortaya çıkan virüslerin program kodlarını çözmeye ve bunları bir veri bankasında toplamaya gayret ederler. Anti-virüs yazılımlarının çoğu bilgisayarınızdaki verileri kontrol ederken, içlerindeki veri dizilerinin (string) bilinen virüs kodlarına uyup uymadığını kontrol ederek çalışırlar. Bu yöntemine en iyi yanları oldukça hızlı uygulanabilmesi ve kodu bilinen virüsleri minimum hatayla ortaya çıkarabilmesidir. Ancak programın veri

bankası hemen her ay güncellenmelidir, yoksa yeni çıkan virüsleri algılamayabilir. Ayrıca bu yöntem her tip virüse karşı da etkili değildir.

j) HEURISTIC ANALIZ

Heuristic analiz metodu çok yüksek işlemci gücüne ihtiyaç duyar ve oldukça zaman harcar. Bu yüzden özellikle eski model sistemlerde kullanılması pek tavsiye edilmez. Ayrıca bu yöntemi kullanan bir anti-virüs programının arama hassasiyeti yükseltilerek daha yavaş ama detaylı bir araştırma yapması sağlanabilir. Böylece bulunması zor virüsler de rahatlıkla yakalanabilir, ancak "yanlış alarm" sayısı da aynı ölçüde çoğalacaktır.

Heuristic analiz yönteminde, anti-virüs yazılımı özellikle çalıştırılabilir program dosyalarını "sanal" olarak çalıştırır ve onların olması gerektiği gibi davranıp davranmadıklarını kontrol eder. Eğer bir programın çalışmasında belirgin aksilikler gözlenirse o zaman alarm verilir, ancak program aslında "gerçekten" çalıştırılmadığından virüs harekete geçip yayılmaz. Bu yöntemin en büyük avantajı henüz varlığı açığa çıkmamış ve kodu bilinmeyen virüs türlerini bile yakalayabilmesidir. Ancak uygulanması oldukça fazla zaman ve işlemci gücü gerektiren bir yöntemdir.

k) ON-LINE KONTROL

Bu yöntemde anti-virüs yazılımı bilgisayarın açılmasıyla birlikte devreye girer ve devamlı aktif durumda kalır. Arka planda çalışan program, olası virüs giriş noktalarını ve o an çalışmakta olan yazılımları devamlı gözaltında tutar, daha önce anlatılan yöntemlerden bir ya da birkaçını uygulayarak uygulamalardaki "tuhaflıkları" arar. Bu yöntem teorik olarak oldukça güvenlidir, özellikle yeni bulaşmaya ya da sistem içinde yayılmaya çalışan virüsleri kolayca saptayabilir. Ne var ki uygulamada çok fazla işlemci gücü gerektirir ve bilgisayarı oldukça yavaşlatabilir. Ayrıca sistem içindeki yüksek veri akışını kontrol ederken sık sık "yanlış alarm" verilmesi de mümkündür.

l) NASIL SEÇMELİ, NEREDEN BULMALI?

Anti-virüs yazılımı seçerken dikkat etmeniz gereken en önemli unsur, edinmeyi düşündüğünüz programın yukarıda anlatılan yöntemlerden en az iki tanesini uygulayarak çalışıyor olmasıdır. Böylelikle sisteminizin virüslere karşı güvenliği büyük miktarda artırılmış olacaktır. Ayrıca iyi bir anti-virüs yazılımı sadece virüsleri bulmak ve imha etmekle yetinmez, ayrıca bu işlem esnasında zarar görmüş olan dosyaları da onarabilir, böylece veri kaybı önlenmeye çalışılır.

Ancak hangi yazılımı seçerseniz seçin, kullanımda dikkat etmeniz gereken bazı unsurlar vardır. İlk olarak kullandığınız yazılımı sık sık güncellemeniz gerekir, böylelikle yeni virüslere karşı çaresi duruma düşmezsiniz. Tanınmış yazılım firmaları sundukları anti-virüs yazılımları için sık sık güncelleme paketleri çıkarırlar ve bunları özellikle Internet sitelerinde ücretsiz olarak dağıtırlar. Kaliteli bir anti-virüs yazılımı için hemen her hafta güncelleme paketi sunulabilir, bunların boyutu nispeten küçüktür ve indirilmeleri fazla zaman gerektirmez.

Peki uygun bir anti-virüs yazılımını nereden bulacaksınız? Öncelikle bilgisayar yazılım ve malzemeleri satan yerlerden bunları temin edebilirsiniz. Eğer bunu yapamıyorsanız o zaman başka kaynaklardan faydalanmanız gerekecektir. Özellikle Internet üzerinde, hemen tüm ciddi firmaların sitelerinde çeşitli anti-virüs yazılımları bulunmaktadır. Ayrıca piyasadaki bilgisayar dergilerinin yanında verilen CD-ROM'lardan da bu tür yazılımları edinebilirsiniz. Çoğunlukla kısıtlı süre için denemeniz amacıyla Shareware olarak dağıtılan bu yazılımları, eğer memnun kalırsanız makul bir fiyat karşılığında satın alabilirsiniz. Ayrıca bazı yazılımlar tamamen ücretsiz Freeware olarak da dağıtılabilmektedir.

m) EN ÇOK KULLANILAN ANTİVİRÜS YAZILIMLARI

1. Norton Antivirus
2. Pc-Cillin Antivirus
3. Panda Antivirus
4. KAV (Kaspersky Anti Virus)
5. Mc-Afee Antivirus
6. AVG Antivirus
7. F-Prot Antivirus
8. AntiVir

9. Trojan Remover