Siber Dünyanın Bombacıları

Çığır İlbaş
cigir@baskent.edu.tr
Eleştirel - Yaratıcı Düşünme ve Davranış Araştırmaları Laboratuvarı

Siber Dünyanın Bilgisayar virüsleriyle tanışması, 10 Kasım 1983 günü ABD'li doktora öğrencisi Fred COHEN tarafından sunulan konferans bildirisiyle gerçekleşmiştir. Ancak Bilgisayar virüslerinin tarihi incelendiğinde, 1970'li yılların ilk yarısında çok kullanıcılı ağ sistemlerinde virüs özelliği taşıyan yazılımların varlığı dikkati çekmektedir. Bu tür programlardan "The Creeper" bilinen en eski virüs olma özelliğine; The Creeper programını etkisiz hale getiren "The Reeper" adlı bir diğer yazılım da bilinen en eski antivirüs programı olma özelliğine sahiptir.[1]

1980'li yıllarda bilgisayar virüsü kavramı için çeşitli mitler söz konusuydu. Bilgisayar virüslerinin bir çeşit organizma olduğu ya da çok farklı bir teknolojiyle yazıldığı gibi gerçek dışı hikayeler gündemdeydi.

Bilgisayar virüsleri için operasyonel bir tanım yapmak gerektiğinde bazı unsurlar ön plana çıkmaktadır. Virüsler birer bilgisayar programıdır. Güncel bilgisayar dilleriyle yazılırlar. Ancak bir programın virüs olarak adlandırılabilmesi için çalıştığı bilgisayar sisteminde kendini gizlemesi, sistemde kopyalama, silme, ekleme işlemleri yoluyla birtakım zararlar vermesi ve farklı bilgisayar sistemlerine kendisini kopyalayabilmesi gerekmektedir. Ayrıca "Polimorfik" adı verilen özel tip virüsler kendilerini sistemde boyut değiştirerek ya da yeni virüsler türeterek gizleme özelliğine sahiptirler.

Bilgisayar teknolojisinin gelişmesiyle virüs yapılarında da belirgin gelişmeler gerçekleşmiştir. İlk zamanlarda sadece dosyalara bulaşan ve disket yoluyla farklı sistemlere bulaşan virüsler, günümüzde internet olanaklarını en iyi şekilde kullanarak birkaç gün içinde bütün dünyayı etkileyebilecek güce sahip olmuşlardır. Söz konusu yeni nesil virüslere "worm" adı verilmektedir. Internet öncesi eski nesil bilgisayar virüsleri ise, bilgisayar magazin dergilerinin verdiği disketler ve korsan programlar aracılığıyla yayılmaktaydı.

İlk IBM uyumlu PC virüsü Pakistanlı Farook Alvi adlı programcı yazmıştır. Virüsün kaynak kodlarında
"Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAB BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE :430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination..... !!"
ifadesi yer almaktadır. Günümüzde ise bilişim yasaları nedeniyle virüs yazarları kişisel bilgilerini deşifre etmemekte sadece bireysel veya toplumsal mesajlar iletmektedirler.

Türk virüsleri arasında toplumsal mesaj veren en iyi örnek GencVir.1000 virüsüdür. Virüsün bulaştığı bilgisayarda,
"Ey Turk gencligi! Birinci vazifen Turk istiklalini, Cumhuriyetini, ilelebet, muhafaza ve mudafaa etmektir. Mevcudiyetinin ve istikbalinin yegane temeli budur. Muhtac oldugun kudret, damarlarindaki asil kanda,mevcuttur M.Kemal ATATURK"
ifadesi görüntülenmektedir.

Özellikle 2004 yılında virüs yazan kişi ve gruplar arasında şifreli mesajlar aracılığıyla bir çeşit rekabetin oluştuğu virüs sayı ve türevlerinin hızlı artışına da bu rekabetin neden olduğu düşünülmektedir.[2]

Bilgisayar dünyasında yüksek risk seviyesinde değerlendirilen en tehlikeli virüs 1998 yılında yazılan W95.CIH (Chernobyl) virüsüdür. Çernobil nükleer felaketinin yıldönümü olan 26 Nisan'da aktif hale gelen virüs dünya genelinde 4 milyar dolar zarara yok açmıştır.[3]

Ofis program dosyalarında hasara yol açan ve Makro Virüsü olarak adlandırılan türün ilk örneği, 1995 yılında yazılan WM.CONCEPT virüsüdür. Söz konusu virüs açık kaynak kodluydu ve diğer makro virüslerinin oluşturulmasını sağladı.

İlk "worm" (internet kanalıyla yayılan zararlı kod), Robert Morris tarafından 1988 yılında yazılan 99 satırlık bir programdır ve kısa süre içinde 60 binden fazla bilgisayara yayılmıştır.

Bilgisayarlarda güvenlik açığı yaratarak şifre ve dosyaların elde edilmesini sağlayan Trojan türü programların ilk yaygın örneği, Mart 1998 yılında Carl Fredrik Neikter tarafından yazılan NetBus isimli programdır.

Günümüzde tanımlanmış bilgisayar virüslerinin sayısı 80 binin üzerindedir. Antivirüs programlarının virüs kodunu tespit edip veritabanlarına alması işleminde, kimi zaman 2 - 3 aya varan gecikmeler nedeniyle hiçbir antivirüs programı tam anlamıyla koruma sağlayamamaktadır.

Virüsler teknolojide hem olumlu hem de olumsuz etkilere yol açmaktadır. Birer siberterör saldırısı olarak bilgisayar ve Internet kullanımında tedirginliklere, özellikle e-ticaret uygulamalarında azalmalara yol açtığı gibi yeni jenerasyon virüsler

[1] http://www.viruslist.com/eng/viruslistbooks.html?id=16 (**Computer Viruses by Eugene Kaspersky)**

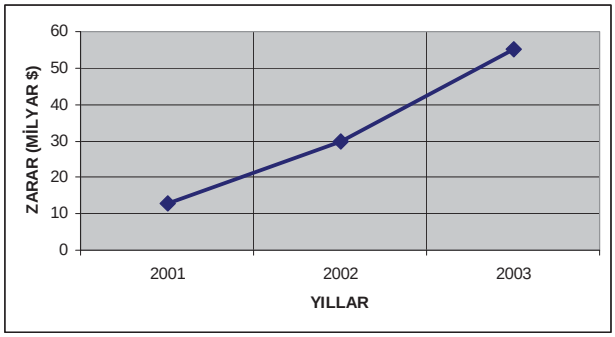
[2] http://www.ntvmsnbc.com/news/259968.asp?0m=-16S

[3] http://arsiv.hurriyetim.com.tr/hur/turk/99/04/28/ekonomi/03eko.htm

internet ve e-posta trafiğini ciddi ölçüde yavaşlatmaktadır. Virüslerden korunmak için kullanılan antivirüs yazılımları bilgisayar teknolojisinde çok büyük öneme sahip olan işlemci hızını düşürmektedir. Diğer yandan güvenlik sistemlerine gereken önemin verilmesinin altını çizmekte ve algoritma mantığına çeşitli katkılarda bulunmaktadır.

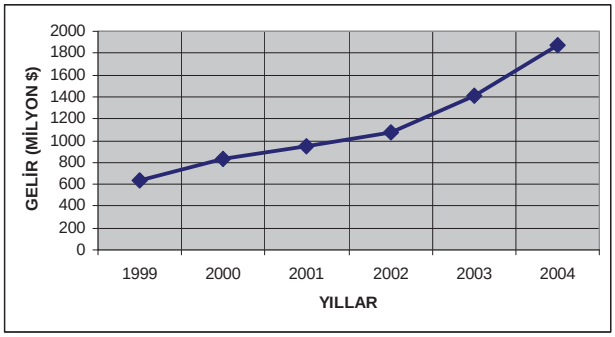
Siberterör açısından ele alındığında, bilgisayar virüsleri, amacı olan ancak hedefi olmayan saldırılardır. Bir kasabanın içme suyu deposuna zehirli madde ekleyip ertesi gün kasabanın günlük yaşantısındaki değişimi ve kaosu izleyen bir kişiyle virüs yazarları arasında davranışsal ve psikolojik açıdan benzerlikler olduğunu söylemek mümkündür.

Virüsler geçtiğimiz yıl ekonomiyi 55 milyar dolar civarında zarara uğratmıştır. 2004 yılında bu zararın iki katına çıkması beklenmektedir. 2002 yılında söz konusu zarar 30 milyar, 2001'de ise 13 milyar dolar olarak gerçekleşmiştir. (Şekil 1)



Şekil : Virüslerin dünya ekonomisine verdiği yıllık toplam zarar.

Antivirüs firmaları ise, yıllık ortalama 1.5 - 2 milyar dolar gelir elde etmektedir. Son üç yılda antivirüs firmalarının elde ettikleri gelirle virüslerin ekonomiye açtığı zararlar arasında aynı yönde artan bir trend dikkati çekmektedir. (Şekil 2)



Şekil 2: Antivirüs sektöründe lider bir firmanın yıllık gelirleri.

Virüs yazarları BBC'nin araştırmasına göre 14 - 26 yaş arasındaki genç erkeklerden oluşmaktadır.[4] Ortak özellikleri; bilgisayar başında çok uzun süre kalmaları, antisosyal kişilik özellikleri taşımaları. Ayrıca sanıldığının aksine çok zeki bireyler değiller.

Antivirüs şirketi Symantec'te uzman olan ve virüs yazarları üzerine araştırmalar yapan Sarah Gordona göre; yaygın kanaatin aksine virüs yazarları yalnızlığı seven, "underground" yaşayan ve çok zeki olmayan insanlardır.[5]

Bilgisayar virüslerinin günümüzde her sene artan ölçüde ciddi bir sorun olmasının temelinde, Internet'in kontrolsüz gelişimi ve Internetin ilk dönemlerinde geleceğe ilişkin öngörü yapılamaması gerçeği yer almaktadır. Konuyla ilgili olarak İnternetin fikir babaları arasında yer alan Dr. Leonard Kleinrock, "*Internet virüsleri, pornografi siteleri, çocuk pornografisi, Internet sitelerindeki hatalar, güncellenmeyen adresler, tarayıcı yazılımlardaki açıklar gibi internette sıkça karşılaşılan sorunları öngörebilseydik bunlara karşı hazırlıklı olabilirdik. Hiçbirimiz Internetin bu kadar büyüyeceğini tahmin edemedik.*" şeklinde bir açıklama yapmıştır.[6]

Bu veriler ışığında 2005 yılının virüsler açısından çok daha hareketli ve sorunlu geçeceği tahmin edilmektedir. Global çözümler üretilmediği sürece, virüs tehlikesinin her sene artan oranlarda ortaya çıkması ve Interneti kullanılamaz hale getirmesi olasılığı söz konusudur.

Yeni jenerasyon virüsler, bulaştığı bilgisayarın adres defterindeki kayıtlar arasından rastlantısal olarak adresler seçip virüslü e-postayı transfer etmektedir. Bu nedenle sisteminde virüs bulunmayan bir kullanıcıdan bir başkasına virüs transferi gerçekleşmiş gibi algılanabilmektedir. Bu durum virüslerin hızlı yayılmasını sağladığı gibi "spam e-posta" trafiğini belirgin ölçüde yoğunlaştırmaktadır.

Kullanıcı olarak alınabilecek önlemler; bilgisayar sistemine bir antivirüs yazılımı yükleyip düzenli olarak güncellemek, özel verileri Internet ortamından koruyup yedekleme ünitelerinde saklamak ve özellikle e-postalar konusunda daha dikkatli ve temkinli olmak şeklinde sıralanabilir.

[4] http://www.bbc.co.uk/science/hottopics/computerviruses/crime.shtml
[5] http://www.hurriyetim.com.tr/haber/0,,sid~12@tarih~2002-02-14-m@nvid~95194,00.asp
[6] http://www.ntvmsnbc.com/news/278013.asp