TEKNOLOJİ VE YAŞAM

İNTERNETTE MAHREMİYET: GÜVENLİK VE GÜVENLİĞİ SAĞLAMA YOLLARI*

Uzm. Psk. Tarık Solmuş

Bilişim teknolojisindeki sürekli gelişmeler ve artık neredeyse günlük pazar alışverişlerinin bile yapılageldiği internet ortamındaki bilgi paylaşımı, güvenlik sorunlarını da beraberinde getirmektedir. Amerika'da yapılan bir araştırmada, her üç bilgisayardan birinde casus yazılımların (spyware) bulunduğu saptanmıştır. Geçtiğimiz yılda dünyanın önde gelen petrol dağıtım şirketlerinden birine yönelik yalnızca 1 saat içerisinde 25.000 virüs saldırısı gerçekleştiği belirlenmiştir. Güvenlik konusu, çeşitli kötü niyetli yazılımların/tehlikelerin son zamanlarda cep telefonlarına bile bulaşıyor olmaları nedeniyle de ayrı bir önem kazanmıştır. Bir güvenlik sorunu olarak, istenildiğinde web sayfaları "çökertilebilmekte" ya da kopyalanabilmektedir. İki yıl kadar önce bir bankanın web sayfası 'hacker'lar tarafından kopyalanmış; o gün içerisinde internet bankacılığı aracılığıyla bankanın web sayfası üzerinden işlem yapan tüm kullanıcılar durum fark edilene kadar neyazık ki aslında "başka bankalar" için işlem yapmıştı. Bununla birlikte, bir güvenlik ihlali olarak şifreler kırılabilmektedir; örneğin, Hotmail ya da Yahoo'ya ait bir e-posta hesabınızın şifresinin kırılıp, e-postalarınızın okunması ya da sizin adınıza başka yerlere e-posta gönderilmesi gibi işlemler aslında düşündüğünüz kadar zor değil J. Tabi buarada siz de eğer isterseniz bilgisayarınıza çeşitli programlar yükleyerek tüm internet kullanıcılarının sahip olduğu-internetteki kimliği anlamına gelen IP (Internet Protocol) numaranızı saklayabilir; böylelikle örneğin ziyaret ettiğiniz web sayfalarının öğrenilmesini engelleyebilir, internette tamamen "görünmez" olabilirsiniz. Dünyanın en büyük kütüphanesi olarak kabul edebileceğimiz internetteki bilgi ve veri akışının her geçen gün artarak katlanacağını düşündüğümüzde güvenlik sorunlarının çözümü kendisini önemli bir noktada göstermektedir. Aşağıda, öncelikle kullanıcıların karşılaşabilecekleri güvenlik sorunları/tehditlerine yer verilmiş ve sonrasında da bu sorunların üstesinden gelebilecek bazı araçlara/programlara değinilmiştir. Ayrıca, her program hakkında, programa ulaşabileceğiniz web adresi ve programlar arasında bir seçim yaparken kararınızı etkileyebileceğini düşündüğümüz ücret bilgisi de verilmiştir. Bu noktada, aylık olarak yayınlanan bazı bilişim dergilerinin promosyon amaçlı olarak verdiği CD'ler aracılığıyla bazı programların tam sürümlerine (full version), bazı programların ise örneğin 1 aylık deneme sürümlerine (trial version) ulaşabileceğinizi söyleyelim. Özellikle deneme sürümleri, programların performansını deneyebilmeniz ve seçimde bulunabilmeniz açısından yararlı olacaktır.

**Makalede yer alan tüm bilgiler Mayıs 2005 tarihlidir.*

Güvenliğe Yönelik Tehditler

Bilgisayarınızın mahremiyetine/güvenliğine yönelik tehditleri, *virüs, casus yazılım* (spyware), *Truva atı* (trojan horses), *çevirici* (dialer), *reklam penceresi* (PopUp), *çöp posta* (spam mail), *kötü şakalar* (hoaxes) ve *internet solucanı* (worm) kategorilerinde toplayabiliriz. Bunların dışında, özellikle, kredi kartı kullanımınız sırasında klavyenizde bastığınız tüm tuşların bir kaydını tutan ve böylelikle örneğin kredi kartınıza olası "yeni

bir ortak yaratan" *Keylogger'ları* ya da internet tarayıcınızın (örneğin, internet explorer ya da mozilla) ayarlarını değiştirip, örneğin siz ne yaparsanız yapın hep o pornografik içerik taşıyan web sayfasının açılmasını sağlayan *Hijacker'lığı* casus yazılım kategorisinde ele alıyoruz. *Hacker'lığa* bireysel kullanıcılar (home users) için önemli bir tehlike oluşturmaması nedeniyle değinmiyoruz.

Virüsler: Virüsler, bilgisayarınıza e-posta ya da internet aracılığıyla bulaşırlar. Bir virüs bilgisayarınıza bulaştığı anda öncelikle kendisine gizlenecek bir yer bulur; kendisini yapacağı işleme göre farklı dosya ya da programlara enjekte eder. Eğer bir e-posta virüsü ise, adres defterinizde bulunan kişilere kendisini göndererek başka bilgisayarlara da bulaşır. Virüsler bulaştıkları anda harekete geçebilecekleri gibi belirli bir tarihte de etkin hale gelebilirler. Tüm virüsler farklı zararlar verirler. "Boot" virüsleri sabit (hard) diskinize yerleşerek tüm verilerinizin silinmesine neden olabilirler. 1993 yılında ölümünden kısa bir süre sonra (bir söylentiye göre öldürülmesini "protesto amaçlı" olarak) Uğur Mumcu adına aynı adla bir virüs üretilmiş; virüs hiçbir antivirüs programı tarafından temizlenememiş ve bulaştığı her bilgisayara format atılmasını gerektirmişti. "Makro" virüsleri ise, Word ya da Excel'de hazırlamış olduğunuz dosyalarınıza bulaşarak okunamaz hale getirebilirler.

Bilgisayarınızda bir virüsün olup olmadığını anlamanın bazı yolları vardır. Bilgisayarınız özellikle son günlerde oldukça yavaşlamıştır, üstelik bu durum aynı anda birden fazla dosyayla çalışmadığınız halde gerçekleşiyordur. Daha önce rahatlıkla açabildiğiniz bazı dosyaları artık açamıyorsunuzdur ya da bilgisayar bazı dosyaların kayıp olduğuna yönelik mesaj veriyordur (bu durum sisteminize yerleşen virüsün dosyalarınızın bir bölümünü silmesi ya da değiştirmesinin bir sonucudur). Bellek kapasitenizde anlık düşüşler olur ya da örneğin 2 GB'lik bir sabit disk kapasiteniz olduğu halde, dosya kaydedilebilecek yer kalmadığına ilişkin mesajlar almaya başlarsınız. Bir dosyanızın, örneğin Word dosyanızın adı ya da özellikleri kendiliğinden değişmiştir. Bilgisayarınız kendiliğinden kapanıp açılabilir ya da bir kapanır artık kapanış o kapanıştır. CD-ROM'unuz kendiliğinden açınıp kapanır, klavyenizin tuşları siz basmadığınız halde yazı yazar, ekranınız aniden kararır, fareniz kendi kendine hareket eder.

Diyelim ki, bilgisayarınızda herhangi bir antivirüs programı var ve bu program bir virüs uyarısı veriyor. Öncelikle, virüsün adını not etmenizi öneririz; böylelikle gerektiğinde internet üzerinden virüsün nasıl bulaştığı/yayıldığı ve ne tür zararlar verdiği gibi konularda ayrıntılı bilgi edinebilirsiniz. Bu bilgiye de, örneğin, antivirüs programınızın web sayfasındaki virüs ansiklopedisinden/veri bankasından (her antivirüs programının bu tür bir virüs bankası mutlaka vardır) ulaşabilirsiniz. Daha sonra, antivirüs programının sizi yönlendirdiği şekilde davranmanızı öneririz; program ya sizden virüslü dosyaları silmenizi ya da silemiyorsanız eğer karantinaya almanızı isteyecektir. Bununla birlikte, diyelim ki, bilgisayarınızda antivirüs programınız yok ama siz virüs olduğundan kuşkulanıyorsunuz (örneğin, bilgisayarınız çok yavaşladı ya da artık bir Word dosyasını 2 dakikada açmaya başladı). Bu durumda, internete bağlanıp ücretsiz ve de anında tarama (online-scan) yapan bir antivirüs programı aracılığıyla bilgisayarınızı tarattırabilirsiniz (Bunu, örneğin, Panda Platinum'um www.pandasoftware.com ya da McAfee'nin www.mcafee.com adresleri üzerinden yapabilirsiniz). Bir başka yol da, daha önce acil durumlarda kullanmak üzere hazırladığınız (böyle bir cd'yi mutlaka hazırlamış olduğunuzu umuyoruz), sistem başlangıç CD'si ("system

start-up" ya da "bootable" cd) kullanarak bilgisayarınızı yeniden başlatmanız ve bir antivirüs programı kullanarak virüsü temizlemenizdir. Sistem başlangıç CD'si, bilgisayarınızın veri işlem sürecini sağlayan bazı temel .sys ve .com dosyalarını içerir. Bu cd'yi, örneğin, en iyi CD&DVD kopyalama-yazma programı olarak da önerebileceğimiz Nero'yla (Nero Burning Rom ya da diğer adıyla Nero Toolkit) kolaylıkla hazırlayabilirsiniz.

Casus Yazılımlar (Spyware): Öncelikle, burada söz edilen "kötü niyetli" tüm güvenlik tehditlerinin (truva atları, internet solucanları vb.) temel olarak bir casus yazılım olduğunu söylemeliyiz. Bir casus yazılımın daha doğrusu bu yazılımı bilgisayarınıza sokmayı başaran kişinin temel amacı, sisteminiz hakkında bilgi toplamak, internette yaptığınız sörflerin de yardımıyla temel ilgi alanlarınızı/sörf alışkanlıklarınızı belirlemek ve bunları da büyük oranda reklam kuruluşlarına satarak para kazanmaktır. Diyelim ki, bilgisayarınızda "CoolWebSearch" adlı casus yazılım var ve diyelim ki, yıllar önce tecavüz konulu bir yüksek lisans tezi hazırladınız; aradan yıllar geçtikten sonra da ne tür gelişmeler olduğuna ilişkin, örneğin Google'da geniş çaplı bir tarama yaptınız. Bu taramanızı saptayan kötü niyetli kişiler, mail adresinizi pornografik içerikli yayınlar yapan web sitelerine satıyorlar. Kısa bir süre sonra, belirli bir ücret karşılığı canlı tecavüz yayını yapan (ya da böyle olduklarını iddia eden) pornografik web sitelerinden bazılarının reklam pencereleriyle (PopUp) boğuşma olasılığınızın yüksek olacağını söyleyebiliriz. Casus yazılımların, bilgisayarınıza, özellikle .mp3 müzik, pornografik resim-film, oyun demoları, film fragmanları ya da ücretsiz (freeware) yazılımlar indirebileceğiniz web sayfaları aracılığıyla bulaşacağını söylemeliyiz. Bu tür başlıklarda program indirdikten sonra, programı çalıştırmadan önce mutlaka güvenlik taraması yapmanızı öneririz. Buarada, son haftalarda, Windows Media Player'ın bir film formatı olan .wvm uzantılı film ya da fragmanların da casus yazılımlar içerdiğini ve kullanmadan önce mutlaka güvenlik (özellikle antispyware) taraması yapmanız gerektiğini belirtelim.

Truva Atı (Trojan Horses): Truva atları virüslerle çok karıştırılmalarına karşın, onlardan tamamen farklı olan yazılımlardır. Virüsler bilgisayarınıza yerleşip kendilerini yayarlar, dosyalarınızı silebilir ya da değiştirerek zarar verirler. Truva atları ise, kendilerini yaymazlar, dosyalarınıza ve bilgisayarınıza doğrudan bir zarar vermemekle birlikte internete her bağlandığınızda otomatik olarak etkin hale geçerler. Bilgisayarınızı çalıştırdığınız her saniyenin virüsün kendisini yayabilmesi için bir olanak olduğunu söyleyelim. Ancak, Truva atları, internet kullanımıyla ilişkili olması nedeniyle, internete bağlanmadığınız sürece bir sorun yaratmayacak olan yazılımlardır. Truva atlarının temel amaçları, bilgisayarınızda bir boşluk bulup "açık kapı" yaratmaktır. Bir önemli farklılık da, virüsleri bir antivirüs programı olmadan bilgisayarınızdan kaldıramazken bir truva atını eğer adını biliyorsanız bilgisayarınızdan kaldırabilme şansınızın olmasıdır (örneğin, "NewDotNet" casus yazılımını "Denetim Masası/Ekle-Kaldır" aracılığıyla sisteminizden kaldırabilirsiniz). Truva atı, genellikle e-posta yoluyla ya da ICQ ve Messenger gibi anında mesajlaşma uygulamalarını kullanarak bulaşır. Bilgisayarınıza .exe, .scr ya da .msi uzantılı bir dosyanın çalıştırılması ile bulaşan Truva atlarının büyük çoğunluğu kendilerini Windows'un açılışına (registry files) yerleştirir. Sistemde kullanılmayan iletişim bağlantı noktalarından (port) birini kendisine ayırarak beklemeye başlayan Truva atı, bir anlamda açık bir arka kapı niteliğindedir. Böylelikle, dün-

yanın herhangi bir yerindeki bir kullanıcı bilgisayarınızdaki dosyaları görebilir, kopyalayabilir, silebilir, bazı komutlar aracılığıyla farenizi ya da klavyenizi sanki onun elindeymiş gibi kullanabilir, hatta size örneğin X dosyasını A klasöründen alıp B klasörüne kopyalamanız gerektiği gibi doğrusu küstahça "önerilerde" bile bulunabilir. Bununla birlikte, klavyenizde bastığınız her tuşu kaydederek, örneğin *internet üzerinden kredi kartıyla alışveriş yaptığınızda* oluşan klavye notu aracılığıyla *kredi kart numaranızı ve şifrenizi* öğrenebilir. Bu noktada, çok acil bir durum olmadığı ve başka hiçbir iletişim kanalı seçeneğiniz kalmadığı sürece, kredi kart ya da banka hesap numaralarınızı e-posta ya da anında mesajlaşma programları (ICQ ve Yahoo Messenger gibi) üzerinden başka bir kişiye göndermemenizi öneririz. Truva atlarının bir zarar verici yönü de sizi, ne yaparsanız yapın onun istediği web sayfasının açılmasını sağlayacak biçimde kilitlemesidir; bu tür web sayfaları da genellikle ticari ya da pornografik sayfalardır. Diyelim ki, bilgisayarınızda böyle bir Truva atı var, TTnet kullanıyorsunuz, internete bağlandığınıza ilişkin mesajı gördünüz ve e-postalarınıza bakmak için "Adress" kısmına mail.yahoo.com yazdınız ve beklemeye başladınız, sanıyoruz gördüklerinize inanamayacaksınız. Pek çok kullanıcı, böyle bir durumdan, "Başlat Menüsü/Denetim Masası/Internet Seçenekleri/Genel" seçeneğini kullanarak internete bağlandığında otomatik olarak açılmasını istedikleri web sayfasının (home page) adını değiştirerek kurtulmaya çalışırlar. Bu geçici bir çözümdür çünkü bilgisayar kapatılıp daha sonra yeniden açıldığında ve internete bağlanıldığında hiçbir şeyin değişmediğini görülebilecektir. WhenU, NewDotNet, Attack, BackDoor, DeepBO, Netbus, SubSeven, Priority, Kid Terror ve CrazzNet en sıklıkla görülen truva atlarındandır. Microsoft AntiSpyware, Ad-Aware, Spybot - Search & Destroy, McAfee AntiSpyware gibi programlar truva atlarını yakalama ve silme konusunda ustadırlar.

Çeviriciler (Dialers): Çeviriciler, özellikle pornografi içeren internet sayfalarında bulunan ve normal internet bağlantınızı (ve de tabi ki bağlantı ücretinizi) kesip sizi uluslararası hatlardan (örneğin, 900'lü hatlar) internete bağlayan yazılımlardır. Çeviricilerin, ağırlıklı olarak pornografik siteler için kullanılmakla birlikte başka sitelerden de bulaşabileceği olasılığı göz önüne alındığında, bir önlem olarak telefon hatlarınızı uluslararası aramalara kapatmanızı öneririz.

Reklam Pencereleri (PopUp): Reklam pencereleri, web sayfalarını ziyaret ettiğinizde aniden ekrana gelen reklam içerikli pencerelerdir. Reklam pencerelerinin doğrudan bir zararı yoktur, ancak içeriğinde yer alan herhangi bir bağlantı (link) virüs ya da truva atı içerebilir, bu nedenle üzerindeki hiçbir bağlantıyı tıklamamanızı öneririz, bu pencerelerden kurtulmanın en kolay yolu, sağ üst köşesinde yer alan çarpı işaretini (close) tıklayarak pencereyi kapatmanızdır. Bu tür pencerelerle başa çıkabilmek için "PopUp Blocker" sınıfında yer alan güvenlik programlarını kullanabilirsiniz. Ancak, Ad-Aware gibi bu konuda uzmanlaşmış programları ya da tüm kötü niyetli yazılımlara karşı tam bir güvenlik sağlayan McAfee Internet Security Suite veya Norton Internet Security programlarından birini kullanmanızı öneririz.

Çöp Posta (Spam Mail): Çöp postalar, sizin istediğiniz ve bilginiz dışında posta kutularınıza gelen reklam iletileridir. Ünlü güvenlik şirketlerinden Kaspersky Labs'ın yöneticisi Eugene Kaspersky'e göre 2004 ilkbaharında dünyada gönderilen e-postaların % 60 ile % 70 arasında değişen bir oranın çöp posta iletileri olduğu tahmin ediliyor. "Casinomuzda kumar oynamak artık çok kolay, tıklayın yeter" ya da "Tebrikler, bizden 3 adet

ücretsiz DVD kazandınız, ama önce sitemizi ziyaret etmeniz gerekiyor" cümlelerini içeren ve virüs taşıyabilen postalar, çöp posta grubuna girmektedir. Bu postaların bilgisayarınıza bulaşma yollarından biri belki de en önemlisi, size tanımadığınız bir mail adresinden gelen postaya yanıt vermenizdir. Diyelim ki, bilgisayar ürünleri satan bir şirketten size reklam içerikli bir posta geldi, bu aslında çöp posta uzmanların sanki seçkisizce posta göndermelerinin bir sonucu (üstelik içinde neredeyse kesinlikle virüs olduğunu söyleyebiliriz), yani özellikle birebir size gönderilmiş bir posta değildir. Diyelim ki, siz de bu tür postalar almak istemediğiniz için iletinin geldiği adrese "lütfen beni e-posta üye listenizden çıkarır mısınız" gibi aslında ne yaptıklarını bilseniz haklı olarak hiç de bu kadar kibar olmayacağınız bir cevap yazıyorsunuz. Üzgünüz, çünkü iletiyi size gönderen kişi mail adresinizi *asıl şimdi* öğrenmiş oluyor. Peki çözüm? Elbetteki, bu tür postaları açmadan silmek. Ama daha gerçekçi ve güvenli olanı, antispam programlarını kullanarak, daha baştan size böyle bir postanın gelmesini engellemek. Antispam programları, size internet üzerinden bulaşan çöp postaları siz o postayı/postaları açmadan, hatta görmeden önce belirleyip ayıklayan programlardır. Çöp postalarla baş edebilmek için McAfee Spamkiller, MailWasher ya da Norton Anti Spam programlarından birinin kullanılması yararlı olacaktır. Bu arada, dünyada en sıklıkla kullanılan iki posta hizmeti sağlayıcı kurumları olan Yahoo'nun Norton tarafından ve Hotmail'in de Trend Micro-PCcillin tarafından korunduğunu; bu iki posta adresi sağlayıcısına ait posta adresleriniz varsa eğer, kendinizi daha güvende hissedebileceğinizi söyleyebiliriz. Örneğin, Norton Yahoo'ya her gün gelen ortalama 1 milyar çöp postayı ayıklayabiliyor; postayı açsanız bile uyarı mesajı veriyor, bu durumda da web tarayıcınızın (örneğin, internet explorer) "geri" seçeneğini tıklamanız yeterli. Çöp postaların, kullanıcıların ilgisini çekebilecek başlıklarla (örneğin, "Hi", "Something for you", "I Love You" gibi) gönderildiğini ve genellikle 31 ya da 41 kilobayt'lık bir kapasiteye sahip olduklarını söyleyelim.

Kötü Şakalar (Hoaxes): Bunlar size e-posta aracılığıyla gelen yalan-yanlış mesajlardır. Mesajı gönderen kişinin amacı kullanıcıda panik yaratmaktır, bu amacında da büyük olasılıkla başarılı olur. Sizden, örneğin, son iki gün içerisinde internette çok ciddi bir virüsün yayılmakta olduğunu, isterseniz bu virüsten korunabileceğinizi, ama bunu yapmak için de onun belirttiği adımları izlemenizi ister. Hatta, bazen, güveninizi kazanmak amacıyla bu tür postaların sanki McAfee, Panda ya da Norton gibi güvenlik şirketleri tarafından gönderilmiş gibi göründüğü durumlar söz konusu olabilir; örneğin gönderici adresi support@symantec.com'dur (Symantec Norton'un üreticisidir). Sizden yapmanızı istediği aşamalar, yüksek bir olasılıkla içi bir sürü teknik terimle dolu olan adımlardır; bazı dosyaları silmenizi ya da özelliklerini değiştirmenizi ister, bu dosyalar da genellikle .exe, .com ya da .sys uzantılı dosyalardır. Bu dosyalar, bilgisayarınızın çalışması için gerekli olan temel sistem dosyalarıdır. Diyelim ki, örneğin bir sistem kur (setup) dosyasını silmeyi başardınız. Bu durumda, sizin adınıza, geçtiğimiz en yakın sürede önemli dosyalarınızın bir yedeğini almış olmanızı dilemekten başka bir şey kalmaz.

Internet Solucanları (Worm): Internet solucanları, virüslere çok benzemekle birlikte, dosyalara zarar vermeyip kendi kendilerini bir zarar verici dosya haline getirmeleri ve yayılmaları nedeniyle virüslerden ayrılırlar. Bilgisayarınıza e-posta yoluyla ve ek dosya olarak (attachment) doğrudan bulaşırlar, ayrıca, içerisinde solucan taşıyan bir web sayfasına bağlantısı bulunan bir posta da bil-

gisayarınıza dolaylı olarak solucan bulaşmasına aracılık etmiş olur. Solucanlar, kullandığınız posta servisinizdeki (Yahoo ya da MS Outlook gibi) adres defterinizi kullanarak başka kullanıcılara da bulaşmaya çalışırlar. Ad-Aware, Spybot-Search & Destroy ve Norton Internet Security gibi güvenlik programları bu solucanlardan kurtulabilmeniz için kullanabileceğiniz programlardandır.

Güvenliği Sağlamaya Yönelik Araçlar-Programlar

Aşağıda da görülebileceği gibi, internet güvenliğini sağlamaya yönelik birçok program bulunmakta. Özellikle, başta virüsler, Truva atları ve internet solucanları olmak üzere bir çok zararlı yazılıma karşı koruyucu bir güvenlik programı olması amacıyla geliştirilmiş 20 kadar antivirüs ya da tam internet güvenliği programı bulunmakta. Ancak, burada yalnızca, kullanım kolaylığı, yaygınlığı, tarama kapasitesi, güncellenebilirlik durumu ve sistem performansı üzerindeki etkisi gibi temel noktalar açısından bilişim teknolojisinde kendini kanıtlamış olan programlara yer veriyoruz. Örneğin, *F-Prot'u* 90'lı yıllardaki başarısını sürdürememesi nedeniyle önermiyoruz; ancak dilerseniz www.f-prot.com adresi üzerinden programı inceleyebilir hatta indirip kullanabilirsiniz. *eTrust EZ* ve *Norman Virus Control* programlarının yalnızca "adının bilindiğini", *"ClamAV"* ve *ESED Nod32*'inin de yalnızca Linux kullanıcılarının işine yarayacağını söyleyelim. *F-Secure*'un geniş çaplı bir güvenlik sağlayamamasının yanında, bilgisayarınızı en çok yavaşlatan (işlemcinizi en çok yoran) program olduğunu söyleyelim. *AVG Antivirus* ve *AntiVir Personal Edition* programlarını da, nitelikli birer antivirüs programları olmaları ve ücretsiz olmalarıyla tercih edilmelerinin yanında, yalnızca virüsler konusunda uzmanlaşmış olmaları; McAfee, Norton ya da BitDefender kadar geniş kapsamlı bir koruma sağlayamamaları nedeniyle önermiyoruz. Kuşkusuz, bu noktada, bu makalede yer alan tüm bilgilerin (ya da önerilerin) ilgili konularda kaynak kullanımının (örneğin, her programın kendi web sayfası ve çeşitli sayfalar üzerinden incelenmesi gibi) yanında kişisel deneyimlere dayalı olduğunu özellikle belirtmeliyiz.

Buarada, aşağıda *kısaca* tanıtmaya çalıştığımız tüm programlar temel olarak "antispyware" ya da "antivirus" sınıfındayer alan programlardır. Üçüncü güvenlik sınıfını oluşturan "firewall" (güvenlik duvarı) sınıfında yer alan programlara da (Kerio Personal Firewall, Sygate Personal Firewall ve ZoneAlarm Pro gibi), gerek bu programların ağ (LAN ya da WAN gibi) ve sistem güvenliği konusunda uzmanlaşmaları ve gerekse ileri düzey bilgisayar kullanıcıları için yararlı-gerekli olacağı inancıyla değinmiyoruz.

Microsoft AntiSpyware Beta 1: Microsoft, kurucusu ve sahibi Bill Gates'in evindeki bilgisayarlarında bile casus yazılımların bulunmasının da etkisiyle, Aralık 2004 tarihinde ünlü antispyware yazılım firması Giant AntiSpyware'i satın alarak programı Ocak 2005'te Microsoft AntiSpyware adı altında piyasaya sürdü. Program henüz deneme (Beta) aşamasında, 31 Temmuz 2005 tarihi itibariyle ya yine Beta sürümüyle, ama başka bir isimle ya da tam sürümüyle kullanıcıların hizmetine sunulacak. Microsoft AntiSpyware'in şu andaki en iyi casus yazılım önleyici program olduğunu; Ad-Aware ve Spybot - Search & Destroy gibi bu konuda tanınmış programları bile geride bıraktığını söyleyebiliriz. Programı, istediğiniz dosyaları ya da tüm bilgisayarınızı tarattıracak biçimde ayarlayabilirsiniz, isterseniz taramayı otomatik olarak yaptırabilirsiniz (örneğin, her gün saat 15.00'da). Programın örneğin anında koruma (real-time protection) seçeneği ile, internet bağ-

lantınızı izlemesini, her türlü casus yazılımı ya da dışarıdan yapılacak müdahaleyi daha bilgisayarınıza bulaşmadan engellemesini sağlayabilirsiniz. Programın önemli özelliklerinden biri, kendisini otomatik olarak güncelleyebilmesi. Microsoft AntiSpyware'in bilgisayarınızda mutlaka bulunmasını öneriyoruz.

Web Adresi: www.microsoft.com/athome/security/spyware/product

Ücreti: Ücretsiz

Ad-Aware SE: Ad-Aware SE'nin virüsler dışındaki diğer kötü niyetli yazılımlar için en iyi güvenlik programlarından biri olduğunu söylemek olanaklı. Program, virüsler hariç tüm kötü niyetli yazılımları tarıyor. Programı "Perform full system scan" modunda çalıştırmanızda yarar var; böylelikle bilgisayarınızdaki tüm sistem, sürücü ya da dosyalar taranıyor. Bir casus yazılım bulduğunda da sizin seçiminize göre ya karantinaya alıyor ya da siliyor. Kritik bir durumla karşılaştığında sistemi yeniden başlatıyor ve işletim sisteminizin (Windows 98 ya da XP gibi) etkin olmasından önceki tüm süreci tarıyor. Programı belirli aralıklarla güncelleştirmenizde de yarar var.

Web Adresi: www.lavasoft.de

Ücreti: Ücretsiz

Spyware Blaster: Program, casus yazılımları bulup silen diğer AntiSpyware programlarını "sollayarak" kendi "kara listesinde" (veri bankası) yer alan yazılımların bilgisayara bulaşmasını daha baştan engelliyor. Böylelikle yazılımlar bilgisayarınıza giremiyor, girse bile zarar veremiyorlar. Ayrıca, program, siz internete her bağlandığınızda onu etkinleştirmenize gerek kalmadan, üstelikte size hiç fark ettirmeyecek ve sizi engellemeyecek biçimde kendiliğinden çalışmaya başlıyor. Programı belirli aralıklarla güncelleştirmeniz yeni yazılımlara karşı korunmanız açısından da önemli. Programı etkili bir şekilde kullanabilmeniz için "Status" kısmında bulunan "Enable All Protection" seçeneğinin ve "Internet Explorer - Restricted Sites" kısımlarında yer alan tüm seçeneklerin işaretli olması gerekiyor.

Web Adresi: www.javacoolsoftware.com

Ücreti: Ücretsiz

Spybot - Search & Destroy: Bu program da en nitelikli/başarılı güvenlik programlarından biri. Programla, Ad-Aware SE'de olduğu gibi virüsler hariç tüm yazılımları bulup etkisiz hale getirebiliyorsunuz. Oldukça kapsamlı bir program; son güncellenmiş haliyle birlikte 23.000'ne yakın yazılımı yakalayabiliyor. Türkçe versiyonunun olması nedeniyle de kullanışlı bir program olduğu söylenebilir. Diğer programlarda olduğu belirli aralıklarla güncelleştirmenizde yarar var. Programı etkili bir şekilde kullanabilmeniz için "Immunize" ikonunun altında yer alan "Enable permanent blocking of bad addresses in internet explorer" seçeneğinin işaretlenmiş olması gerekiyor.

Web Adresi: www.safer-networking.org

Ücreti: Ücretsiz

McAfee Internet Security Suite (Virus Scan, Personal Firewall Plus, Privacy Service ve Spam Killer): McAfee Internet Security Suite'in internet güvenliği konusundaki en iyi program olduğunu söylemeliyiz. Program, virüs, Truva atı, reklam iletileri ya da internet solucanları gibi tüm kötü niyetli yazılımlara karşı bir güvenlik çemberi oluşturuyor. Örneğin, McAfee Virus Scan seçeneği ile, Windows'unuzu her başlattığınızda virüs taraması yaptırabiliyorsunuz, program internete bağlandığınızda başta internet bağlantınız olmak üzere tüm gelen e-postaları, ek dosyaları (attachment), indirdiğiniz (download) programları tarı-

yor, program ayrıca isterseniz sizin belirleyeceğiniz bir zamanda da otomatik olarak tarama yapabiliyor. Bir casus yazılım ya da kritik bir web sayfasıyla karşılaştığında sizi uyarıyor, isterseniz uyarmasına gerek kalmadan silmesi yönünde de komut verebiliyorsunuz. Kendi kara listesinde yer alan web sayfalarına girmek istediğinizde ya da tehlikeli içerikler taşıyan haber gruplarına (mail groups) üye olmak istediğinizde sizi uyarıyor ya da izin vermiyor, belirli başlıklar taşıyan çöp postalarını ("Hi", "I Love You" gibi), daha size ulaşmadan engelliyor. Kişisel mahremiyetinize yönelik her türlü girişimi (şifrelerinizin kırılması ya da çalınması, web tarayıcınızın ya da sayfanızın değiştirilmesi-"Hack" edilmesi gibi) engelliyor. Daha bir çok önemli özelliği olan McAfee Internet Security Suite'i tercih etmenizi öneriyoruz.

Web Adresi: www.mcafee.com

Ücretii: 44.99 USD

Bitdefender Professional Plus: Program temel olarak bir antivirüs koruma programı, ancak bunun yanında Truva atları, internet solucanları ve çeviriciler için de tam bir güvenlik sağlıyor. Ayrıca, programın kendisini otomatik olarak da güncelleme seçeneği var. Programın, bilinen tüm virüsleri tanıdığını öne sürmesinin yanında, isminin çok duyulmamış olmasını da belirtmeliyiz. Ancak bu durumunda tabi, programın yeterince nitelikli/başarılı olmamasından mı, yoksa McAfee, Norton ve Kaspersky gibi bilinen antivirüs programlarının önüne geçememesinden mi kaynaklandığını bilemiyoruz.

Web Adresi: www.bitdefender.com,

www.dijitaltrend.com

Ücreti: 44.95 USD

Norton Internet Security (Personal Firewall, Antivirus ve Anti Spam 2004): Norton Internet Security, Norton'un güvenlik duvarı olan Personal Firewall, antivirüs programı olan Norton Anti Virüs ve antispam programı olan Norton Anti Spam programlarının tüm işlevlerini kapsıyor. Bilgisayarınıza bu programlardan herhangi birini ya da hepsini tek tek yüklemek yerine Norton Internet Security programını yüklemek daha kolay ve yararlı olacaktır. Program, antivirüs ve antispam özelliklerinin yanında (virüs taraması, internet solucanlarına karşı koruma, çöp postaları filtreleme gibi) örneğin, girmek istemediğiniz ya da kullanmak istemediğiniz tüm program, web sayfası ya da posta gruplarına karşı kişisel bir güvenlik çemberi gibi işlev görüyor. Örneğin, hangi web sayfalarına gireceğinize ya da web sayfalarının açılabileceğine siz karar/izin veriyorsunuz. Ayrıca, hızlı temizleme (Quick Clean) seçeneğiyle de girdiğiniz web sayfalarına ait üm izleri (adresleri vb) silebiliyorsunuz. Bu olumlu yanlarının yanında, yalnızca Internet Security'nin değil tüm Norton koruma programlarının bilgisayarınızı yavaşlattığını, Norton Anti Virüs'un bazı virüsleri yakalayamadığını ya da tanımlayamadığı bazı programlara da virüsmüş gibi davranıp örneğin otomatik olarak silebildiğini unutmamak gerekiyor. Norton AV, örneğin, istediğiniz şarkıları .mp3 olarak sıkıştırıp bilgisayarınıza yüklemenizi sağlayan bir dönüştürme programı olan Audio Catalyst'in ya da .pdf (Adobe Acrobat Reader) uzantılı dosyaları .doc (Word) uzantılı dosyalara dönüştürmenizi sağlayan PDFGrabber'ın kur (setup) dosyalarını virüsmüş gibi algılayabiliyor. Bu noktada, programa, örneğin bir çöp postayla ya da virüsle karşılaştığı anda ne yapacağına ilişkin olarak öncelikle size danışması gerektiğine yönelik komut vermek ("Ask me what to do" seçeneğini işaretlemek) yararlı olacaktır.

Web Adresi: www.symantec.com

Ücreti*:* 69.95 USD

Trend Micro/PC-cillin Internet Security: Program, virüslere, çöp postalara ve tüm casus programlara karşı güvenlik sağlıyor. Eğer etkin bir ağ virüsü bulunursa bilgisayarın etkilenmesini ve virüsün diğer bilgisayarlara yayılmasını engellemek amacıyla da internet bağlantısını bile kilitleyebiliyor. Programın yeni çıkan virüslere karşı kendisini otomatik olarak güncellemesi de olumlu bir özelliği. Hotmail kullanıcılarının PC-cillin tarafından korunduğunu da söylemeliyiz.

Web Adresi: www.trendmicro.com

Ücreti: 69.00 USD

Kaspersky AntiVirus Personal: Kaspersky Anti Virus, güncel işletim sistemlerinin tümünü, e-posta ağ geçidini ve güvenlik duvarını destekliyor, virüsün saldırabileceği her noktayı tarıyor. Program, etkin internet bağlantısı olan bir bilgisayarda her üç saatte bir kendisini otomatik olarak güncellemesiyle, üstelik internet bağlantısı kesildiğinde bu güncelleme işlemine daha sonra bağlantının sağlandığı an bıraktığı yerden devam etmesiyle (bu kullanıcılar için tasarruf sağlıyor) ve etkin durumdayken "sessiz sedasız kendi kendisine" çalışıyor olması nedeniyle bilgisayar kullanıcılarının tercih ettiği bir program. Ancak, McAfee Virus Scan ya da Norton Anti Virus kadar geniş bir virüs tanıma kapasitesinin olmaması olumsuz yönlerinden.

Web Adresi: www.kaspersky.com

Ücreti: 41.50 USD

Acronis Privacy Expert Suite 7: Bu program, özellikle işletim sistemi ve çeşitli uygulamalar tarafından kullanıcıdan habersiz olarak kaydedilen kişisel bilgileri ortadan kaldırıyor. Bu güvenlik programıyla, örneğin Windows tarafından kaydedilen gezindiğiniz web sayfaları, girdiğiniz parolalar (örneğin, üye olduğunuz bir sinema sitesine girerken kullandığınız şifreler) ve görüntülediğiniz belgeler gibi özel verilerin başkalarının eline geçmesini engellemiş oluyorsunuz. Program, özellikle gizliliğiniz, casus yazılımlar ve reklam pencereleri için ideal.

Web Adresi: www.acronis.com

Ücreti: 29.99 USD

Ashampoo WinOptimizer Platinum Suite 2: WinOptimizer Platinum Suite 2, temizlik ve güvenlik araçları ile Windows'unuzun yükünü hafifleterek sisteminizin daha hızlı, temiz ve güvenli olmasını sağlıyor. Program, temizlik modülleri (Drive Cleaner, Registry Cleaner ve Internet Cleaner) ve işlev modülleri (File Associator, IP Spam ve PopUps) başlıkları altında toplanabilir. Bu seçenekleri kullanarak, örneğin sabit diskinizdeki kullanılmayan ("artık" durumda bulunan) dosyaları bulup temizleyebilir, böylelikle de boş alan yaratabilirsiniz. Windows kayıt defterindeki kullanılmayan dosyaları saptayıp silebilir, böylece de sisteminizin daha hızlı ve güvenli çalışmasını sağlayabilirsiniz. Internet Cleaner seçeneğiyle de, internette gezinirken siz farkında olmadan sisteminize bulaşan ve güvenliğinizi tehdit eden bilgileri bulup silebilirsiniz. Program, eğer isterseniz bütün bu güvenlik işlemlerini tek komutla gerçekleştirmesi açısından kullanışlı, ancak bilgisayarınızda bir başka güvenlik yazılımı da varsa eğer (örneğin, Acronis Privacy Expert Suite ya da Norton Internet Security gibi) işlevini ve etkililiğini yitiriyor. Bu noktada, *bazı güvenlik programlarının, kendileri yüklendikten sonra bir başka güvenlik programının yüklenmesini engellediğini de* söylemeliyiz. Diyelim ki, bilgisayarınızın daha güvenli olmasını istediğiniz için iki antivirüs programın bulunmasını istiyorsunuz ve diyelim ki, bilgisayarınızda Norton Anti Virüs var. Bu durumda Norton Anti Virüs Kaspersky Anti Vi-

rüs'ün yüklenmesini engeller. Burada, mantıksal olarak ya da teknik açıdan bakıldığında, birbiriyle uyum sağlayan iki antivirüs programını (örneğin, Norton AV ve AntiVir Personal Edition) bilgisayarınıza yükleyebileceğinizi, ancak, bunun birçok açıdan çok riskli olacağını belirtelim.

Web Adresi: www.ashampoo.com

Ücreti: 49.99 USD

Internet ortamında mahremiyeti ve güvenliği sağlamanın çok güç olduğunu, hatta % 100 güvenlik sağlamanın da neredeyse olanaksız olduğunu söylemeliyiz. Ancak, yukarıda kısaca tanıtmaya çalıştığımız programlardan "Microsoft AntiSpyware", "Ad-Aware", "Spybot - Search & Destroy" ve "Spyware Blaster" programlarının virüsler dışındaki tüm kötü niyetli yazılımlar için başlı başına bir koruma çemberi oluşturacağını söyleyebiliriz. Başkaları tarafından sanki güvenlik paranoyanız varmış gibi algılanma kaygınızı bir yana bırakıp (sanki böyle bir paranoyanızın olması da kötü bir şeymiş gibi J) bu dört programı da bilgisayarınıza yüklemenizi öneririz. Bu programlardan hiçbiri birbirleriyle çakışmazlar dolayısıyla bilgisayarınıza zarar vermezler, üstelik birinin yakalayamadığı casus yazılımı ötekinin yakalıyor olması da önemli bir özellik, bir anlamda birbirlerini tamamlıyorlar. Bu programlara ek olarak, özellikle virüsler, truva atları ve çöp postalarla başa çıkabilmek için, internet güvenliği konusundaki en iyi iki program olan (tabi ki bizce) McAfee Internet Security Suite ve Norton Internet Security programlarından birini yüklemenizi öneririz. Ancak, McAfee'nin gerek sistem performansını düşürmemesi/yormaması ve gerekse örneğin casus yazılımlara karşı daha etkili olması nedeniyle Norton'un birkaç adım önünde olduğunu ve en azından bugün itibariyle (Mayıs 2005) bilişim dünyasındaki en iyi güvenlik programı (tabiî ki yine bizce) olduğunu söyleyebiliriz.

Bazı güvenlik programları kendilerini otomatik olarak güncellerken (auto update) bazı programları sizin belirli aralıklarla güncellemeniz (manuel update) gerekmektedir. Bu noktada, hangi güvenlik programını kullanırsanız kullanın, program(lar)ınızı belirli aralıklarla (örn., en geç on günde bir kez) güncellemenizin çok yararlı olacağını söylemeliyiz.

Kaynaklar

...(2004). Chip, Sayı: 6, 8, 9.

...(2004). Byte, Sayı: 7, 12.

...(2004). Pcnet, Sayı: 80.

...(2004). Pcworld, Sayı: 25.

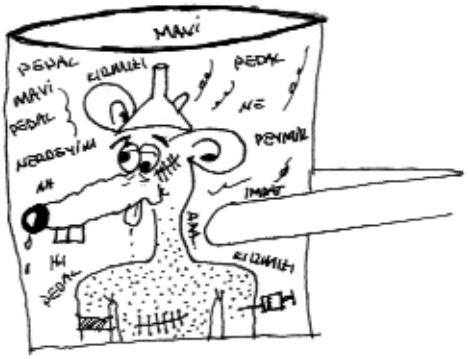
SELiM HOCA'NIN FARELERi

Prof. Dr. Selim Hovardaoğlu
Çizen: Ozan Hovardağolu

Artık herşeyin değiştiğini biliyor musunuz?

Bir zamanlar mutfak faresi..

..tarla feresi gibi çeşitli fareler vardı...



Sonra birgün labroseksüel fareler çıktı.

Ama durun...!
Şimdi günün trendi metroseksüel fare olmak!

Peki siz metroseksüel fare misiniz? Metroseksüel farelerin alışkanlıkları sizde var mı?
İşte bu sorulara yanıt bulmak için Selim Hoca'yı izlemeye devam edin...