Monitörden Yansıyanlar

Levent Daşkıran

Goner: Dostlukla Yayılan Tehlike

Fazla değil, daha birkaç ay önce bu sayfalarda Code Red virüsüne hayli geniş yer ayırmış ve yarattığı etkilerden uzunca bahsetmiştik. Bu ve ardından gelen daha tehlikeli Nimda gibi virüslerin aslında virüs dünyasına getirdiği yeni bir şey vardı: Bu ikili, virüslerin, klasik yayılma şekli olan bir dosyanın çalıştırılması ilkesinden daha gelişmiş bir yöntemle, sunucu yazılımlarındaki güvenlik açıklarını hedef alarak kendi kendine yayılıyorlardı. Bu yayılma biçiminin de virüs programcılarının bundan sonraki genel tercihi olacağı öngörülüyordu.

Lakin akıllanmayan taraf virüs programcıları mı, yoksa kullanıcılar mı, buna karar vermek zor. Geçen sene e-posta mesajları aracılığıyla yayılan Love Bug (bilinen adıyla I Love You) virüsünün bilgisayar sistemlerinde ne büyük hasarlar meydana getirdiği bazılarının kulağına küpe olmamış olacak ki, aynı prensiple yayılan Goner (Pentagone) virüsünün yine oldukça fazla can yaktığı söyleniyor. Bu tarz virüslerde genel prensip şu: Virüslü bir dosyayı ya da e-posta eklentisini, boş bulunup üzerine çift tıklayarak çalıştırdığınızda, virüs sizi ön planda bir şeylerle oyalarken, arka planda adres defterinizi talan etmeye başlıyor ve listenizden belirlediği sayıda kişiye kendisinin birer kopyasını gönderiyor. Kullanıcıların tuzağa düştüğü yer de aslında tam burası, çünkü virüslü dosyaların geldiği yer öyle tanımadığınız bilmediğiniz bir kişi değil. Tarık'ın bilgisayarına bulaşan virüs, Tarık'ın adres defterini talan ederken en iyi arkadaşlarından Levent'e de kendini gönderiyor, Levent "Tarık'tan bana zarar gelmez" deyip gelen e-posta eklentisini açtığında hop bu defa Levent'in üzerinden olay Mustafa'ya sıçrıyor. Mesajların ve dosya isimlerinin çiçek, böcek, sevgi mesajlarıyla süslü olması da karşılıklı güvenin yarattığı pozitif etkinin üzerine tuz biber. "Cehenneme giden yol iyi niyet taşlarıyla örülüdür" diye bir söz vardır hani, işte durum aynen öyle.

Goner ise geçen seneki Love Bug örneğindeki sevgi mesajlarını tuhaf bulmuş olacak ki, ilgi çekmek için sanki çok güzel bir ekran koruyucuymuş gibi davranmayı yeğliyor. Gelen mesaj "Hi" (Selam) başlığını taşıyor, mesaj gövdesinde de "How are you? When I saw this screensaver, I immediately thought about you. I am in a harry, I promise you will love it!" yazılı. Türkçe'si "Selam, nasılsın? Bu ekran koruyucuyu gördüğüm anda aklıma sen geldin. Şimdi acelem var, söz veriyorum görünce çok seveceksin" şeklinde bir şey (hurry değil, gerçekten de harry yazmışlar). Ekte gelen SCR uzantılı dosya ise UPX (Ultimate Packet for eXecutables) formatında sıkıştırılmış bir VBS, yani Visual Basic Script dosyası ve boyu 38K. Çalıştırıldığında sistem klasörleri altında kendi kopyalarını oluşturuyor ve her bilgisayar açıldığında çalışabilmek için başlangıç dosyalarının arasına yerleşiyor. Tabii Goner'in olaya kendi kattığı şeylerin sayısı az değil; Mesela sistemde mIRC adlı chat ve ICQ adlı online iletişim programları bulursa, yayılmak için e-posta mesajlarının yanında bunlardan da faydalanmayı ihmal etmiyor. En ilginciyse, sıkı durun, kodunda tanımlı olan 30'dan fazla firewall ve anti-virüs programı bulaştığı sistemde mevcutsa anında siliniyor. Silemezse, bir sonraki açılışta silinmeleri için ufak bir WININIT.INI dosyası oluşturup Windows'un başlangıçta çalıştırılacaklar listesine yerleştiriyor. Yani virüsün sisteminize bulaştığını anladığınız anda, anti-virüs yazılımlarınızın yerinde yeller estiğini görmeniz işten değil.

Korunmak için yapılacak şey belli: En yakınınızdan bile gelse, özellikle de içeriği İngilizce olan mesajlardaki ekli dosyalara karşı temkinli yaklaşın. Internet Explorer 6 ve Office XP altındaki Outlook 2002 sürümü e-posta virüslerine karşı bir koruma sağlıyorlar, ama sağladık dedikleri koruma, e-posta eklentilerinin ne olursa olsun açılmaması şeklinde olduğu için bana pek kullanışlı gelmedi. Hani insana sürekli virüs gelmez ya, arada önemli bir doküman falan da gelir. Koruma denilen şey onları da engelliyor...

Bir şekilde bu virüsün size bulaştığını düşünüyorsanız http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.removal.tool.html adresinden Symantec'in Goner temizleme aracını indirip kullanabilirsiniz. Bu arada Goner virüsünü yazanların 15-16 yaşlarında İsrail'li dört genç olduğunu ve suçlu bulunmaları halinde 5 yıla kadar hapis istemiyle Tel-Aviv'de bir hapishaneye koyulduklarını da dip not olarak ekleyelim. FBI'ın gençleri yakalamak için izlediği takip yöntemi de tam polisiye filmlere konu olacak cinsten. Gerçi polisiye filmler de zaten FBI hikayeleri üzerine kurulur ya...

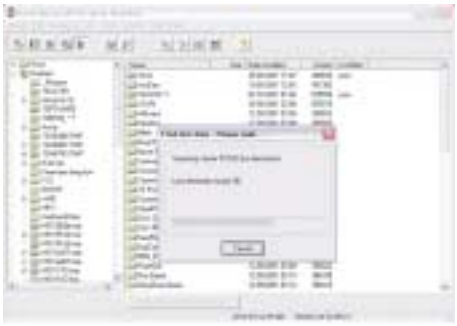
Soğutalım Ama...

Hatırlarsanız geçen ay ısınan PC bileşenleri için zararlı oluşundan dem vurup, aktif soğutma sistemlerinin devre dışı kalmasının ne gibi sonuçlar yaratabileceği konusuna bir video linki vermiştik (http://www4.tomshardware.com/cpu/01q3/010917/heatvideo-05.html#download_the_first_toms_hardware_test_lab_video). Bu ay elime geçen bir resimse, soğutma olayının evhamlı kullanıcılarca ne denli ciddiye alınabileceğinin bir örneği. Ancak bu kasadaki pervane sanmıyorum ki dönsün; yoksa ne masa üstünde monitör kalır, ne duvarda kapı... Hoş bir dizayn, güzel bir espri diyelim ve geçelim. Bu arada bir arkadaşımın "boru kullanarak ne güzel şeyler yapıyor insanlar" şeklinde olaya getirdiği yorum da oldukça yerinde...

levent_daskiran@hotmail.com

Sabit Diskten Veri Kurtarmak

Biliyorsunuz, ortalık virüs kaynıyor ve birçoğunun verdiği zarar da öyle hoş görülebilecek boyutlarda değil. Bunların kimisi sabit diskinizden veri siliyor, kimisi sabit diskinizin dosya ayırma tablosu olan FAT'ı silip dosyalarınızı erişilemez hale getiriyor, kimisi de hiç uğraşmayıp direkt formatla her şeyi acımadan yok ediyor. Düşünsenize; yıllardır topladığınız resimler, doküman arşiviniz, önem verdiğiniz dosyalar bir anda kendi dikkatsizliğiniz ya da bir kendini bilmezin yazdığı virüs yüzünden karanlıklara gömülecek. Eyvah, eyvah...



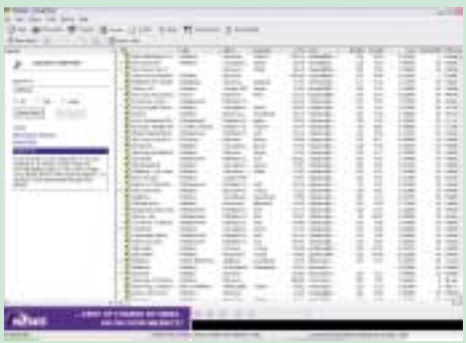
Sabit disklerinizdeki kayıp bilgileri Drive Rescue ile kurtarma şansınız var.

Ancak, sabit disk üzerindeki bilgiler manyetik plakalarda saklandıkları için, normalde bir dosyanın silinmesi, genellikle plakanın o noktasındaki manyetik olarak kaydedilmiş bilgilere ulaşmak için kullanılacak anahtarın silinmesi şeklinde gerçekleşir. Yani dosya silinir, ama üzerinde bir şeyler yazmadığınız sürece dosyalar sabit disk plakası üzerinde manyetik olarak saklanır. İşte bu sayede, en kötü durumlarda bile çoğu zaman üzerine başka bir şey yazılmadığı sürece bu manyetik kayda ulaşılıp dosyanın geri çağırılması mümkün. Peki nasıl?

Elbette bu işi yapan yazılımlar sayesinde... Genelde bunu yapan programlar ücretlidir, fakat bu ay editörü olduğum PC Magazine Türkiye dergisi için hazırladığım konu üzerine yaptığım bir araştırma sırasında ücretsiz olanına da rastladım. http://home.arcor.de/christian_grau/rescue/index.html Adresinden çekebileceğiniz Drive Rescue adlı yazılım, sabit diskinizi baştan aşağı tarayarak kendi kayıp, ama manyetik kaydı sağlam dosyaları bir bir bulup, kurtarılabilecek durumda olanları önünüze diziyor. Yazılımı sadece FAT tablosu bozulmuş veya format atılmış sabit disklerdeki verileri hayata döndürmek için değil, ayrıca çöp kutusundan sildiğiniz dosyaları geri getirmek için de kullanabiliyorsunuz. Mutlaka edinip iyi bir yerlere saklayın, benden şiddetle tavsiye. Değerini ancak lazım olduğunda anlarsınız.

KaZaA da mı Kazaya Kurban?

Müzik paylaşımının, MP3'le birlikte hayal bile edilemeyecek bir seviyeye gelmesi ve ufak dosyalar haline getirilen müzik eserlerinin telif falan dinlemeden kullanıcılar arasında paylaşılması, uzun zamandır RIAA'nın (Recording Industry Association of America-Amerikan Müzik Yapımcıları Birliği) canını sıkıp duruyordu. Sonuçta geçen sene MP3 dosyalarının kullanıcılar arası serbest paylaşımını esas alan Napster'a bir patladılar, pir patladılar. 1999 Yılında Sean Parker ve Shawn Fanning adlı 20 yaşlarında iki gencin kurduğu bu sistem, kullanıcıların birbirlerinin bilgisayarındaki müzik dosyalarını görerek doğrudan paylaşabilmeleri esasıyla çalışıyordu. 2000 Yılında haklarında RIAA tarafından dava açılıp 2001 yılının ortalarında faaliyetleri sonlandırılana kadar da, milyonlarca kullanıcılarıyla epey bir sükse yaptılar. Hatta bir ara Metallica ve Dr. Dre ile aralarında sıcak savaş bile yaşandı. Öte yandan, dava sırasında bu ikilinin anlaşma ile davayı sonuçlandırma karşılığı RIAA'ya 1 milyar dolar önermeleri de oldukça düşündürücüydü... Sonuçta RIAA Napster'i affetmedi, davayı kazanıp Napster'in faaliyetlerini durdurmanın ötesinde, bir de ceza davası açtı ve halen duruşmalar devam ediyor.



Faithless'e ait müzik parçalarının arama sonuçları. E tabii, şimdi RIAA buna dava açmasın da ne yapsın?

Ancak Napster'in dosya paylaşım yapısı olan P2P (Peer to Peer, Emsalden Emsale) öyle güzel bir fikirdi ki, hemen başka programlar tarafından da uygulamaya konuldu. Hatta, iş müzikle kalmadı, kısa zaman içinde her türden dosyayı paylaştıran 100 civarında program ortada boy gösterdi. Bu programların kullandığı P2P sistemi genel hatlarıyla şu şekilde çalışıyor: Ortada bir servis ve bu servise bağlı, ellerindeki dosyayı paylaşıma açmış kullanıcılar var. Kullanıcı bir dosyayı aradığında, sistem diğer kullanıcıların paylaşıma açtığı dosyalara bakıyor ve dosya bulunduğunda iki kullanıcı, birbirine bağlayarak aradan çekiliyor. Böylece dosya bir bilgisayardan diğer bilgisayara doğrudan aktarılıyor. İşte bu sistemin şu aralar en verimli altyapılarından biri FastTrack ve yapımcıları KaZaA isimli dosya paylaşım altyapısını yönetiyor. Ayrıca MusicCity ve Grokster adlı servisler de FastTrack altyapısını kullanıyorlar. Popülaritelerine gelince; şu anda bilgisayarıma yüklediğim KaZaA paylaşım yazılımının gösterdiğine göre, dosya paylaşımı yapan kullanıcı sayısı 501.057, paylaşımdaki dosya sayısı 71.915.000 ve bu dosyaların toplam boyutu 398.576 GB imiş. Fazla da söze gerek yok yani.

Her neyse, Amerikan mahkemeleri aracılığıyla Napster'a dava açıp uzunca bir hukuk süreci ardında onu güzelce çökerten RIAA, bu kez de Alman mahkemeleri aracılığıyla KaZaA'nın peşine düşmüş durumda. Aralık ayı içinde servisleri durdurması için KaZaA'ya ihbar çeken ve FastTrack sistemini kullanan diğer iki servisi de gözlem altına alan mahkemeye KaZaA'nın ertesi gün gönderdiği yanıt ilginç: "Yapamayız!". Neden olarak da, Napster'den farklı olarak kullanıcıların bir sunucu vasıtasıyla değil, birbirleri üzerinde bağlantı kurduğu gibi bir iddia sunuyorlar. Ayrıca şimdiye dek 18 milyondan fazla kullanıcının programlarını çektiğini ve bunları takip etmenin veya sınırlandırmanın mevcut sistemde mümkün olmadığını savunuyor. RIAA ise buna inanmıyor, lakin asıl sorun böyle teknik bir konuda kanıt yaratıp mahkemeyi ikna etmek.

Bana sorarsanız, bu işin artık durdurulamaz biçimde çığırından çıktığını ve durdurmak için harcanan emeklere yazık olduğunu düşünüyorum. Bugün bir servisi mahkeme dışında kapatmaya zorlayamıyorsunuz ve bu da Napster örneğinde 2 yıl sürdü. Oysa benzer bir diğer programın yazılması için geçen süre sadece birkaç gün. Bakalım RIAA bu işten ne zaman sıkılacak, alternatif üretenler sıkılacak gibi değil çünkü.

Önümüzdeki aylarda bu sayfalarda bilgisayarla ilgili merak ettiğiniz konular veya çok sorulan soruların cevaplandığı küçük bir köşe açmak niyetindeyim. Bu konudaki fikirlerinizi ve varsa dergide cevaplanmasını istediğiniz, bilgisayar teknolojileriyle ilgili soruları yukarıdaki e-posta adresime gönderebilirsiniz.