■ Umut AYTAR / Salih SEZEN ■ ■ Teknoloji

ilgisayar kullanımının artmasıyla birlikte, güvenliğini tehdit eden faktörlerde de büyük artış oldu. Özellikle şahsî bilgisayarlara(PC) yönelik saldırılar artık internete giren herkesin muzdarip olduğu bir mevzu. Saldırılardan korunmak için anti-virüs yazılımları kullanmak ya da sistem geri yüklemek en sık başvurulan yöntemlerden. Ancak sisteme giren bazı virüslerden kurtulmanın tek yolu bilgisayarı formatlamaktır. Peki, bütün bilgisayar kullanıcılarının dert yandığı bu virüslerin kaynağı nedir? Kimler tarafından, ne amaçla kullanılır?

Virüs kelimesinin asıl anlamı zehirdir. Bu ismin verilmesinin nedeni biyolojik virüslerle olan benzer-

likleridir. Her iki virüs de olabildiğince çoğalabilme yeteneğine sahiptir ve bulaştıkları yerlerde zarara vol açar. Biyolojik virüsler ile bilgisayar virüsleri arasında benzerlik olduğu kadar farklılıklar da vardır. Farklılıkların en belirgin olanı biyolojik virüslerin kesin kaynağının bilinememesidir. Bilgisayar virüslerininse kodlar vasıtası ile kaynakları bellidir.

İlk ne zaman ortaya çıktı?

Virüslerin kısa tarihine bakacak olursak, ilk ortaya çıkışının bilgisayarın tarihi kadar eski olduğu görebiliriz. Virüs sisteminin mantığı John Von Neuman adlı bilgisayarcı tarafından 1948 yılında ortaya atılmıştır. O da "kendi kendini kopyalayabilen bilgisayar programlarının vapılabileceği" görüşüdür. Bu görüş virüs sisteminin kaynağını teşkil etmiştir.

Ne tür virüsler vardır?

Birçok çeşidi bulunan virüslerin en önemlileri solucanlar ve Truva atlarıdır. Solucanların en önemli özelliği bir bilgisayardan diğerine otomatik olarak atlayabilme yeteneğine sahip olmalarıdır. Solucan bir bilgisayara bulaştığında önce dosyaların veya bilgi iletişim özelliklerinin denetimini ele geçirir ve kendi kendine ilerlemeye başlar. Mail ağına girip eposta defterinde bulunan herkesin bilgisayarına yayılabilir. Daha sonra bu yayıldıkları kişilere üzerinden yeni bilgisayarlara ulaşmaya çalışır. Sık görülen zararları internet hızını yavaşlatırlar ve kayıtlı dosyaları silerler.

Fayda sağlıyor gibi görünerek bilgisayara zarar veren Truva atı virüsü bilgisayar güncelleme sistemi, ağ güvenliği sağlama sistemi gibi programların içerisinde bilgisayara bulaşır. Son derece tehlikelidirler. Verebileceği zararlar arasında dosya kaybına yol açma, sistemi çökertme ve bilgisayar donanımında hasar oluşturma vardır

Nasıl bulasırlar?

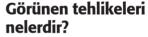
İnternetin icadına kadar virüsler bir bilgisayardan diğerine diskler vasıtası ile bulaşıyordu. Ancak günümüzde en etkili virüs vayılma volu internetten dosva paylaşımı ile karşımıza çıkmaktadır. Zararlı internet

> sitelerinin vanında e-posta voluyla bulasabilen virüsler de çok sık bir şekilde kullanıcıların başını ağrıtıyor. Bu yüzden internet kullanırken güvenilir olmayan sitelere girilmemeli ve şüpheli mailler açılmadan hemen silinmelidir.

Bir anti-virüs firmasının yaptığı analizlere göre şahsî bilgileri korsanların ulaşımına sunuyor.

Bu virüs bilgisayarınızda Windows'da, svchost.exe, Explorer.exe ve Services.exe gibi isimlerle karşınıza çıkabilir. Aynı araştırmanın sonuçlarına göre Conficker solucanının en büyük kurbanı %28,08'lik görülme oranıyla Ukraynalılar oldu. Ukrayna'yı Rusya (%18,69), Güney Afrika (%15,21) ve Bulgaristan (%15,02) izledi. Türkiye'de görülme oranı ise %5,98 düzeyindedir.

Microsoft'un yaptığı bir araştırmaya göre ise, güvenlik açısından en tehlikeli ülke sıralamasında Türkiye, Sırbistan Karadağ'ın ardından ikinci sırada yer almaktadır. Bu yüzden virüslere karşı bilinçlenmeli ve çok geç olmadan daha ciddi tedbirler almalıyız.



sayarlarda en çok karşılaşılan tehdit yüzde 8.85 ile "Win32/ Conficker" adlı solucan türüdür. Bu virüs önce Windows Otomatik Güncellestirmeler va da Windows Güvenlik Merkezi gibi sistem hizmetlerini devre dışı bıraktıktan sonra, ek bir yazılım indirip kullanıcının özel bilgilerine ulaşıyor ve bu bilgi-