Bilgisayar virüsü nedir?



www.yzokul.com.tr

Bilgisayar virüsü nedir?



Bilgisayarlar hakkında virüs kelimesini duymuşsundur. Bilgisayar virüsü, kendini diğer dosyalara veya programlara ekleyerek kopyalayan zararlı yazılımdır. Kısa cevap budur ve sana net bir başlangıç noktası verir. Sonraki sayfalar bu cevabın her parçasını sade bir dille açıklar, böylece virüsün ne olduğunu ve nasıl çalıştığını anlayabilirsin.



Yazılım, bilgisayarın izlediği talimatlar bütünüdür; sana adım adım ne yapacağını söyleyen bir tarif gibi. Bilgisayardaki programlar ve dosyalar yazılımdan oluşur. Yazılım olmadan bilgisayar ne yapacağını bilemez. Bunu anlamak, bir virüsün nerede saklanabileceğini ve nasıl davranabileceğini görmek için zemini hazırlar.



Zararlı, kasıtlı olarak zarar vermek veya istenmeyen şeyler yapmak için oluşturulmuş demektir. Yani zararlı yazılım, bir bilgisayara zarar vermek veya onu kötüye kullanmak için yapılmış yazılımdır. Sana yardım etmek için orada değildir; istemediğin bir şeyi yapmak için oradadır. Bu kelime önemlidir çünkü bilgisayar virüsü zararlı yazılım grubuna aittir.



Bilgisayar virüsü, özel bir hilesi olan bir zararlı yazılım türüdür: kendini kopyalar. Bunu diğer dosyalara veya programlara eklenerek yapar. Bu kopyalama, onu herhangi bir zararlı programdan çok virüs yapan şeydir. Yani virüs, zaten sahip olduğun şeylere yapışarak yayılan zararlı yazılımdır.



Virüsü, normal bir dosyaya veya programa yapışan küçük bir ek parça olarak düşün. Dosya hâlâ normal görünür, ama virüs onunla birlikte taşınır. O dosya veya program çalıştığında virüs de onunla birlikte gider. Bu ekleme, bir virüsün bir yerden başka bir yere taşınmasını sağlayan kilit harekettir.



Zararlı yazılım, zararlı yazılımların büyük ailesidir ve virüs bu ailenin yalnızca bir üyesidir. Başka üyeler de vardır; örneğin kendi yollarıyla yayılan solucanlar. Yani her zararlı program bir virüs değildir. Bunu hatırlamak, virüs kelimesini doğru kullanmana ve bir virüsü özel yapan şeyi anlamana yardımcı olur.



Bir virüs yalnızca eklendiği dosya veya program çalıştırıldığında harekete geçer. O zamana kadar sadece orada ekli durur. Çalışmaya başladığında dosyaları değiştirebilir veya başka zararlı eylemler yapabilir. Yani çalışma anı, virüsün bir şey yapma fırsatını yakaladığı andır. Bu yüzden bilinmeyen dosyaları açmak ve çalıştırmak riskli olabilir.



İşte somut bir örnek: çalışan bir virüs, bilgisayardaki dosyaları değiştirebilir veya onlara zarar verebilir. Bir belgeyi artık doğru açılmayacak şekilde değiştirebilir ya da bir programı tuhaf davranacak şekilde değiştirebilir. Bu dosya değişikliği, bir virüsün sorun çıkarma yollarından biridir. Zarar, çalışırken yaptığı değişikliklerden gelir.



Bir virüsün nasıl yayıldığı türüne bağlıdır. Bazı virüsler dosyalar aracılığıyla yayılır; bu dosyalar paylaşıldığında veya çalıştırıldığında bir dosyadan diğerine geçer. Diğerleri farklı şekillerde yayılır. Her virüse uyan tek bir kalıp yoktur. Yani bir virüs hakkında bir şey duyduğunda, türü sana muhtemelen nasıl hareket ettiğini söyler.



Bir virüsün ne yaptığı da türüne bağlıdır. Bazıları açılmayan bir dosya gibi küçük sorunlara yol açar. Diğerleri birçok dosyanın değişmesi veya kaybolması gibi daha büyük zararlara yol açar. Etkilerin hepsi aynı değildir. Yani her virüsün aynı şekilde davrandığını varsayamazsın; her türün kendi davranışı vardır.



Temel bir koruma adımı, yazılımını güncel tutmaktır. Güncellemeler, zararlı yazılımların kullanabileceği bilinen zayıflıkları giderir. Güncellemeleri yüklediğinde, bir virüsün açmaya çalışabileceği kapıları kapatırsın. Güncellemeyi düzenli bir alışkanlık haline getir ve programlarının ve işletim sisteminin üreticilerinin sağladığı düzeltmeleri almasına izin ver.



Bir diğer temel koruma adımı, dosyaları ve programları güvenilir kaynaklardan almaktır. Güvenilir kaynaklar, zararlı yazılım kapma olasılığını azaltır. Bilinmeyen bağlantılar yerine resmi web sitelerinden ve bilinen uygulama mağazalarından indir. Bir eki açmadan veya bir dosyayı çalıştırmadan önce nereden geldiğini ve o kaynağa güvenip güvenmediğini sor.



Yaygın bir hata, her zararlı programı virüs olarak adlandırmaktır. Bir virüsün daha büyük zararlı yazılım ailesi içinde yalnızca bir tür olduğunu unutma. Solucanlar ve başka türler vardır ve hepsi aynı şekilde çalışmaz. Doğru kelimeyi kullanmak, neyle karşı karşıya olduğunu ve ne tür bir korumanın mantıklı olduğunu anlamana yardımcı olur.



Bir diğer yaygın hata, bir virüsün kendi kendine bir şey yaptığını düşünmektir. Harekete geçebilmesi için bir dosyanın veya programın çalıştırılması gerekir. Enfekte dosya hiç açılmaz veya çalıştırılmazsa virüs etkin kalmaz. Yani neyi çalıştırdığın konusunda dikkatli olmak korumanın bir parçasıdır, çünkü virüs o anı bekler.



Tek bir kuralın tüm virüslere uyduğunu düşünmek de bir hatadır. Yayılma ve etkiler türe göre değişir, bu yüzden her durumu kendi içinde ele al. Dosyalar aracılığıyla yayılan bir virüs, başka bir şekilde yayılandan farklı davranabilir. Genel fikri öğren, sonra ayrıntıya ihtiyaç duyduğunda belirli türe bak.



Özetle: bilgisayar virüsü, kendini dosyalara veya programlara ekleyerek kopyalayan zararlı yazılımdır. Zararlı yazılımın bir türüdür ve eklendiği dosya çalıştırıldığında harekete geçer. Yayılma ve etkiler türe göre değişir. Kendini korumaya yardımcı olmak için yazılımını güncel tut ve güvenilir kaynaklar kullan.