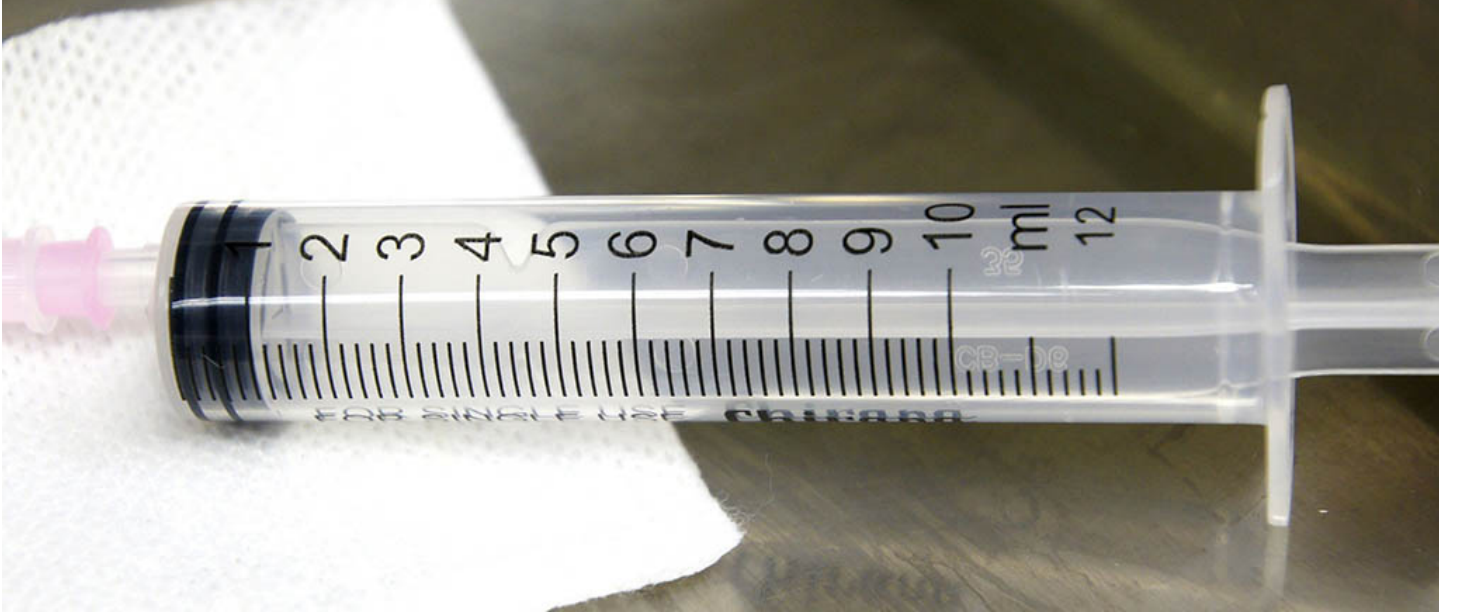


Kötücül Yazılımlar (Virüsler, Truva Atları, Solucanlar)

İnternette bireye ve kullanıcıya doğrudan veya dolaylı zarar veren birçok kötücül yazılım mevcuttur. Bu kötücül yazılımlara Malware ismi verilmektedir. Malware, "Malicious software"ın kısaltılması olan virüsler, truva atları, trojanlar ve istenmeyen diğer kötü niyetli yazılımların genel adıdır. Malwareler bilgisayar sistemlerine zarar vermek, bilgilerimizi çalmak ve diğer kötü amaçlı yazılımlardır. Bu kötü amaçlı yazılımları genel olarak bilgisayar virüsleri, truva atları, solucanlar, casus yazılımlar ve keylogger'lar olarak özetleyebiliriz.

İnternette bireye ve kullanıcıya doğrudan veya dolaylı zarar veren birçok kötücül yazılım mevcuttur. Bu kötücül yazılımlara Malware ismi verilmektedir. Malware, "Malicious software"ın kısaltılması olan virüsler, truva atları, trojanlar ve istenmeyen diğer kötü niyetli yazılımların genel adıdır. Malwareler bilgisayar sistemlerine zarar vermek, bilgilerimizi çalmak ve diğer kötü amaçlı yazılımlardır. Bu kötü amaçlı yazılımları genel olarak bilgisayar virüsleri, truva atları, solucanlar, casus yazılımlar ve keylogger'lar olarak özetleyebiliriz.



Bilgisayar virüsleri, bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini internet üzerinden diğer bilgisayarlara yayarak yavaşlamalara veya başka sorunlara neden olacak şekilde tasarlanmış yazılım programlarıdır. Virüsler, herhangi bir bilgisayara değişik yollarla girebilir ve bu bilgisayarlarda istenmeyen sonuç ve zararlara yol açabilir.

Bilgisayarınızda virüs olduğunu nasıl anlarsınız?

1. Bilgisayarınız olağan dışı şekilde yavaşladıysa,
2. Yeni ya da daha önce kullandığınız harici diskler artık çalışmıyorsa,
3. Ekranınızda garip ve çok sayıda mesajlar belirliyor,
4. Kullandığınız programlar çöküyor ya da çok yavaş çalışıyorsa,
5. Doküman ya da dosyalarınızın isimleri, dosya boyutları, kayıt tarihleri kendi kendine değişiyorsa,
6. İnternette dosya 'indirme' ve 'yükleme' hızınız çok düştüyse,
7. Monitörünüzde tuhaf hareketler oluyorsa DİKKAT!!!!

Virüslerden korunma yolları

- Bir dosya ekinde tam olarak ne olduğunu bilmedikçe, bilmediğiniz birinden gelen bir e-posta ekini asla açmayın.
- Bilgisayarınızda mutlaka anti-virüs programınız ve güvenlik duvarınız olmalı. Virüslerden korunmak için birçok anti-virüs programı bulunmaktadır. Örneğin; AVAST, NOD32, KASPERSKY, PANDA VE SYMANTEC vb. Bu programlar internet koruma paketi olarak güvenlik duvarı da bulundurabildiği gibi işletim sisteminizin de güvenlik duvarını kullanabilirsiniz.
- Virüslerden koruma yazılımınızı her zaman güncel tutun. Güncel olmayan anti-virüs yazılımları size hiçbir zaman bir yarar sağlamaz. Çünkü virüsler de kendini devamlı güncelliyor.
- Harddisk, cd, flashdisk vb. gibi donanımlara bilgi yüklemeyen veya bu donanımlardan bilgisayarınıza veri göndermeden önce bu donanımları anti- virüs yazılımları ile tarayın.
- İşletim sisteminizi devamlı güncel tutun ve orijinal (lisanslı) yazılım programları kullanın.
- Bilmediğiniz web sayfalarında çok fazla dolaşmayın ve bu sayfalardan çok fazla programı/dosyayı bilgisayarınıza indirmeyin. İndirdiğiniz dosyaları da muhakkak bilgisayarınızdaki anti-virüs yazılımları ile tarayın. Tek bir virüs programına bağlı kalmak istemiyorsanız aşağıdaki bağlantıdan indirdiğiniz dosyayı bu sayfanın sistemine yükleyerek tüm anti-virüs yazılımlarla tarama gerçekleştirebilirsiniz:

<https://www.virustotal.com/>

Ama şunu da unutmayın ki, bir anti-virüs yazılımı her virüsü bulup yok edemez. Bunun için gerekli tedbirleri önceden alınız.

Truva atı, yararlı gibi görünen ancak aslında zarara yol açan kötücül yazılımlardır. Mitolojideki Truva atı nasıl bir armağan gibi görünüp, aslında Troya kentini ele geçirecek askerleri taşıyordusa; bu truva atları da yararlı yazılımlar gibi görünen bilgisayar programlarıdır, Truva atları, eklendikleri program dosyasının çalıştırılması sonucu aktif olurlar ve kullanıcıların kopyalamasıyla yayılırlar. Normal virüsler gibi tespitleri kolay değildir. Etkilerini bulaştıktan sonra gösterirler. Truva atları, internetinizi yavaşlatabilir, bilgisayarınızdaki dosyalarınızı silebilir veya dosya üzerinde değişiklikler yapabilir.

Truva atlarından korunma yolları

- Tanımadığınız birinden bir e-posta alırsanız veya bilmediğiniz bir e-posta eki alırsanız kesinlikle açmayın. Bir e-posta kullanıcısı olarak mutlaka postanın kaynağını teyit edin.
- E-posta ayarlarınız yaparken eklerin otomatik olarak açılmayacağından emin olun. Bazı e-posta servis sağlayıcıları kendi bünyesinde ekleri açmadan önce virüs taraması yapılmasını sağlayan programlar sunar.
- İşletim sistemleri kullanıcılarını kesin tehditlerden korumak için güncellemeler yayınlarlar. Microsoft gibi yazılım geliştiriciler, truva atı veya virüslerin kullanabilecekleri açıkları kapatabilmek için yamalar (güncellemeler) yayınlarlar. Eğer sisteminizi bu yamaları kurarak güncel tutarsanız bilgisayarınız daha güvenli olacaktır.
- Peer to peer (P2P) veya yerel ağı paylaşan µTorrent, Kazaa, Limewire, Ares ve Gnutella gibi programların kullanımının kısıtlanması faydalı olur. Çünkü bu programlar genellikle virüs veya truva atı gibi programlarının yayılması konusunda korumasızdır.

Solucan da, diğer zararlı yazılımlar gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır; ancak bunu truvalardan farklı otomatik olarak yapar. Truva virüsü bilgisayara girdiğinde hangi programla girmişse o programın açılmasını bekler, program açılmazsa truva atı bilgisayarda aktifleşemez. Ayrıca, Truva atı direk bilgisayarın işletim sistemine zarar verir. Solucan ise zarar vermez sadece girdiğiniz siteleri, girdiğiniz kullanıcı adı ve şifreleri, indirdiğiniz programları, yani bilgisayarda yaptığınız her şeyi programcısına rapor olarak bildirir. Solucan ilk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteminize girdikten sonra kendi başına ilerleyebilir. Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir. Örneğin bir solucan, e-posta adres defterinizdeki herkese kopyalarını gönderebilir ve sonra aynı şeyi onların bilgisayarları da yapabilir. Bir solucan genellikle kullanıcı eylemi olmaksızın yayılır ve kendisinin tam kopyalarını (olasılıkla değiştirilmiş) ağlardan ağlara dağıtır. Bir solucan bellek veya ağ bant genişliği tüketebilir, bu da bilgisayarın çökmesine yol açabilir.

İnternetteki Solucan Örnekleri

İnternette sörf yaparken karşımıza çıkan küçük pencerelerde ilgi çekici şeyler bulunmaktadır. Bunlara tıkladığımızda web tarayıcınız solucan virüsü taşıyan dosyalar indirir. Tıkladığımız andan itibaren virüs bilgisayarımızda etkinleşir. Bazı penceredeki veya e-postanıza gelen yazıların örnekleri:

1. Tebrikler Sitemize giren 1.000.000. kişisiniz. Bizden çeşitli hediyeler kazandınız.
2. Tebrikler Amerika'ya iki haftalık seyahat hakkı kazandınız.
3. Bu soruyu bilin çekilişte çeşitli ödüller sizin olsun.

Yazımızın devamı için;

<https://www.guvenliweb.org.tr/dokuman-detay/kotucul-yazilimlar-2-casus-yazilimlar-keyloggerlar-botnetler>

ETİKETLER

[#KötücülYazılımlar](#)