ZARARRLI YAZILIMLAR

BİLGİSAYAR VİRÜSLERİ

Virüsler en genel ifade ile bilgisayarınıza, programlarınıza, dosyalarınıza değişik şekillerde zarar verebilen, düzgün çalışmalarını engelleyen bilgisayar programlarıdır. Virüsler;

I. Kendilerini kopyalayabilir.
II. Mail olarak başkalarına gönderebilir
III. Herhangi bir durumda ya da tarihte kendini aktif yapabilir.

Dünyanın ilk bilgisayar virüsü bir öğrenci deneyi olarak yazılmıştı, bugün ise piyasada 60,000virüsün bulunduğu tahmin ediliyor.

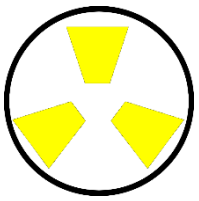
CREEPER VİRÜSÜ

Creeper Virüsü

* 1 971 yılında kayıtlara ilk bilgisayar virüsü olarak geçmiştir.
* ARPANET'deki bilgisayarlara bulaşmıştır.
* Bulaştığı bilgisayara herhangi bir zarar vermeyen Creeper asıl zararını, programcıları virüs mantığıyla tanıştırarak vermiştir.

ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı), Birleşik Devletler Savunma Bakanlığı bünyesine bağlı ARPA (Gelişmiş Savunma Araştırmaları Projeleri Birimi) tarafından geliştirilen dünyanın ilk paket dağıtımı ağı ve evrensel İnternet'in öncülüdür.

ÇERNOBİL VİRÜSÜ



* 1 998 yılının Haziran ayında Tayvan'da ortaya çıkmış ve çok kısa bir sürede tüm dünyaya yayılmış,
* Dünya genelinde yaklaşık 20 ila 80 milyon dolar zarara yol açmış, birçok bilgisayardaki önemli bilgileri yok etmiştir.
* Windows işletim sistemindeki hayati dosyalara zarar vermiş ve sistemlerin çökmesine sebep olmuştur.
* Ayrıca açılış dosyalarına da zarar vermiştir.
* Bir oyunun demo sürümünün içine de sızan virüs bu demo sürümle de yayılmıştır.
* Çernobil nükleer santralinin patlaması sonucu çevreye verdiği zarara benzetilmesi sebebi ile de çernobil virüsü diye anılmıştır.

MELİSA VİRÜSÜ

* 1 999 yılında ortaya çıkan **Melissa** virüsü ise elektronik posta yolu ile bulaşmıştır.
* İlk olarak 26 Mart 1 999 yılında görülmüştür.
* "İşte aradığınız belge... Bu belgeyi sakın kimseye gösterme ;-)„.
* Mesajı içeren bir elektronik postada ekli. DOC uzantılı bir kelime işlemci dosyasının açılması ile bulaşan ve otomatik elektronik posta yollayan virüstür.

* 2003 yılından sonraki kelime işlemci programları virüsten etkilenmemiştir.

I LOVE YOU VİRÜSÜ

* 2000 yılında ortaya çıkmıştır.
* **Loveletter (Aşk mektubu)** olarak da bilinen virüs, elektronik postalara eklenen **"Love- Letter-For-You.TXT.vbs."** adlı programın çalıştırılması ile bulaşmış, elektronik posta uygulamasının adres defterindeki kişilere kendini gönderen virüstür.
* ILOVEYOU virüsünün yaklaşık olarak 1 0 ila 1 5 milyar dolar zarara neden olduğu sanılmaktadır.

CODE RED SOLUCANI

* Bir bilgisayar worm'u olarak bilinen ve ağ sunucuları üzerinde yayılan Code Red, ilk olarak 2001 yılında görüldü.
* Oldukça tehlikeli olan bu solucanın amacı ise web sunucusunun zayıf noktalarını tespit edip zarar vermekti.
* Bady ismiyle de bilinen Code Red, sunucunun web sayfalarında ise şu mesajı yayınlamıştır. **"HELLO! Welcome to http://www.worm.com! Hacked by Chinese!."**
* 400.000 kadar sunucuyu etkilediği sanılan Code Red, kısa sürede bir milyondan fazla bilgisayara sızmayı başarmıştır.

BAGLE VİRÜSÜ

* 8 Ocak 2004 tarihinde ilk kez görülmüş,
* On milyonlarca dolar zarara neden olan ve sayısız PC'ye sızmayı başarmıştır.
* Bagle, elektronik postalardaki dosyaları kullanarak yayılmaya çalışmıştır.
* Bagle'ın en kötü tarafı 60 ila 1 00 kadar türevinin olmasıydı.
* Diğer bir deyişle Bagle'ın virüs tarayıcılara yakalanması pek kolay değildi.
* PC'lere sızan Bagle, veri ve uygulamalara kolayca ulaşabiliyordu.
* Finansal ve kişisel bilgiler dâhil hemen her veriye eli uzanabilen bir virüstür.
* Bagle. B türevinin yayılması 28 Ocak 2004 tarihinden itibaren durduruldu.
* Ancak Bagle'ın diğer türevleri hâla tehdit unsuru olmayı sürdürüyor.

Bagle Virüsü

SASSER VİRÜSÜ

* 30 Nisan 2004 tarihinde görülmüştür.
* Havayolu şirketlerine kadar ulaşmış uçuşların ertelenmesine sebep olmuştur.
* Klasik solucanların aksine, elektronik postaları kullanmayan Sasser, güncel olmayan işletim sistemlerinin güvenlik açıklarını kullanmıştır.
* 17 yaşındaki bir Alman lise öğrencisi tarafından yazılan ve 18. yaş gününde yaymaya başladığı Sasser'ın yarattığı zarar öylesine büyük oldu ki bu Alman genci bilgisayarlara karşı sabotajda bulunduğundan dolayı hapis cezasına mahkûm edildi.

CRYPTOLOCKER VİRÜSÜ

* İlk olarak 2013 yılında ortaya çıkmıştır.
* Fidye isteyen kategoride (ransomware) bir zararlı yazılımdır.
* Virüs, şifrelediği her bir klasöre ve kullanıcı masaüstüne "SIFRE_COZME_TALIMATI. html" benzeri bir dosya eklemektedir.
* Bu web sayfası şeklindeki dosya bilgisayardaki dosyaların özel bir program ile şifrelendiğini, dosyaları kurtarmanın tek yolunun şifre çözen programı satın almak olduğunu belirtmiştir.
* Virüsün dosyaları şifrelemesi durumunda, yapılabilecek çok fazla seçenek bulunmadığından önemli olan husus virüsün bulaşmasını engellemektir.

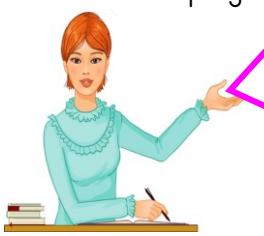
KORUYUCU YAZILIMLAR VE KULLANIM AMAÇLARI

GÜVENLİK DUVARI

- Güvenlik duvarı bilgisayarımızın veri trafiğini kontrol eden bir yazılım ya da donanımdır.
- Güvenlik duvarı kullanmak en temel koruma yöntemlerindendir.
- Bazı işletim sistemlerinde güvenlik duvarı uygulaması işletim sistemi ile gelmektedir.
- Uygulama cihazınızı yavaşlatsa dâhi, uygulamayı durdurmamak ve güncellemek önemlidir. Çünkü bu yazılımlar, yetkisiz kullanıcıların ve solucanların bilgisayara girişini engelleyip istenmeyen trafiği engelleyerek bilgisayarları korur.
- Güvenlik duvarı sadece bireysel kullanıcılar tarafından değil daha gelişmiş güvenlik önlemlerine ihtiyacı olan kurumlar tarafından da kullanılır.

ANTİVİRÜS PROGRAMLARI NELER YAPAR?

- Bilgisayarınızı zararlı yazılımlara karşı korur ve mevcut zararlı yazılımları tespit eder. Mümkünse siler, silemezse de karantinaya alır.
- Bazı virüsler dosyalara da bulaşır.
- Antivirüs programları virüslerin dosyalarınıza bulaşmasını engeller.
- Başkasına ait taşınabilir bir belleği bilgisayara takmadan önce virüs taraması yapmak önemlidir. Tarama sonucu her zaman zararlı yazılımı bulamayabilir. Çünkü, antivirüs programları tüm virüsleri tanımayabilir. Virüsleri temizlemek için virüslerin antivirüs programlarında tanımlı olmaları gerekir.
- Güncelleme ile antivirüs programlarının etki alanı genişletilebilir.
- E-posta yolu ile aldığınız dosyaları açmadan önce de virüs taraması yaparak bilgisayarınızı koruyabilirsiniz.
- İnternette gezinirken, siber saldırıya uğrayabilirsiniz.
- Antivirüs programları; gizliliği arttırarak internette gezinmenizi güvenli hâle getirmeye, bunu yaparken de bilgisayar performansını üst seviyede tutmaya çalışır.
- İnternette en sık karşılaşılan sorunlardan biri istemediğiniz bir sayfada gezinirken istemsiz başka bir sayfaya yönlendirilmek ve gezinmeyi engelleyecek reklamların açılmasıdır.
- Antivirüs programları bu durumlarla da mücadele etmeye çalışır.
- Antivirüs programları size, parola bilgilerinizi güvenli tutabileceğiniz araçlar sunar.
- Antivirüs programları, kapsamlı güvenlik durumu raporlaması sağlar.
- Kötü amaçlı eylemleri sonlandırmanızı sağlar bazen zararlı yazılımların verdiği zararları geri almaya çalışır. Bozulan içeriğin onarılması buna bir örnektir.
- Akıllı işaret (kare barkodlar, karekodlar) bağlantılarının güvenliğini denetlerler.
- Bilgisayarlar gibi akıllı telefonlar da zararlı yazılımlardan korunmalıdır.
- Antivirüs programları, yazılımların ağ bağlantılarını engellemesinin önüne geçmeye çalışır.



Sonuç olarak,

- Antivirüs programları cihazlarımızı korumamızda çok önemli yardımcılardır. İşlerini daha iyi yapabilmeleri için sıkça güncellenmeleri gerekir.
- Güvenli sitelerden elde edilmeyen antivirüs yazılımlarının bile virüs içerebileceğini unutmayalım.

ZARARLI YAZILIMLAR; AMAÇLARI, BULAŞMA ŞEKİLLERİ, VERDİKLERİ ZARARLARIN BOYUTLARI GİBİ BİRÇOK ÖLÇÜTE GÖRE GRUPLANABİLMEKTEDİR.

* Bilgisayarınızdaki bilgileri çalabilir ve başkalarına gönderebilirler.E-posta hesaplarınız, parola bilgileriniz gibi.
* İşletim sisteminizin veya diğer programlarınızın çalışmamasına,hatalı çalışmasına neden olabilirler.
* Bilgisayarınızdaki dosya veya klasörleri silebilir,kopyalayabilir,yerlerini değiştirebilir veya yeni dosyalar ekleyebilirler.
* Yaptığınız her şeyi kaydedebilirler.Klavyede yazdığınız her şey veya fare ile yaptığımız tüm hareketler gibi.
* Ekranda can sıkıcı veya kötü amaçlı web sitelerine yönlendiren açılır pencereler oluşturabilirler.
* Tüm verisiyle diski silebilir, hatta biçimlendirebilirler.
* Saldırganların kullanması için güvenlik açıklıkları oluşturabilirler.
* Başka zararlı programların bulaşmasını sağlayabilirler.
* Bilgisayarınız üzerinden başkalarına saldırabilirler.
* Bilgisayarınızın ya da internetin kaynaklarını kullanır, yavaşlamalara neden olabilirler.