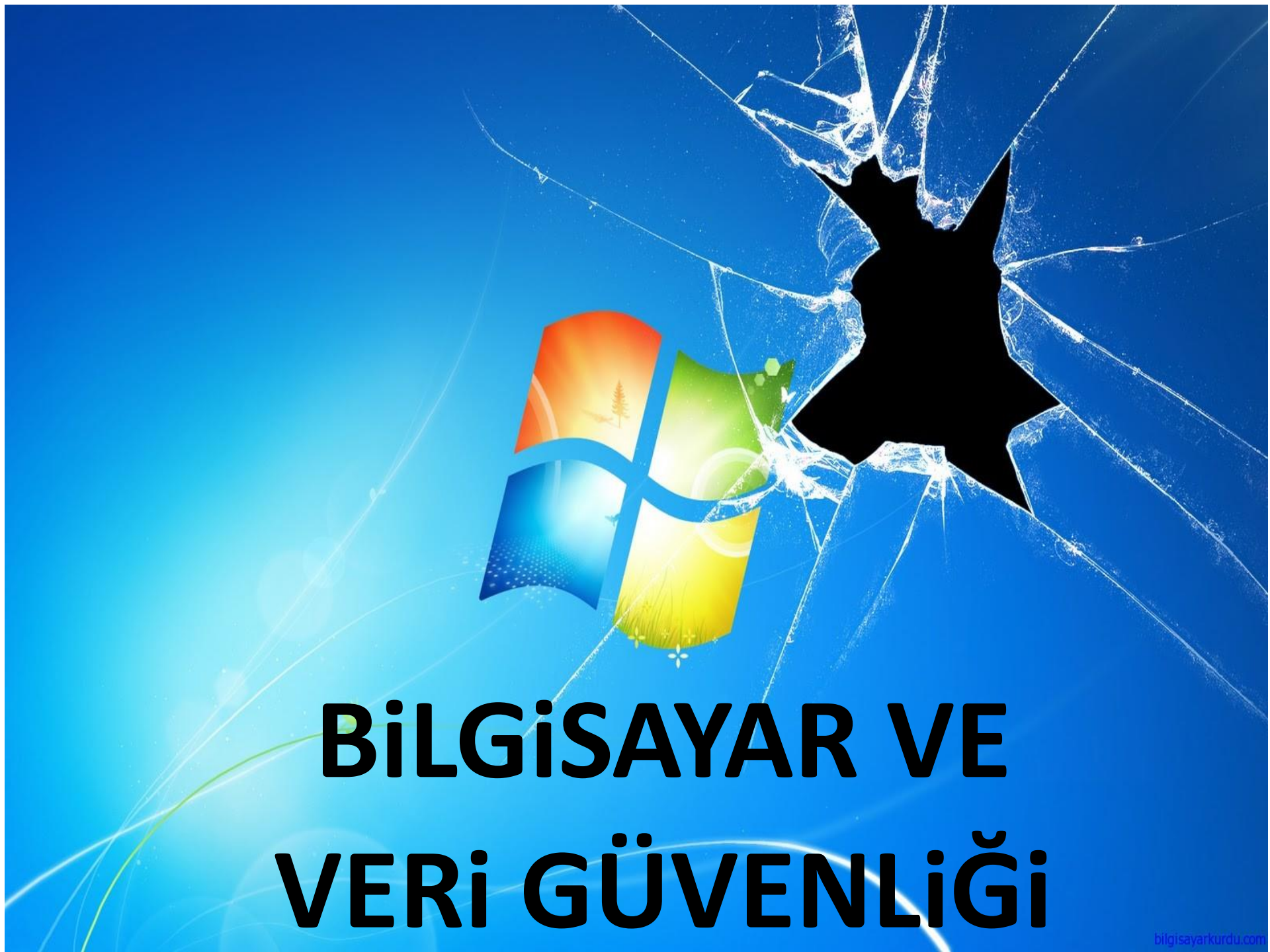


BiLGiSAYAR VE VERi GÜVENLiĞi

VERİ NEDİR? BİLGİ NEDİR?

- Veri bilginin işlenmemiş hali yani ham hali, Bilgi ise verinin işlenmiş haline denir.
- Veri bazı işlem ya da işlemlerden geçerek bilgiye dönüşmektedir.

- Örneğin, öğrenciler hakkındaki veri, soyadlarına göre alfabetik olarak düzenlenebilir. İşlenen veri bilgiye dönüşünce, karar vericiye yararlı olması için kısaltılabilir ve özetlenebilir.

BİLGİ VE VERİ GÜVENLİĞİ,

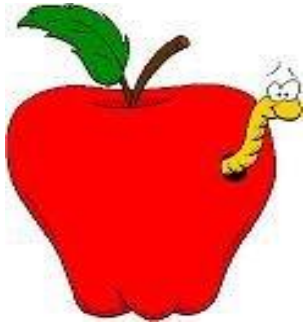
- Bilginin «izinsiz» veya «yetkisiz» bir biçimde erişimi, kullanımı, değiştirilmesi, ifşa edilmesi, ortadan kaldırılması, el değiştirmesi ve hasar verilmesini «önlemek» olarak tanımlanır.

- Disk, iletişim ağı, yedekleme ünitesi ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasını ifade eder.

VERİ GÜVENLİĞİNİN ÜÇ TEMEL BOYUTU

Veri güvenliğinin 3 temel boyutu bulunmaktadır:

"gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti olur.



- **Gizlilik:** Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.

- **Bütünlük:** Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

- **Erişilebilirlik:** Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

VERİ GÜVENLİĞİNİ TEHDİT EDEN KAYNAKLAR;

- Teknik saldırılar (kötü amaçlı yazılımlar)
- Kötü niyetli kişi saldırıları (hacker)
- Sistem hataları (donanım arızaları ve kullanıcı hata
- Yangın, su baskını, terör gibi dış etkenler

VERİ GÜVENLİĞİNİ TEHDİT ETME SEBEPLERİ

- Para hırsızlığı
- Yazılıma zarar verilmesi
- Bilgi çalınması
- Bilgiye zarar verilmesi
- Servislerin izinsiz kullanılması
- Zarar vermeden güvenlik ihlali
- Sistemlerin kısmen veya tamamen devre dışı kalması

BİLGİ GÜVENLİĞİ FARKINDALIĞI OLUŞTURULMASININ 10 ALTIN KURALI

- Dikkat ve farkındalık
- Belirli periyotlarla bilgileri yedekleme ve yedeklenen bilgileri güvenli alanlarda tutma
- En az 20 karakterden oluşan şifreler kullanma ve bunları belirli periyotlarda güncelleme
- Yeni güvenlik yaklaşımlarının takip edilip uygulanması,
- Güvenliği sağlamada anti-virüs, anti-spam, anti-casus ve güvenlik duvarı gibi çözümlerin kullanılması ve bunların güncel tutulması
- Bilinmeyen veya anlaşılmayan hususlar konusunda şüpheci olunması ve uzmanlardan destek alınması,

BİLGİ GÜVENLİĞİ FARKINDALIĞI OLUŞTURULMASINDA 10 ALTIN KURAL

- Kullanılmayan bilgilerin sistemlerden kaldırılması sadece ihtiyaç duyulan bilgilerin elektronik ortamlarda barındırılması, ihtiyaç olmayan yazılımların bile sistemlere yüklenilmemesi
- Elektronik ortamları kolaylıkla takip edilebilir ve izlenebilir ortamlar olduğunun her zaman hatırda tutulması
- Konu ile ilgili olarak kullanıcıların bilgilerini artırmaları
- Sahip olunan bilgi varlıklarının gerektiği gibi korunması veya paylaşılmaması ve başkalarının bilgilerini izinsiz kullanmama ve sistemlerine izinsiz girilmemesi gerektiği ve bunun da suç olduğunun hatırlanması

SALDIRI YÖNTEMLERİ

KÖTÜ AMAÇLI YAZILIMLAR (MALEWARE)

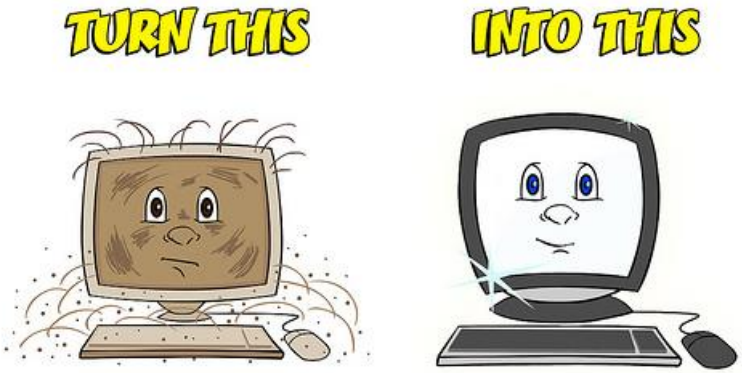
Kullanıcı bilgisi veya izni olmadan bir bilgisayara sızmak ve muhtemelen zarar vermek için tasarlanmış kod parçalarıdır.

1. **Virüs** (virus),
2. **Casus** (spyware),
3. **Korku** (scareware),
4. **Reklam** (adware),
5. **Truva atı** (trojan horse),
6. **Solucan** (worm),
7. **Rootkit** ve diğer tiplerde istenmeyen yazılımlar bu kapsamdadır.

KÖTÜ AMAÇLI YAZILIMLAR (MALEWARE)

- İkinci aşama ise sisteme bulaşan bir zararlı yazılımın tespit edilmesi, kaldırılması veya karantinaya alınmasıdır.

- Öncelikli önlem bu yazılımların sisteme bulaşmasını önlemektir.



- Kötü amaçlı yazılımlar ile mücadele etmek için mutlaka uygun ve güncel güvenlik yazılımları gereklidir.

1- Bilgisayar Virüsleri

- Kullanıcının bilgisi haricinde bilgisayarda çalışan bir koddur.
- Dosyalara veya makro gibi kodlara bulaşırlar.
- Koda erişildiğinde ve çalıştırıldığında bilgisayara bulaşmaktadır.
- Virüsler çoğalabilme yeteneğine sahiptir ve kendilerini bilgisayarın her yerine bulaştırabilirler.
- Virüs bulaşan dosyalara diğer bilgisayarlar tarafından ulaşıldığında virüs diğer sistemlere de bulaşabilir.
- Her türlü zararlı yazılıma yanlış bir algılama ile virüs denilmektedir.

Virüs Belirtileri

- Bilgisayarın normalden daha yavaş çalışması
- Normal olmayan hata mesajları
- Antivirüs programlarının çalışmaması
- Bilgisayarın sık sık kilitlenmesi
- Bozuk görüntü veya bozuk baskılar
- Tuhaf sesler oluşması
- Sabit diskin sürekli kullanımda olması
- Bilgisayarın istem dışı davranışlarda bulunması
- Disk sürücüleri veya uygulamaların doğru çalışamaması
- Simgelerin kaybolması veya yanlış görünmesi
- Veri dosyalarının artan sayıda bozuk çıkması
- Otomatik olarak oluşturulmuş klasörler ve dosyalar

2- Casus Yazılımlar (Spyware)

Spyware = Spy + Software

- Spyware farkında olmadan bir web sitesinden download edilebilen veya herhangi bir üçüncü parti yazılım ile birlikte yüklenebilen kötü amaçlı bir yazılım tipidir.
- Genelde, kullanıcının izni olmaksızın kişisel bilgilerini toplar.
- Herhangi bir kullanıcı etkileşimi olmaksızın bilgisayar ayarlarını değiştirebilmektedirler.
- Çoğunlukla web reklamları ile bütünleştirilmiştir.
- En belirgin bulgusu, tarayıcı açılış sayfasının değiştirilmesidir.
- Özellikle ücretsiz yazılım araçlarının kurulumlarına dikkat edin.

Spyware Belirtileri

- Web tarayıcının açılış sayfasının sürekli değişmesi
- Her arama yapılmasında özel bir web sitesinin açılması
- Aşırı derecede popup penceresi görüntülenmesi
- Ağ bağdaştırıcısının aktivite LED'inin veri aktarımı olmadığı anlarda bile yoğun aktivite göstermesi
- Kendiliğinden çalışan yazılımlar
- Firewall ve/veya antivirüs programlarının kapanması
- Yeni programlar, simgeler ve sık kullanılanların kaybolması
- ADSL kotanızın beklenenden çok fazla kullanılmış olması

3- Korku Yazılımları (Scareware)

- Yeni bir saldırı türüdür.
- Amacı sizi korkutarak para kazanmaktır.
- Genelde bilgisayarınız pek çok virüs tarafından ele geçirildiğini ve temizlenebilmesi için belirli bir yazılıma lisans ücreti ödemeniz gerektiğini söylenir.

4- Reklam Yazılımları (Adware)

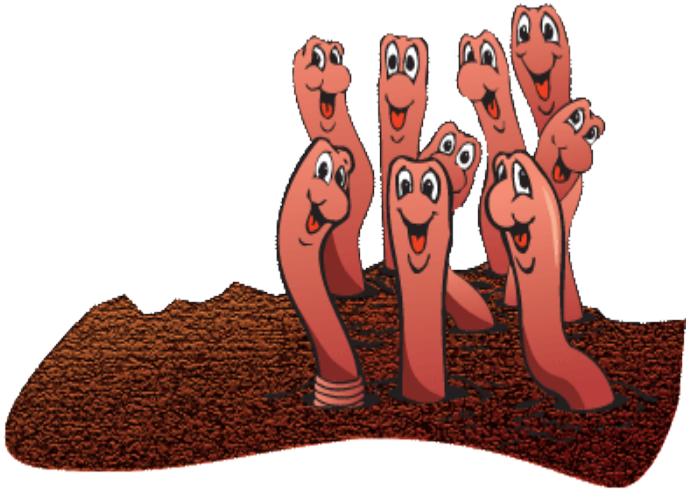
Adware = Advertisement + Software

- Reklam amaçlı yazılımlardır.
- Bu reklamlar genelde popup (açılır pencere) şeklindedir.
- Bilgisayara zarardan çok kullanıcıya sıkıntı veririler.
- Genelde bilgisayara casus yazılımlarla birlikte bulaşırlar.

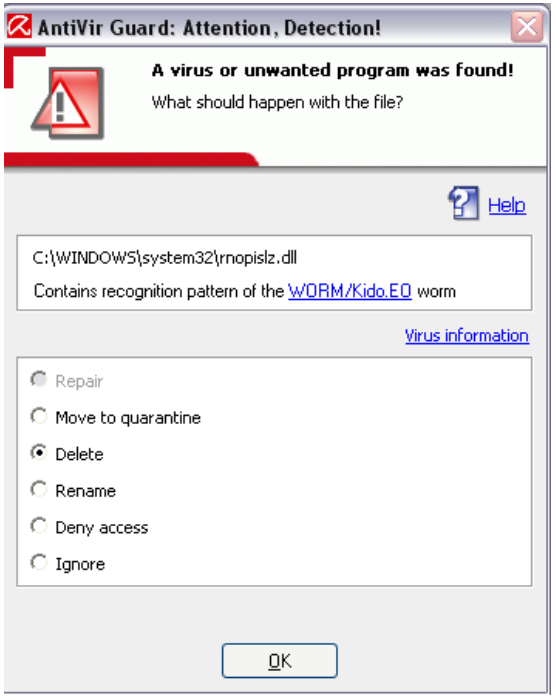
5- Truva Atları (Trojan Horses)

- Görüntüde istenilen fonksiyonları çalıştıran, ancak arka planda kötü amaçlı fonksiyonları da gerçekleştiren yazılımlardır.
- Bunlar teknik olarak virüs değillerdir ve farkında olmadan kolayca download edilebilirler.
- Saldırgana sistemin sahibinden daha yüksek ayrıcalıklar tanıyan ve çok tehlikeli sayılacak becerilere sahip olan trojanlar vardır.
- Truva atları, ücretsiz olarak yüklediğiniz yazılımlarla bir arada da gelebilir.
- Crack Yazılımlarına dikkat!!!

6- Solucanlar (Worms)

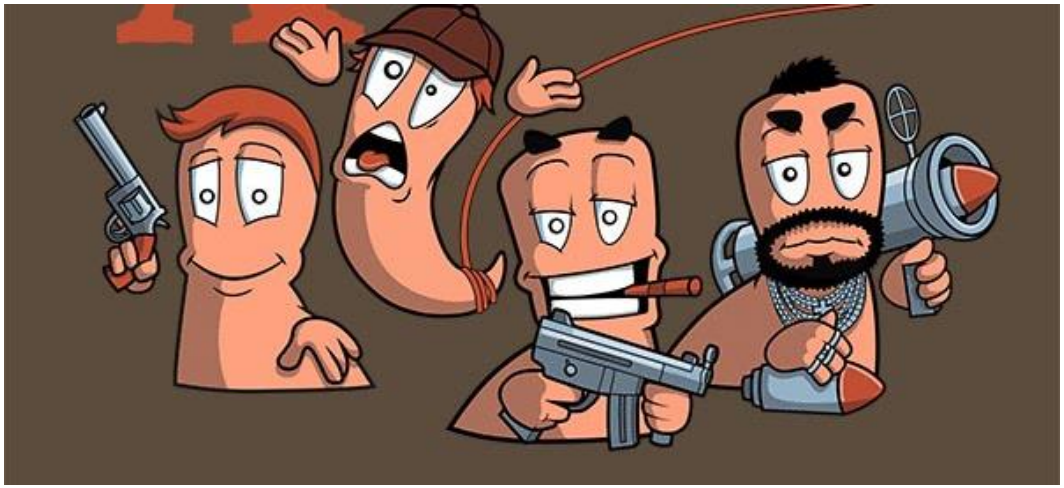


- Solucanlar, uygulamalar ve işletim sistemindeki güvenlik açıklıklarından ve arka kapılardan yararlanır.
- Solucanlar çalışmak için kullanıcıya gereksinim duymazlar.
- Daha çok ağ paylaşımları ve toplu e-mailler ile yayılırlar.
- Virüsler ile arasındaki fark, kendilerini çoğaltamamalarıdır.

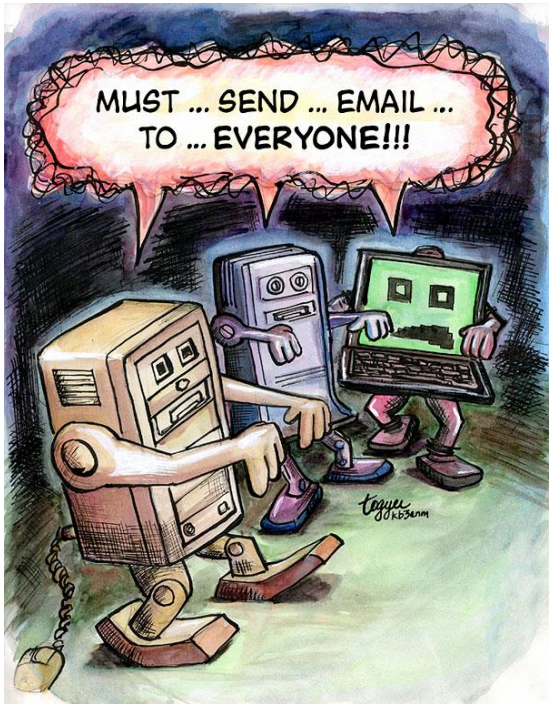


En ünlü Solucanlar (Worms)

- ILOVEYOU, bir e-mail eklentisi olarak dağıtılmış ve 5.5 milyar dolarlık bir zarara neden olmuştur.
- Code Red 359,000 siteyi etkilemiştir.
- SQL Slammer tüm interneti bir süreliğine yavaşlatmıştır
- Blaster ise bilgisayarınızı tekrar tekrar yeniden başlatabilir.



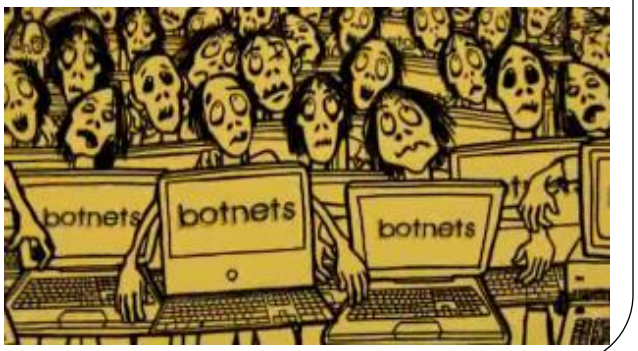
Zombi Bilgisayarlar (Botnet)



- Kötü amaçlı yazılımlar tarafından ele geçirilmiş sistemlerdir. Genellikle “truva atları” tarafından.

- Bu sistemler bir kısır döngü içerisinde sürekli olarak zararlı yazılım yayarlar ve kullanıcıları bunun farkında değildir.

- Aynı zamanda bilişim suçları için potansiyel bilgisayarlardır Botnet, spam yollamak ve şantaj yapmaya çalışmaktan, devlet ağlarına saldırmaya kadar farklı alanlarda, siber suçlular tarafından saldırıları yürütmek amacıyla kullanılabilir.



- Hatta bu yüzden işlemediğiniz suçlar ile ilgili adli makamlarla muhatap bile olabilirsiniz.

SOSYAL MÜHENDİSLİK

- Sahte senaryolar uydurmak (pretexting)
- Güvenilir bir kaynak olduğuna ikna etmek (phishing)
- Güvenilir bilgi karşılığında yardım, para, eşantiyon, hediye, … önermek
- Güven kazanarak bilgi edinmek
- Omuz sörfü, çöp karıştırmak, eski donanımları kurcalamak

Yöntemler - Güvenilir olduğuna ikna etmek

From: Komiser Kolombo

To: Ben

Bu email adresinden yüksek düzey bir bürokrata küfür içerikli mesaj atılmıştır. Konuyu incelemem için mesajı alır almaz şifrenizi yollamanız gereklidir.

- Genellikle e-posta üzerinden gerçekleşen bir yöntemdir.
- Saldırgan, amacına ulaşmak için güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan geldiğine inandırır.
- Hedef, saldırılanı bilgi vermeye zorlamak ya da hatalı bir hareket yapmaya (sahte web sitesine tıklamak, virüslü yazılım kurmak, …) yönlendirmektir.

Yöntemler - Bilgi Karşılığı Başka Bir Şey Önermek

Tebrikler! Çekilişimizi kazandınız. Parayı yollamamız için lütfen bize hesap numaranızı ve doğum tarihinizi gönderin.

- Hassas bilgiye ulaşmak için, kişinin hassasiyetlerini kullanan bir yöntemdir.
- Kurban, sonunda karlı (ya da zarar görmeden) çıkacağına ikna edildi
- ği bir senaryoyla hassas bilgiyi verebilir, ya da saldırgan yerine zararlı işlemler yapabilir.
- Hediyeli anket,Ödüllü soru,…

Yöntemler - Güven Kazanmak

Yıllar sonra Facebook'tan ilkokul arkadaşımla karşılaştım. O da sistem yöneticisiymiş. Sabaha kadar Msn'den mesleğimiz hakkında konuştuk.

- Saldırganın hedefine, iş dışında ya da iş sırasında güvenini sağlayacak şekilde iletişime geçip ikna ederek bilgi vermesine ya da istediğini yaptırmasına dayanan bir yöntemdir.
- Şirket/kuruma sağlayıcı olarak yaklaşıp erişim hakkı olan personelle güvene dayanan arkadaşlık kurmak
- İş dışında oluşan ilişkileri suistimal etmek
- Kurbanla ortak ilgileri / beğenileri paylaşıyor izlenimi vererek güven sağlamak

Yöntemler - Diğer

- **Omuz sörfü -** Şifreyi yazarken, erişimi kısıtlı sistemlere erişirken kurbanı izlemek
- **Çöp karıştırmak -** Çöpe atılmış CD, disket, kağıt, ajanda, not, post-it, … gibi eşyaları incelemek
- **Eski donanımları kurcalamak –** Hurdaya çıkmış, ikinci el satış sitelerinde satışa sunulmuş, çöpe atılmış, kullanılmadığı için hibe edilmiş donanımın içeriğini incelemek

Sosyal Mühendislik
Alınacak önlemler

- Taşıdığınız, işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edin.
- Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edin.
- Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgilerinizi kimseye söylemeyin.
- Şifre kişiye özel bilgidir, sistem yöneticinize bile telefonda veya e-posta ile şifrenizi söylemeyin. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapacaktır.

TEHDİTLERDEN KORUNMA YÖNTEMLERİ

KORUNMA YÖNTEMLERİ

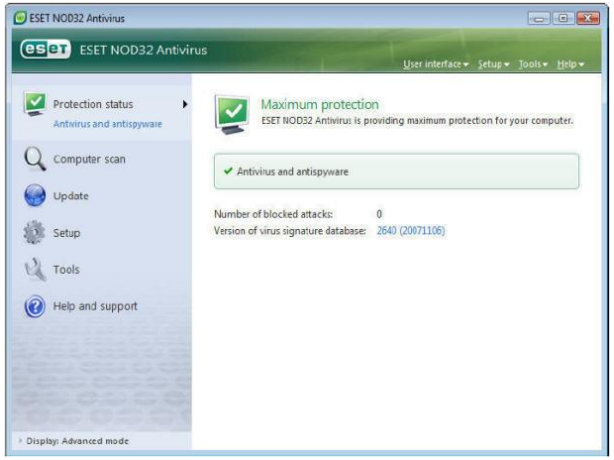
1. **Güvenlik yazılımları**
   - Antivirüs, firewall …
2. **Yazılım güncellemeleri**
3. **Kimlik doğrulaması**
4. **Verilerin yedeklemesi**
5. **Verilerin erişim izinleri**
6. **Verilerin şifrelenmesi**
7. **Verilerin güvenli şekilde silinmesi**
8. **Bilinçli kullanıcı davranışları**

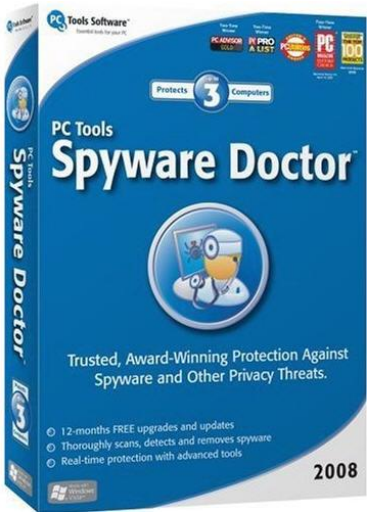
1- Güvenlik Yazılımları

- Güvenlik yazılımları çeşitli şekillerde sisteminizi korurlar
  - **Antivirüs, antispyware;** zararlı yazılım engelleme ve temizleme
  - **Firewall;** ağ paketlerinin erişim izinlerini denetlenmesi
  - **Denetim merkezleri;** güvenlik yazılımlarının etkinliğinin kontrolü
- Her bilgisayar, bir anti virüs yazılımına sahip olmalıdır ve virüs veritabanı sürekli güncellenmelidir
- Windows XP, Vista ve 7 sürümleri yerleşik güvenlik duvarı, antispyware yazılımı ve denetim merkezleri sunmaktadır

Zararlı Yazılımların Tespit Edilmesi

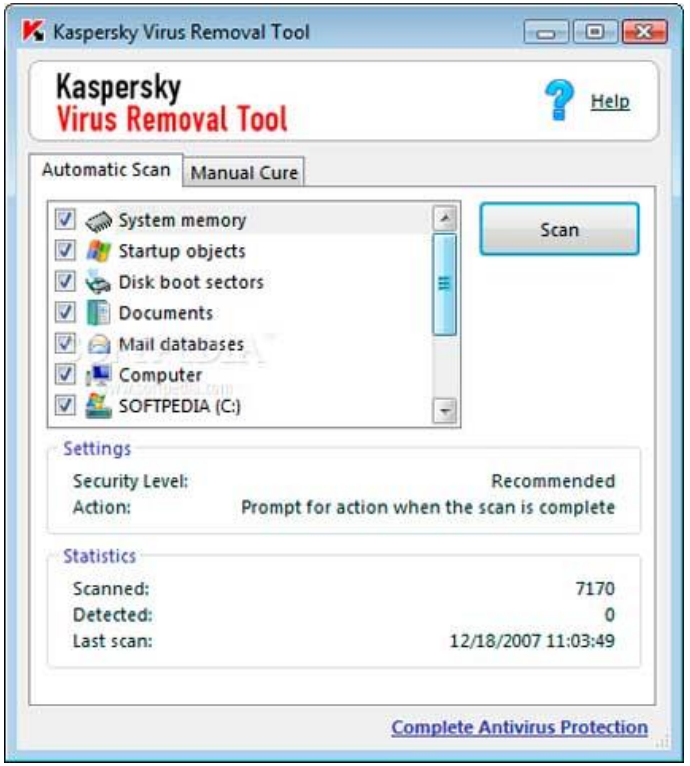
- Eğer bir sistem zararlı bir yazılım tarafından etkilenirse, en basit bulgu sistemin cevap verme süresinin gecikmesi olacaktır.
- Sistem istenmeyen veya yanlış davranışlar sergileyebilir.
- CPU ve bellek kaynakları doğrudan veya arka planda kullanılır.
- Tutarsız davranışlar karşısında sistem mutlaka güvenlik yazılımları ile taranmalıdır.





Zararlı Yazılımların Temizlenmesi

- Zararlı bir yazılım tespit edildiğinde temizleme için internet bağlantısını kesin ve mümkünse güvenli moda geçin
- Kurulu güvenlik yazılımları devre dışı kalmış ise veya güncel değil ise, harici ortamlardan çalışan tarama yazılımları kullanın
  - Knoppix, BartPE veya MiniPE gibi otomatik donanım taraması gibi birçok destek sağlayan kurulum gerektirmeyen önyükleme ortamları gerekebilir
- Öncelikli işlem zararlı yazılımın temizlenmesi veya karantinaya alınmasıdır
- Üçüncü alternatif ise veri veya programların silinmesidir



Firewall: Güvenlik Duvarları

- Güvenlik duvarları, bilgisayarın veya ağların, ağ ve internet ortamı ile iletişimini takip eden ve tanımlı kurallara göre bu trafiği yöneten yazılımlardır
- İzin verilenler dışındaki tüm portlar kapatılır, açık olan portlar üzerindeki paket trafiği ise sıkı kurallar tarafından denetlenir
- Windows XP, Vista ve 7, yerleşik güvenlik duvarı bulundurur