**Bilgisayar ve Veri Güvenliği**

**BİLGİSAYAR VE VERİ GÜVENLİĞİ**

**Kötü Amaçlı Yazılımlar (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),

**Kötü Amaçlı Yazılımlar (Maleware) Özellikleri**

* Öncelikli önlem bu yazılımların sisteme bulaşmasını önlemektir.
* İkinci aşama ise sisteme bulaşan bir zararlı yazılımın tespit edilmesi, kaldırılması veya karantinaya alınmasıdır.
* Kötü amaçlı yazılımlar ile mücadele etmek için mutlaka uygun ve güncel güvenlik yazılımları gereklidir.
* Bilgisayar Virüsleri Kullanıcının bilgisi haricinde bilgisayarda çalışan bir koddur.
* Dosyalara veya makro gibi kodlara bulaşırlar. n o t b a k . c o m
* Koda erişildiğinde ve çalıştırıldığında bilgisayara bulaşmaktadır.
* Virüsler çoğalabilme yeteneğine sahiptir ve kendilerini bilgisayarın her yerine bulaştırabilirler.

**1- Bilgisayar Virüsleri**

* Virüs bulaşan dosyalara diğer bilgisayarlar tarafından ulaşıldığında virüs diğer sistemlere de bulaşabilir.
* Yanlış olarak her türlü zararlı yazılımın yanlış bir algılama ile virüs olarak tanımlandığını duyabilirsiniz.

**Tipik Virüs Bulguları**

* Bilgisayarın normalden daha yavaş çalışması
* Normal olmayan hata mesajları
* Anti-virüs 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.

**Tipik Spyware Bulguları**

* 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 anti-virüs 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. dersimiz.com
* Virüsler ile arasındaki fark, kendilerini çoğaltamamalarıdır.

**En ünlü Solucanlar (Worms)**

* ILOVEYOU, bir email 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.

**TEHDİTLERDEN KORUNMA YÖNTEMLERİ**

**Korunma Yöntemleri**

* Güvenlik yazılımları
* Antivirüs, firewall …
* Yazılım güncellemeleri
* Kimlik doğrulaması
* Verilerin yedeklemesi
* Verilerin erişim izinleri
* Verilerin şifrelenmesi
* Verilerin güvenli şekilde silinmesi
* Bilinçli kullanıcı davranışları

**Güvenlik Yazılımları**

*Güvenlik yazılımları çeşitli şekillerde sisteminizi korurlar*

1- **Antivirüs, antispyware**; zararlı yazılım engelleme ve temizleme

2- **Firewall**; ağ paketlerinin erişim izinlerini denetlenmesi

3- **Denetim merkezleri**; güvenlik yazılımlarının etkinliğinin kontrolü

• Her bilgisayar, bir anti virüs yazılımına sahip olmalıdır ve virüs veritabanı sürekli güncellenmelidir.

• Windows XP, Vista ve 7, 10 sürümleri yerleşik güvenlik duvarı, antispyware yazılımı ve denetim merkezleri sunmaktadır.