Virüs,
Malware,
Spyware,
Adware
Nedir?

http://www.chip.com.tr/blog/hakanuzuner/Virus-Malware-Spyware-Adware-Nedir_831.html

VİRÜS

- Virüsler birer programdır. Fakat kendi kendilerini kopyalarlar, bir yerden bir yere bulaşırlar. Bilgisayarınız çalıştırıldığında otomatik olarak faaliyete geçerler. Bir virüsün bir diğer dosyaya veya sürücüye geçmesi çok kolaydır. Örneğin virüslü bir disket bilgisayara takıldığında disketin içinde hangi dosyaların olduğuna bakıldığında yani "dır" yazılıp enter tuşuna basıldığında virüs anında bilgisayarınıza bulaşabilir.

Macro virüsü

- Genel işlemleri gerçekleştirmek için programlar tarafından kullanılan bir komut seti olan makroları değiştiren veya bunların yerini alan bir bilgisayar virüsüdür.
- Bu virüsler, sadece hangi macro dili ile yazılmışlarsa o dosyaları bozabilirler. Macro virüsleri hangi temel programa ek olarak yazılmışlarsa o programı her çalıştırmanızda aktif hale geçer ve ilgili programların kullandığı bazı tanımlama dosyalarına da bulaşmaya çalışır. Böylece o programla oluşturulan her dökümana virüs bulaşmış olur.

Kötü niyetli yazılımların genel bir listesini yaparsak:

* sisteminizden dışarı telefon çevirisi yaparlar (auto-dialer - otomatik çevirici)
* sisteminizi uzaktan yönetirler (remote control - uzaktan kumanda)
* özel bilgilerinizi toplarlar (spyware - casus yazılım)
* istenmeyen pencereler gösterirler (adware - rahatsız edici reklâm)
* hangi tuşlara bastığınızı kaydederler (keyloggers - tuş kayıtçıları)
* sisteminize sessizce girer ve tamamen ele geçirirler (rootkit)

Yukarıda saydıklarımız ve bunların dışında teknikler her geçen gün büyük bir hızla çoğalıyor ancak bir bu yazıda kötü niyetli yazılımların en yaygın iki türünü

Truva atı

- Mitolojideki Truva atı nasıl bir armağan gibi görünüp, aslında Troya kentini ele geçirecek Yunanlı askerleri taşıyorduysa; bugünün Truva atları da yararlı yazılımlar gibi görünen bilgisayar programlarıdır, ancak güvenliğinizi tehlikeye atar ve pek çok zarara yol açarlar. Yakın geçmişteki bir Truva atı, Microsoft güvenlik güncelleştirmeleri olduğu iddia edilen eklerin bulunduğu bir e-posta görünümündeydi, ancak ekteki dosyaların virüsten koruma ve güvenlik duvarı yazılımlarını devreden çıkarmayı hedefleyen virüsler olduğu ortaya çıktı.

Trojan horses (Truva Atları)

- Truva Atları genellikle, e-postaların içine yerleştirilerek yollanır. İçine saklandığı program çalıştırılıncaya kadar aktif hale geçmezler. Truva Atı aktif hale geçince, bulunduğu sistemdeki korunmasız host ve serverlar hakkındaki bilgilerin tamamını ya kendi içinde kaydetmeye başlar. Yada bu virüslerin özelliği gereği bulaştığı bilgisayarları uzaktan erişime uygun hale getirdiğinden, elde ettiği bilgileri başka bir bilgisayara internet yoluyla gönderir. Bu virüsü bilgisayarınıza yerleştiren kişi, uzaktan erişim suretiyle sizin bilgisayarınızın içine çok rahatlıkla girerek, dosyaların açarak içeriğinde değişiklik yapmak, dosya silmek, sizin dosyalarınızı kendi bilgisayarına kopyalamak, e-postalarınızı okumak, CD-ROM' u açıp-kapatmak, varsa internet bankacılığı veya kredi kartı bilgilerinizi kopyalamak gibi sizin bilgisayarınızda yapabileceğiniz bütün işlemleri yapabilmektedir. Kısacası, Truva Atı bulaşan bir bilgisayarın, biri siz diğeri de uzaktan erişim metoduyla bilgisayarınıza giren kişi olmak üzere iki kullanıcısı olur.

Logic Bombs (Mantık Bombası)

- Mantık Bombaları, herhangi bir programın içerisine yerleştirilen virüs programlarıdır. Bazı şartların sağlanması durumunda patlayarak yani çalışmaya başlayarak sisteme zarar verirler.
- Çernobil virüsü buna çok iyi bir örnek olabilir. Bombalar, tüm dosyaları ve bilgileri silebilir veya sistemi göçertebilir.

- Çernobil virüsü: sabit diskin belirli kisimlari üzerinde belli yazma islemleri yapan zararli bir virüstür. Buna ek olarak bilgisayarin önemli bir parçasi olan Flash BIOS'a da zarar vermektedir.

Trap doors (Tuzak Kapanları)

“Tuzak kapısı ya da arka kapı, bir sistemin yazılımını yapan kişi tarafından, yazılımın içine gizli bir şekilde yerleştirilen bir virüs yazılımıdır. Bu programın çalıştığı bilgisayara virüsü yerleştiren kişinin, uzaktan erişim yöntemiyle sistem koruyucularını aşarak sızması mümkündür.

Exploit (Sömürmek)

- İşletim Sistemleri ve bazı programların açıklarını bulup bu açıkları kötüye kullanma yöntemine "exploit" deniliyor. Exploit'ler ile sistem şifreleri görülebilir, sistemler hakkında bilgiler elde edilebilinir. Exploitler sistemin olağan olarak çalışmasına engel olurlar ve sisteme dışardan kod göndererek sistemi normal olarak çalıştığına ikna ederler ve genelde de yetkisiz erişim için kullanılmaktadır. Bu tip virüsler, bulaştıkları bilgisayarın hafızasında bulunan e-posta adreslerinin hepsine o bilgisayar üzerinden e-posta göndererek virüsün diğer bilgisayarlara da bulaşmasını sağlarlar. E-maili alan kişi, gelen mailin daha önceden haberleştiği ve tanıdığı bir kişiden geldiğini görerek maili açmakta hiç tereddüt etmez ve kendi bilgisayarına da virüsü bulaştırır. Virüs bu bilgisayar üzerinde de ayanı işlemi tekrarlayarak yayılmaya devam eder. Bu tip virüslerin birçok kullanıcıya hitap eden serverlara bulaştığını düşünürsek, servera bağlanan her bilgisayara bu tip virüslerin bulaşması ile bir anda birçok bilgisayar zarar görmektedir.

Worms (Solucan)

- Solucan da, virüs gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır ancak bunu otomatik olarak yapar. İlk 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. Bu, domino etkisinin getirdiği yoğun ağ trafiği işyeri ağlarını ve Internet'in tümünü yavaşlatabilir. Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar. Ağları kilitlerler ve olasılıkla sizin ve başkalarının Internet'teki Web sayfalarını görüntülerken uzun süreler beklemenize yol açarlar.

Malware

- “Malicious software”‘in kısaltılmasıdır. Virüsler, trojanlar ve istenmeyen kötü niyetli kodların genel adıdır. Truva ati olarak da bilinen virüsler bu kategoriye girerler. Bir programın eklentisi olarak gelebileceği gibi, girmiş olduğunuz enfekte olmuş bir web sitesinden de sizin bilgisayarınıza yüklenebilir.

Rahatsız Edici Reklâmlar (Adware)

- Üzerinde bulundukları bilgisayara özel reklâmlar göstermek için tasarlanmış yazılımlardır.
- Kendi yazdığı programı satmak yerine, belirli firmalar tarafından sağlanan reklamları programın içine gömerek kullanıcıya sunan programların genel adı “adware” dır. Bu programların en belirgin özelliği ücretsiz olarak dağıtılması ve programı yazanın kazancını sizin bilgisayarınızda bu reklamları göstermesi ve sizin de gördüğünüz reklamları tıklamanızdan sağlamasıdır.

- Sistemdeki kişisel veya istatistiksel verileri sahibinin bilgisi ya da izni olmadan üçüncü kişilere gönderebilirler.
- Bu tür yazılımlar size istemediğiniz bilgiyi göstermek aşamasından sizin izniniz olmadan kişisel bilgilerinizi başkalarına açmak konumuna geçtiklerinde kötü niyetli olarak tanımlanabilirler.

Sık karşılaşılan rahatsız edici reklâmlar:

* Masaüstü arama yardımcıları veya indirme yöneticileri
* İnternet alış-veriş veya araştırma yardımcıları
* İmzalanmamış ActiveX denetimleri veya eklentiler
* İnternette gezdikçe para ödeyen reklâm uygulamaları
* Uygulama tarafından eklenen araç çubukları
* Gerçek zamanlı hava durumu raporu sunan araçlar

Rahatsız Edici Reklâmların Etkileri

- Rahatsız edici reklâmlar, bulunmaları ve temizlenmeleri sırasında kaybettirdikleri zaman nedeniyle ve tekrar gelmelerini engellemek için satın aldığınız yazılımlar nedeniyle size para kaybettirirler. Bir ya da birkaç bilgisayarı olan ev kullanıcıları için bu durum çok önemli olmayabilir fakat büyük firmalar açısından düşünüldüğünde bu tür yazılımlar gerçekten büyük masraflar açabilirler. Rahatsız edici reklâmlar genellikle orta seviyede tehlikeli kötü niyetli yazılımlar olarak algılanırlar.

Casus Yazılımlar (Spyware)

- Bu terim hayatımıza 1990'ların ortalarına doğru girmeye başladı. Günümüzde casus yazılım tanımını kullanıcının bilgisi ya da izni olmadan kişisel bilgileri izleyen, toplayan ve üçüncü kişilere gönderen her türlü yazılım için kullanılıyor.

- Adware’den farklı olarak, kullanıcının bilgisayarında hem belirli firmaların reklâmlarını görüntüleyip hem de bir iz kontrol mekanizması oluşturan programlara “Spyware” denir.

- Adware’den en belirgin farkı sizin bilgisayarınızda ne yaptığınızı ve bir kısım kişisel bilgilerinizi (hangi sitelere giriyorsunuz, ne tür içerik sizin ilginizi çekiyor, kredi kartı numaranız nedir, internet şifreleriniz nedir vs.) daha önceden belirlenmiş bir sunucuya, internete bağlandığınız zamanlarda gönderen (bir noktada sizin bilgisayarınızda ajanlık eden) programlardır.

Dialer

- Dialer programlar bilgisayarınızın internet bağlantı ayarlarını değiştirerek sizi ödemeli bir telefon hattına yönlendiren programlardır. Siz bu dialer programlar bulaştığı esnada her zamanki gibi internete bağlanırken eve şişik bir telefon faturası gelince şoke olursunuz, çünkü faturanız birden belki de 10 katı ile artmıştır. Bunun nedeni bu bilgisayarınıza bulaşan dialer programlar internete bağlandığınız numarayı biraz önce belirttiğimiz gibi ücretli bir yurtdışı hattı veya 900lü bir hat ile değiştirip sizi her internete girişinizde bu ücretli hatlar aracılığı ile internete bağlamıştır.