EEE374 SİBER GÜVENLİK

Prof. Dr. Hasan Hüseyin BALIK

(6. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2.Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.5.Kötü amaçlı yazılımlar

2.4. İçerik

- Kötü Amaçlı Yazılım Türleri
- Gelişmiş Israrlı Tehdit
- Yayılma
- Etkilenen İçerik – Virüsler
  - Güvenlik Açığı Sömürüsü – Solucanlar
  - Sosyal Mühendislik – SPAM E-Posta, Truva Atları
- Yük
  - Sistem Bozulması
  - Saldırı Ajanı – Zombi, Botlar
  - Bilgi Hırsızlığı – Keylogger'lar, Kimlik Avı, Casus Yazılım
  - Gizli - Arka Kapılar, Rootkit’ler
- karşı önlemler

Kötü amaçlı yazılım

800-83 (Kötü Amaçlı Yazılım Olayını Önleme Kılavuzu ve Masaüstü ve Dizüstü Bilgisayarlar için Kullanım- Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Temmuz 2013) kötü amaçlı yazılımı şu şekilde tanımlar:

"kurbanın verilerinin, uygulamalarının veya işletim sisteminin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atmak veya mağduru başka bir şekilde irrite etmek veya rahatsız etmek amacıyla genellikle gizlice bir sisteme eklenen bir program."

Kötü Amaçlı Yazılım Terminolojisi 1/2

İsim	Tanım
Gelişmiş Israrlı Tehdit (APT)	Çok çeşitli izinsiz giriş teknolojileri ve kötü amaçlı yazılımlar kullanarak, uzun bir süre boyunca belirli hedeflere ısrarlı ve etkili bir şekilde uygulanan, genellikle devlet destekli kuruluşlara atfedilen, ticari ve siyasi hedeflere yönelik siber suçlardır.
Reklam Yazılımı /Adware	Yazılıma entegre reklam. Pop-up reklamlara veya bir tarayıcının ticari bir siteye yönlendirilmesine neden olabilir.
Saldırı kiti	Sağlanan çeşitli yayılma ve yük mekanizmalarını kullanarak otomatik olarak yeni kötü amaçlı yazılım oluşturmaya yönelik araçlar setidir.
Auto-rooter	Yeni makinelere uzaktan girmek için kullanılan kötü amaçlı hacker araçlarıdır.
Arka Kapı/ Backdoor (trapdoor)	Normal bir güvenlik kontrolünü atlayan herhangi bir mekanizma; bir programdaki işlevlere veya güvenliği ihlal edilmiş bir sisteme yetkisiz erişime izin verebilir.
İndirici / Downloaders	Saldırı altındaki bir makineye başka öğeler yükleyen kod. Normalde, daha sonra daha büyük bir kötü amaçlı yazılım paketini içe aktarmak için önce güvenliği ihlal edilmiş bir sisteme eklenen kötü amaçlı yazılım koduna dahil edilir.
Drive-by download	Site görüntülendiğinde bir istemci sistemine saldırmak için bir tarayıcı güvenlik açığından yararlanan, güvenliği aşılmış bir web sitesinde kod kullanan bir saldırıdır.
İstismar/ Exploits	Tek bir güvenlik açığına veya bir dizi güvenlik açığına özel koddur.
Flood'lar/ Flooder (DoS istemcisi)	Bir tür hizmet reddi (DoS) saldırısı gerçekleştirerek ağa bağlı bilgisayar sistemlerine saldırmak için büyük miktarda veri oluşturmak için kullanılır.
Keylogger'lar/ Keyloggers	Güvenliği ihlal edilmiş bir sistemdeki tuş vuruşlarını yakalar.

Kötü Amaçlı Yazılım Terminolojisi 2/2

İsim	Tanım
Mantık Bombası / Logic bomb	Saldırgan tarafından kötü amaçlı yazılıma eklenen kod. Bir mantık bombası, önceden tanımlanmış bir koşul karşılanana kadar uykuda kalır; kod daha sonra bazı yükü tetikler
Macro virus	Makro veya komut dosyası kodu kullanan, tipik olarak bir belgeye veya belge şablonuna gömülü olan ve belge görüntülendiğinde veya düzenlendiğinde, kendisini bu tür diğer belgelerde çalıştırmak ve çoğaltmak için tetiklenen bir virüs türüdür
Mobil kod	Heterojen bir platform koleksiyonuna değişmeden gönderilebilen ve aynı semantik ile yürütülebilen yazılımdır (ör. komut dosyası ve makro).
Rootkit	Saldırgan bir bilgisayar sistemine girdikten ve kök düzeyinde erişim kazandıktan sonra kullanılan hacker araçları setidir.
Spam programları	Çok sayıda istenmeyen e-posta göndermek için kullanılır.
Casus Yazılım / Spyware	Bir bilgisayardan bilgi toplayan ve tuş vuruşlarını, ekran verilerini ve/veya ağ trafiğini izleyerek veya hassas bilgiler için sistemdeki dosyaları tarayarak başka bir sisteme ileten yazılımdır.
Truva Atı	Yararlı bir işleve sahip gibi görünen, ancak aynı zamanda, bazen onu çağıran bir sistem varlığının meşru yetkilerinden yararlanarak güvenlik mekanizmalarından kaçan gizli ve potansiyel olarak kötü amaçlı bir işlevi olan bir bilgisayar programıdır
Virüs	Tek bir güvenlik açığına veya bir dizi güvenlik açığına özel koddur.
Solucan	Bağımsız olarak çalışabilen ve hedef sistemdeki yazılım açıklarından yararlanarak veya yakalanan yetkilendirme kimlik bilgilerini kullanarak kendisinin tam bir çalışma sürümünü bir ağdaki diğer ana bilgisayarlara yayabilen bir bilgisayar programıdır.
Zombi, bot	İnfekte olmuş bir makineye yüklenen ve diğer makinelere saldırı başlatmak için etkinleştirilen programdır.

Kötü Amaçlı Yazılımın Sınıflandırılması

İki geniş kategoriye ayrılır:

- Öncelikle, istenen hedeflere ulaşmak için nasıl yayıldığına bağlı olarak
- Ardından, bir hedefe ulaşıldığında gerçekleştirdiği eylemler veya yüklere göre

Ayrıca şu şekilde sınıflandırılır:

- Bir ana bilgisayar programına ihtiyaç duyanlar (virüsler gibi parazit kodlar)
- Bağımsız, kendi kendine yeten programlar (solucanlar, truva atları ve botlar)
- Çoğalmayan kötü amaçlı yazılımlar (trojanlar ve istenmeyen e-postalar)
- Çoğalan kötü amaçlı yazılımlar (virüsler ve solucanlar)

Kötü Amaçlı Yazılım Türleri

Yayılma mekanizmaları şunları içerir:

- **Daha sonra diğer sistemlere yayılan virüsler tarafından mevcut içeriğin bulaşması**
- **Kötü amaçlı yazılımın çoğaltılmasına izin vermek için yazılım güvenlik açıklarından yararlanma**
- **Kullanıcıları Truva atları yüklemek veya kimlik avı saldırılarına yanıt vermek için güvenlik mekanizmalarını atlamaya ikna eden sosyal mühendislik saldırıları**

Kötü amaçlı yazılım tarafından hedef sisteme ulaştığında gerçekleştirilen yükler şunlardır:

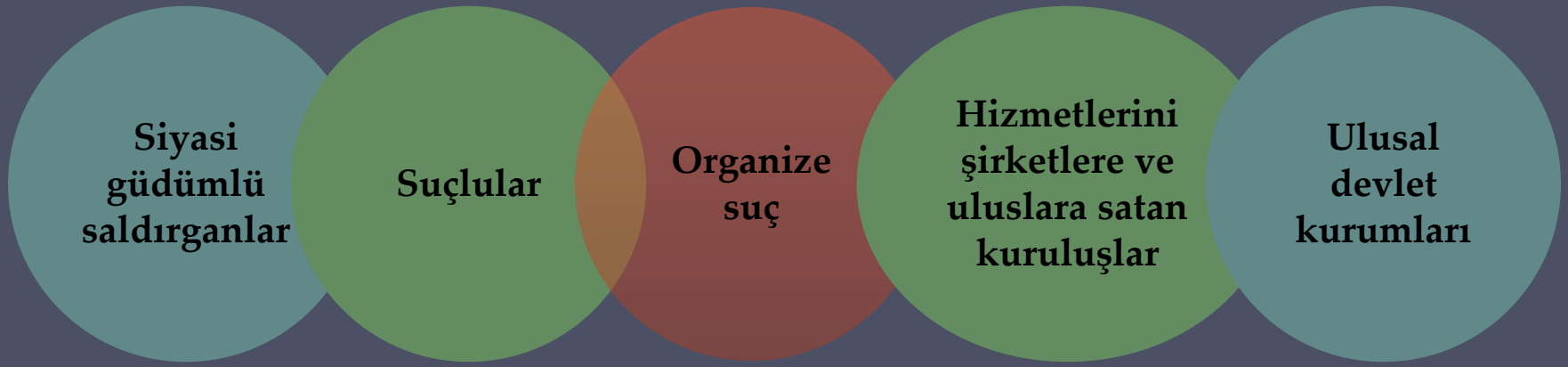
- **Sistem veya veri dosyalarının bozulması**
- **Hizmet hırsızlığı/sistemi bir botnet'in parçası olarak bir zombi saldırı aracısı yapma**
- **Sistemden/keylogging'den bilgi hırsızlığı**
- **Sistemde varlığını gizleme**

Saldırı Kitleri

- Başlangıçta kötü amaçlı yazılımın geliştirilmesi ve dağıtılması, yazılım yazarları tarafından önemli ölçüde teknik beceri gerektiriyordu.
  - 1990'ların başında virüs oluşturma araç takımlarının geliştirilmesi ve ardından 2000'lerde daha genel saldırı kitlerinin geliştirilmesi, kötü amaçlı yazılımların geliştirilmesine ve dağıtılmasına büyük ölçüde yardımcı oldu.
- Araç takımları genellikle " suç yazılımı" olarak bilinir.
  - Acemilerin bile dağıtabileceği çeşitli yayılma mekanizmalarını ve yük modüllerini dahil edin
  - Saldırganların bu araç setlerini kullanarak oluşturabileceği varyantlar, sistemleri onlara karşı savunanlar için önemli bir sorun oluşturuyor.
- Örnekler:
  - Zeus
  - Angler
  - Blackhole
  - Sakura
  - Phoenix

Saldırı Kaynakları

- Bir başka önemli kötü amaçlı yazılım geliştirmesi, saldırganların genellikle teknik yeterliliklerini meslektaşlarına göstermek için motive olan bireylerden, aşağıdakiler gibi daha organize ve tehlikeli saldırı kaynaklarına geçiştir:



- Bu, mevcut kaynakları ve kötü amaçlı yazılımların yükselişinin arkasındaki motivasyonu önemli ölçüde değiştirdi ve saldırı kitlerinin satışını, güvenliği ihlal edilmiş ana bilgisayarlara erişimi ve çalınan bilgileri içeren büyük bir yeraltı ekonomisinin gelişmesine yol açtı.

Gelişmiş Israrlı Tehditler (APT'ler)

- son yıllarda ön plana çıkmıştır.
- Çok çeşitli izinsiz giriş teknolojilerinin ve kötü amaçlı yazılımların seçilen hedeflere (genellikle ticari veya politik) iyi kaynaklı, kalıcı uygulaması
- Genellikle devlet destekli kuruluşlara ve suç kuruluşlarına atfedilir
- Dikkatli hedef seçimi ve uzun süreler boyunca gizli izinsiz giriş çabaları ile diğer saldırı türlerinden farklıdır.
- Yüksek profilli saldırılar şunları içerir:
  - Aurora, APT1, Shady RAT - Çin
  - Red October, Mask, Gauss - Rus güvenlik firması Kaspersky
  - DarkSeul - Kuzey Kore
  - Stuxnet, Flamei Daqu – ABD ve İsrail

APT Özellikleri

Gelişmiş

- Saldırganlar tarafından, gerektiğinde özel kötü amaçlı yazılımların geliştirilmesi de dahil olmak üzere çok çeşitli izinsiz giriş teknolojilerinin ve kötü amaçlı yazılımların kullanımı
- Tek tek bileşenler teknik olarak gelişmiş olmayabilir, ancak seçilen hedefe uyacak şekilde özenle seçilmiştir.

İsrarlı

- Başarı şansını en üst düzeye çıkarmak için saldırıların seçilen hedefe karşı uzun bir süre boyunca kararlı bir şekilde uygulanması
- Hedef tehlikeye girene kadar aşamalı olarak çeşitli saldırılar uygulanabilir.

Tehdit

- Organize, yetenekli ve iyi finanse edilen saldırganların, özel olarak seçilmiş hedefleri tehlikeye atmaya yönelik bir sonucu olarak seçilen hedeflere yönelik tehditler
- İnsanların sürece aktif katılımı, otomatik saldırı araçları nedeniyle tehdit düzeyini ve başarılı saldırıların olasılığını büyük ölçüde artırır.

APT Saldırıları

- Amaç:
  - Fikri mülkiyet veya güvenlik ve altyapı ile ilgili verilerin çalınmasından altyapının fiziksel olarak bozulmasına kadar değişir.
- Kullanılan teknikler:
  - Sosyal mühendislik
  - Hedefli kimlik avı e-postası
  - Hedef kuruluştaki personel tarafından ziyaret edilmesi muhtemel, güvenliği ihlal edilmiş seçili web sitelerinden yapılan indirmeler
- Niyet:
  - Hedefi, çoklu yayılma mekanizmaları ve yükleri olan gelişmiş kötü amaçlı yazılımlarla enfekte etmek
  - Hedef kuruluştaki sistemlere ilk erişim sağlandıktan sonra, erişimlerini sürdürmek ve genişletmek için bir dizi başka saldırı aracı kullanılır.

Virüsler

- Programlara bulaşan yazılım parçası
  - Bunları virüsün bir kopyasını içerecek şekilde değiştirir
  - Kopyalar ve diğer içeriği etkilemeye devam eder
  - Ağ ortamları aracılığıyla kolayca yayılır
- Yürütülebilir bir programa eklendiğinde bir virüs, programın yapmasına izin verilen her şeyi yapabilir.
  - Ana bilgisayar programı çalıştırıldığında gizlice yürütülür
- İşletim sistemine ve donanıma özel
  - Ayrıntılarından ve zayıf yönlerinden yararlanır

Virüs Bileşenleri

Enfeksiyon mekanizması

- Bir virüsün yayıldığı araçlar
- *Enfeksiyon vektörü* olarak da adlandırılır

Tetikleyici

- Yükün ne zaman etkinleştirileceğini veya teslim edileceğini belirleyen olay veya koşul
- Bazen *mantık bombası* olarak bilinir

Yük

- Virüs ne yapar (yaymanın dışında)
- Hasar veya iyi huylu ancak fark edilebilir aktivite içerebilir

Virüs Evreleri

Uyku evresi

Virüs boşta	Sonunda bir olay tarafından etkinleştirilecektir	Tüm virüslerde bu aşama yoktur.

Tetikleme aşaması

Virüs, amaçlanan işlevi gerçekleştirmek için etkinleştirilir	Çeşitli sistem olaylarından kaynaklanabilir

Yayılma Aşaması

Virüs, kendisinin bir kopyasını diğer programlara veya diskteki belirli sistem alanlarına yerleştirir	Yayılan sürümle aynı olmayabilir	Virüs bulaşmış her program, artık bir yayılma aşamasına girecek olan virüsün bir klonunu içerecektir

Yürütme aşaması

İşlev gerçekleştirilir	Zararsız veya zarar verici olabilir

Makro ve Komut Dosyası Virüsleri

- 1990'ların ortalarında, makro veya komut dosyası kod virüsleri, açık ara en yaygın virüs türü haline geldi.
- NISTIR 7298, bir makro virüsünü şu şekilde tanımlar:

  "Kendini belgelere iliştiren ve belge uygulamasının makro programlama yeteneklerini yürütmek ve yaymak için kullanan bir virüs"
- Makro virüsleri, çeşitli kullanıcı belge türlerinde etkin içeriği desteklemek için kullanılan komut dosyası kodunu etkiler.
- Birkaç nedenden dolayı tehdit ediyor:
  - Platformdan bağımsız
  - Kodun yürütülebilir kısımlarını değil, belgeleri enfekte eder
  - Kolayca yayılır
  - Sistem programları yerine kullanıcı belgelerine bulaştıklarından, geleneksel dosya sistemi erişim kontrollerinin, kullanıcıların bunları değiştirmesi beklendiğinden, yayılmalarını önleme sınırlıdır
  - Geleneksel yürütülebilir virüslere göre yazmak veya değiştirmek çok daha kolaydır

Virüs Sınıflandırmaları

Hedefe göre sınıflandırma

- Önyükleme sektörü bulaştırıcısı
  - Ana önyükleme kaydına veya önyükleme kaydına bulaşır ve virüs içeren diskten bir sistem başlatıldığında yayılır
- Dosya bulaştırıcı
  - İşletim sistemi veya kabuğun yürütülebilir olarak kabul ettiği dosyalara bulaşır
- makro virüs
  - Bir uygulama tarafından yorumlanan makro veya komut dosyası koduyla dosyalara bulaşır
- çok parçalı virüs
  - Dosyaları çeşitli şekillerde etkiler

Gizleme stratejisine göre sınıflandırma

- Şifreli virüs
  - Virüsün bir kısmı rastgele bir şifreleme anahtarı oluşturur ve virüsün geri kalanını şifreler.
- gizli virüs
  - Kendisini anti-virüs yazılımı tarafından tespit edilmekten gizlemek için açıkça tasarlanmış bir virüs biçimi
- polimorfik virüs
  - Her enfeksiyonda mutasyona uğrayan bir virüs
- metamorfik virüs
  - Her yinelemede mutasyona uğrayan ve kendini tamamen yeniden yazan ve görünümün yanı sıra davranışı da değiştirebilen bir virüs

Solucanlar

- Bir bilgisayar solucanı kavramı, 1975 yılında John Brunner tarafından tanıtıldı.
- Aktif olarak bulaştırmak için daha fazla makine arayan ve enfekte her makine diğer makinelere yapılan saldırılar için otomatik bir başlatma rampası görevi gören program
- İstemci veya sunucu programlarındaki yazılım açıklarından yararlanır
- Sistemden sisteme yayılmak için ağ bağlantılarını kullanabilirPaylaşılan medya (USB sürücüler, CD, DVD veri diskleri) aracılığıyla yayılır
- Eklere ve anlık ileti dosya aktarımlarına dahil edilen makro veya komut dosyası kodunda yayılan e-posta solucanları
- Aktivasyon üzerine solucan çoğalabilir ve tekrar çoğalabilir
- Genellikle bir tür yük taşır
- Bilinen ilk uygulama, 1980'lerin başında Xerox Palo Alto Laboratuarlarında yapıldı. Hesaplama açısından yoğun bir görevi yürütmek için kullanmak üzere boşta sistemler aramak kötü amaçlı değildi..

Solucan Replikasyonu

Elektronik posta veya anlık mesajlaşma imkanı	• Solucan, kendisinin bir kopyasını diğer sistemlere e-posta ile gönderir • Anlık mesaj servisi aracılığıyla kendisini ek olarak gönderir
Dosya paylaşımı	• Kendi kopyasını oluşturur veya çıkarılabilir medyadaki bir dosyayı enfekte eder
Uzaktan yürütme yeteneği	• Solucan, kendisinin bir kopyasını başka bir sistemde yürütür
Uzaktan dosya erişimi veya aktarım özelliği	• Solucan, kendisini bir sistemden diğerine kopyalamak için bir uzak dosya erişimi veya aktarım hizmeti kullanır.
Uzaktan oturum açma özelliği	• Solucan, bir kullanıcı olarak uzak bir sistemde oturum açar ve ardından kendisini bir sistemden diğerine kopyalamak için komutları kullanır.

Hedef Keşfi

- Tarama (veya parmak izi)
  - Bir ağ solucanı için yayılma aşamasındaki ilk işlev
  - Bulaşacak diğer sistemleri arar
- Rastgele
  - Güvenliği ihlal edilmiş her ana bilgisayar, farklı bir tohum kullanarak IP adres alanındaki rastgele adresleri araştırır
  - Bu, gerçek saldırı başlatılmadan önce bile genel kesintiye neden olabilecek yüksek hacimli İnternet trafiği üretir.
- En iyiler listesi
  - Saldırgan, önce olası savunmasız makinelerin uzun bir listesini derler.
  - Liste derlendikten sonra saldırgan listedeki makinelere bulaşmaya başlar.
  - Her enfekte makineye, taranacak listenin bir kısmı verilir.
  - Bu, enfeksiyonun gerçekleştiğini tespit etmeyi zorlaştırabilecek çok kısa bir tarama süresi ile sonuçlanır.
- Topolojik
  - Bu yöntem, taranacak daha fazla ana bilgisayar bulmak için enfekte olmuş bir kurban makinesinde bulunan bilgileri kullanır.
- Yerel alt ağ
  - Bir ana bilgisayara güvenlik duvarının arkasında enfekte edebiliyorsa, kendi yerel ağındaki hedefleri arar.
  - Ana bilgisayar, aksi takdirde güvenlik duvarı tarafından korunacak diğer ana bilgisayarları bulmak için alt ağ adres yapısını kullanır.

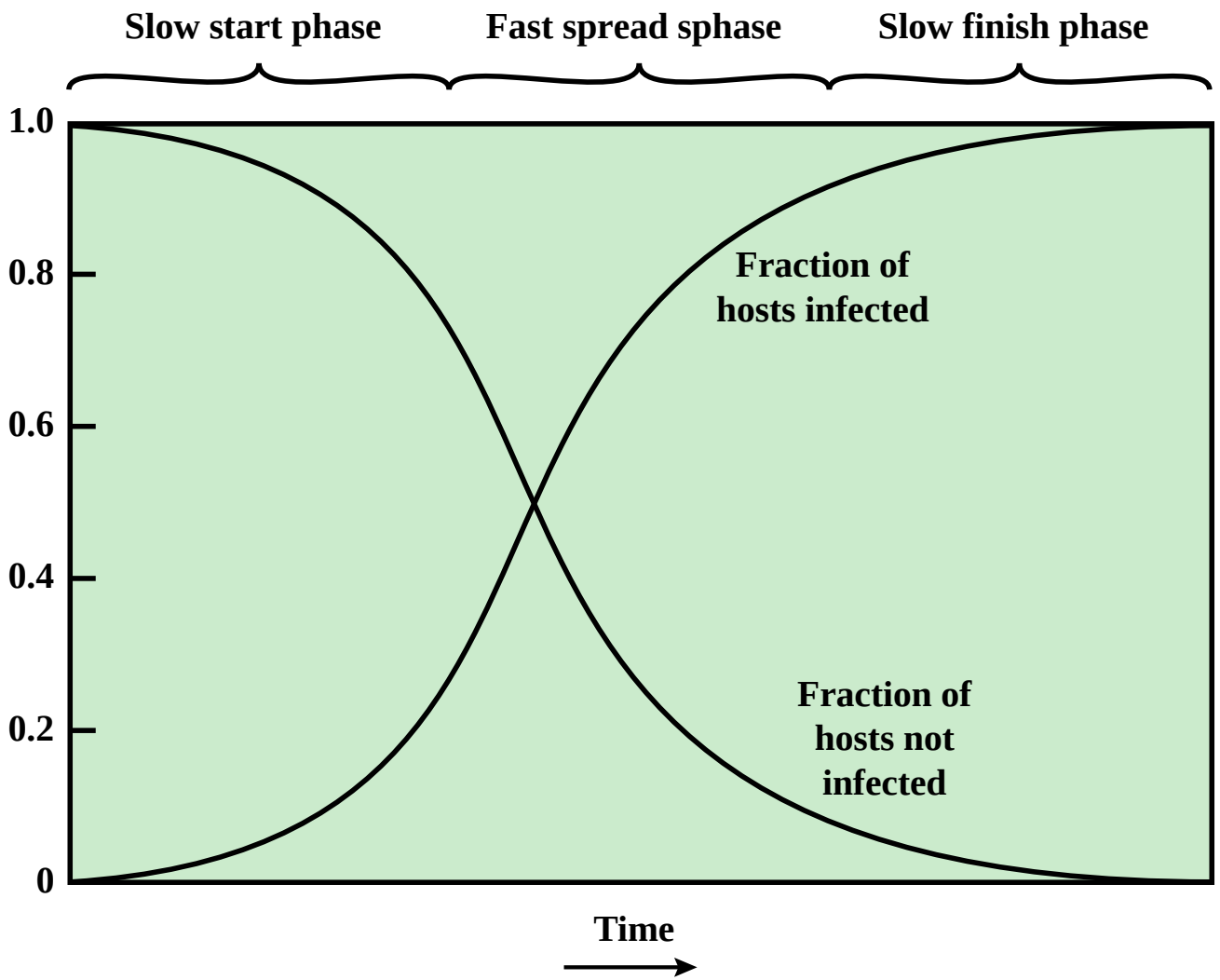


Figure 6.2 Worm Propagation Model

Morris solucanı

- En erken önemli solucan enfeksiyonu
- Robert Morris tarafından 1988'de yayınlandı.
- UNIX sistemlerine yayılmak üzere tasarlanmıştır
  - Diğer sistemlerde oturum açmak için oturum açma/parola kullanmak için yerel parola dosyasını kırmaya çalıştı
  - Uzak bir kullanıcının nerede olduğunu bildiren parmak protokolündeki bir hatadan yararlanıldı
  - Posta alan ve gönderen uzak işlemin hata ayıklama seçeneğinde bir gizli kapıdan yararlanıldı
- Başarılı saldırılar, işletim sistemi komut yorumlayıcısı ile iletişim sağladı
  - Solucan kopyalamak için yorumlayıcıya bir önyükleme programı gönderdi

Gözeçarpan Solucan saldırıları

Melisa	1998	E-posta solucanı Tek bir pakette virüs, solucan ve Truva Atı içeren ilk
Kırmızı kod	Temmuz 2001	İstismar edilen Microsoft IIS hatası Rastgele IP adreslerini araştırır Etkin olduğunda önemli miktarda İnternet kapasitesi tüketir
Kırmızı Kod II	Ağustos 2001	Ayrıca hedeflenen Microsoft IIS Erişim için bir arka kapı kurar
Nimda	Eylül 2001	Solucan, virüs ve mobil kod özelliklerine sahipti E-posta, Windows paylaşımları, Web sunucuları, Web istemcileri, arka kapılar kullanarak yayılma
SQL Slammer'ı	2003 başı	SQL sunucusunda bir arabellek taşması güvenlik açığından yararlanıldı kompakt ve hızla yayılan
sobig.f	2003 sonu	Enfekte makineleri spam motorlarına dönüştürmek için açık proxy sunucularından yararlanıldı
Mydoom	2004	Toplu postalama e-posta solucanı Enfeke olmuş makinelere bir arka kapı kurdu
Warezov	2006	Sistem dizinlerinde yürütülebilir dosyalar oluşturur Kendini bir e-posta eki olarak gönderir Güvenlikle ilgili ürünleri devre dışı bırakabilir
conficker(İndirme)	Kasım 2008	Windows arabellek taşması güvenlik açığından yararlanır SQL Slammer'dan bu yana en yaygın enfeksiyon
Stuxnet	2010	Tespit şansını azaltmak için sınırlı yayılma oranı Hedeflenen endüstriyel kontrol sistemleri

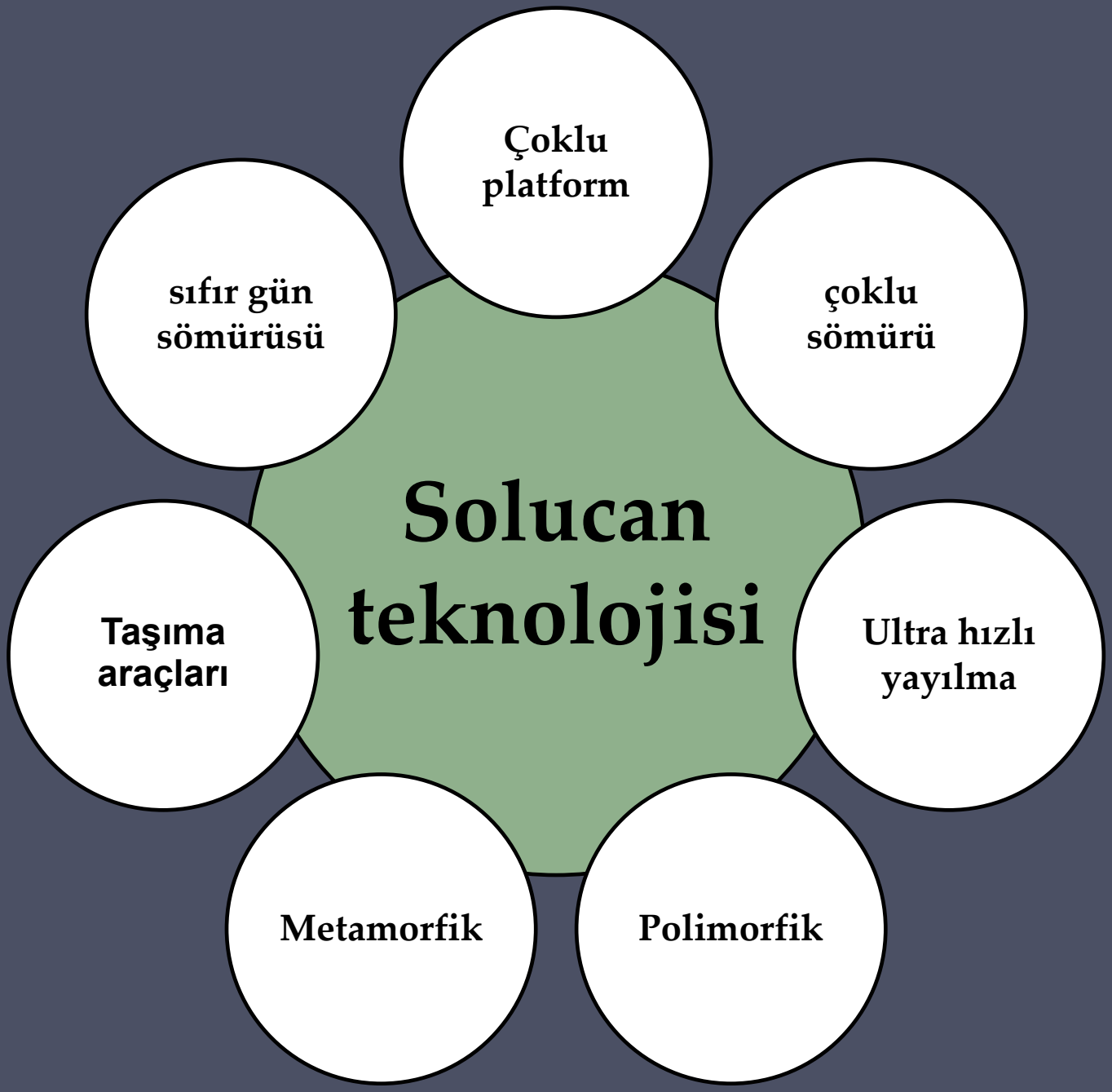
WannaCry

Mayıs 2017'de saatler ve günler içinde son derece hızlı bir şekilde yayılan ve 150'den fazla ülkede hem kamu hem de özel kuruluşlara ait yüz binlerce sisteme bulaşan fidye yazılımı saldırısı

Yama uygulanmamış Windows sistemlerinde SMB dosya paylaşım hizmetindeki bir güvenlik açığından yararlanmaya çalışarak hem yerel hem de rastgele uzak ağları agresif bir şekilde tarayarak bir solucan olarak yayıldı.

Bu hızlı yayılma, yalnızca bir İngiliz güvenlik araştırmacısı tarafından bir "kill-switch" etki alanının yanlışlıkla etkinleştirilmesiyle yavaşlatıldı.

Enfekte sistemlere yüklendikten sonra, dosyaları şifreleyerek kurtarmak için fidye ödemesi talep etti.


Solucan teknolojisi
Çoklu platform
çoklu sömürü
Ultra hızlı yayılma
Polimorfik
Metamorfik
Taşıma araçları
sıfır gün sömürüsü

Mobil Kod

- NIST SP 800-28, mobil kodu şu şekilde tanımlar:
  "heterojen bir platform koleksiyonuna değişmeden gönderilebilen ve aynı anlambilimle yürütülebilen programlar"
- Uzak bir sistemden yerel bir sisteme iletilir ve ardından yerel sistemde yürütülür
- Genellikle bir virüs, solucan veya Truva atı için bir mekanizma görevi görür
- Kendi istismarlarını gerçekleştirmek için güvenlik açıklarından yararlanır
- Popüler araçlar şunları içerir:
  - Java uygulamaları
  - ActiveX
  - JavaScript
  - VBScript
- Yerel sistemdeki kötü amaçlı işlemler için mobil kodu kullanmanın en yaygın yolları şunlardır:
  - Siteler arası komut dosyası oluşturma
  - Etkileşimli ve dinamik Web siteleri
  - Email ekleri
  - Güvenilmeyen sitelerden veya güvenilmeyen yazılımlardan yapılan indirmeler

Cep Telefonu Solucanları

- İlk keşif 2004 yılında Cabir solucanıydı
- Daha sonra 2005 yılında Lasco ve CommWarrior
- Bluetooth kablosuz bağlantıları veya MMS aracılığıyla iletişim kurar
- Hedef akıllı telefon kullanıcıların yüklemesine izin veren hücresel ağ operatörü dışındaki kaynaklardan yazılım uygulamaları
- Tüm bu ilk mobil solucanlar, Symbian işletim sistemini kullanan cep telefonlarını hedef aldı.
- Telefonu tamamen devre dışı bırakabilir, telefondaki verileri silebilir veya cihazı pahalı mesajlar göndermeye zorlayabilir
- CommWarrior, Bluetooth aracılığıyla diğer telefonlara kopyalar, kendisini kişilere MMS dosyası olarak ve gelen metin mesajlarına otomatik yanıt olarak gönderir.
- Cep telefonu solucanları mümkün olsa da, gözlemlenen cep telefonu kötü amaçlı yazılımlarının büyük çoğunluğu, kendilerini yüklemek için truva atı uygulamaları kullanıyor.

Drive-By-Downloads

Tarayıcı ve eklenti güvenlik açıklarından yararlanır, böylece kullanıcı saldırgan tarafından kontrol edilen bir web sayfasını görüntülediğinde, kullanıcının bilgisi veya izni olmadan sisteme kötü amaçlı yazılım indirmek ve yüklemek için hatadan yararlanan kod içerir.

Çoğu durumda kötü amaçlı yazılım, bir solucanın yaptığı gibi aktif olarak yayılmaz.

Kullanıcılar kötü niyetli Web sayfasını ziyaret ettiğinde yayılır

Sulama Deliği Saldırıları

- Drive-by-download saldırıları, güvenliği ihlal edilmiş bir siteyi ziyaret eden herkese yöneliktir. site ve kullanılan istismarlara karşı savunmasız
- Yüksek oranda hedeflenmiş saldırılarda kullanılan bir drive-by download çeşidi
- Saldırgan, ziyaret etmeleri muhtemel web sitelerini belirlemek için hedeflenen kurbanlarını araştırır, ardından bu siteleri taramalarına izin veren güvenlik açıklarına sahip olanları belirlemek için tarar.
- Ardından, hedeflenen kurbanlarından birinin güvenliği ihlal edilmiş sitelerden birini ziyaret etmesini beklerler.
- Saldırı kodu, yalnızca hedef kuruluşa ait sistemlere bulaşacak ve siteye gelen diğer ziyaretçiler için herhangi bir işlem yapmaması için bile yazılabilir.
- Bu, site güvenliğinin algılanmadan kalma olasılığını büyük ölçüde artırır

Kötü amaçlı reklam

Web sitelerine gerçekten zarar vermeden kötü amaçlı yazılım yerleştirir

Saldırgan, amaçlanan hedef web sitelerine yerleştirilme olasılığı yüksek olan ve bunlara kötü amaçlı yazılım içeren reklamlar için ödeme yapar.

Saldırganlar, bu kötü amaçlı reklamları kullanarak, onları görüntüleyen sitelerin ziyaretçilerini enfekte edebilir.

Kötü amaçlı yazılım kodu, tespit şansını azaltmak veya yalnızca belirli sistemlere bulaşmak için dinamik olarak oluşturulabilir.

İstenilen web sitelerine birkaç soru sorulmasıyla kolayca yerleştirilebilmeleri ve takip edilmesinin zor olması nedeniyle son yıllarda hızla büyümüştür.

Saldırganlar, hedeflenen kurbanlarının hedeflenen web sitelerinde gezinerek görünürlüklerini büyük ölçüde azaltabileceğini düşündüklerinde, bu reklamları birkaç saat kadar kısa bir süre için yerleştirebilirler.

Diğer kötü amaçlı yazılımlar, kötü amaçlı bir PDF belgesi görüntülediklerinde, kullanıcının izni olmadan kötü amaçlı yazılım indirip yüklemeleri için yaygın PDF görüntüleyicileri hedefleyebilir.

Tıklama hırsızlığı (Clickjacking)

- Kullanıcı arabirimi (UI) düzeltme saldırısı olarak da bilinir
- Benzer bir teknik kullanılarak tuş vuruşları da ele geçirilebilir.
  - Bir kullanıcı, e-posta veya banka hesabının parolasını yazdığına inandırılabilir, bunun yerine saldırgan tarafından kontrol edilen görünmez bir çerçeveye yazıyor olabilir.
- Saldırganın, enfekte bir kullanıcının tıklamalarını toplamak için kullandığı güvenlik açığı
  - Saldırgan, kullanıcıyı, kullanıcının bilgisayar ayarlarını değiştirmekten, farkında olmadan kullanıcıyı kötü amaçlı kod içerebilecek Web sitelerine göndermeye kadar çeşitli şeyler yapmaya zorlayabilir.
  - Adobe Flash veya JavaScript'ten yararlanan bir saldırgan, meşru bir düğmenin altına veya üstüne bir düğme yerleştirebilir ve bu da kullanıcıların algılamasını zorlaştırabilir.
  - Tipik bir saldırı, bir kullanıcıyı en üst düzey sayfayı tıklamayı planlarken başka bir sayfadaki bir düğmeyi veya bağlantıyı tıklaması için kandırmak için birden çok saydam veya opak katman kullanır.
  - Saldırgan, bir sayfaya yönelik tıklamaları ele geçiriyor ve bunları başka bir sayfaya yönlendiriyor

Sosyal mühendislik

- Kullanıcıları kendi sistemlerinden ödün vermelerine yardımcı olmak için "kandırmak"

Spam

İstenmeyen toplu e-posta

Önemli kötü amaçlı yazılım taşıyıcısı

Yemleme saldırıları için kullanılır

Truva atı

Zararlı gizli kod içeren program veya yardımcı program

Saldırganın doğrudan gerçekleştiremeyeceği işlevleri gerçekleştirmek için kullanılır

Cep telefonu Truva atları

İlk olarak 2004'te çıktı (Skuller)

Hedef akıllı telefon

Yük Sistem Bozulması

Çernobil virüsü

- İlk kez 1998'de görüldü
- Yıkıcı, parazit bellekte yerleşik bir Windows 95 ve 98 virüsü örneği
- Yürütülebilir dosyalara açıldıklarında bulaşır ve bir tetikleme tarihine ulaşıldığında, virüs, sabit sürücünün ilk megabaytının üzerine sıfırlar yazarak virüslü sistemdeki verileri siler ve bu da tüm dosya sisteminin büyük ölçüde bozulmasına neden olur.

Klez

- Windows 95'ten XP'e kadar sistemlere bulaşan toplu posta solucanı
- İlk olarak Ekim 2001'de görüldü
- Kendisinin kopyalarını adres defterinde ve sistemdeki dosyalarda bulunan adreslere e-posta ile göndererek yayılır.
- Sistemde çalışan bazı anti-virüs programlarını durdurabilir ve silebilir.
- Tetikleme tarihinde, sabit sürücüdeki dosyaların boşalmasına neden olur

Fidye yazılımı

- Kullanıcının verilerini şifreler ve bilgileri kurtarmak için gereken anahtara erişmek için ödeme talep eder.
- PC Cyborg Truva Atı (1989)
- 2006 yılının ortalarında, verileri şifrelemek için giderek daha büyük anahtar boyutlarına sahip açık anahtarlı şifreleme kullanan bir dizi solucan ve Truva atı ortaya çıktı.
- Kullanıcının bu verilerin şifresini çözecek anahtarı alabilmesi için fidye ödemesi veya belirli sitelerden alışveriş yapması gerekiyordu.

Fidye yazılımı

- WannaCry
  - Mayıs 2017'de birçok ülkede çok sayıda sisteme bulaştı
  - Virüs bulaşmış sistemlere yüklendiğinde çok sayıda dosyayı şifreledi ve ardından onları kurtarmak için Bitcoin olarak fidye ödemesi istedi.
  - Bu bilgilerin kurtarılması genellikle ancak kuruluşun iyi yedeklemelere ve uygun bir olay müdahalesi ve felaket kurtarma planına sahip olması durumunda mümkün olmuştur.
  - Hedefler kişisel bilgisayar sistemlerinin ötesine geçerek mobil cihazları ve Linux sunucularını kapsayacak şekilde genişletildi
  - Hassas kişisel bilgileri yayınlamakla tehdit etmek veya kısa bir süre sonra şifreleme anahtarını kalıcı olarak yok etmek gibi taktikler bazen mağdurun ödeme yapması için baskıyı artırmak için kullanılır.

yük
Sistem Bozulması

- Gerçek dünya hasarı
  - Fiziksel ekipmana zarar verir
    - Çernobil virüsü BIOS kodunu yeniden yazıyor
  - Stuxnet solucanı
    - Spesifik endüstriyel kontrol sistemi yazılımını hedefler
  - Endüstriyel sabotaj için gelişmiş hedefli kötü amaçlı yazılım kullanma konusunda endişeler var
- Mantık bombası
  - Belirli koşullar karşılandığında "patlamaya" ayarlanmış kötü amaçlı yazılıma gömülü kod

Yük
Saldırı Ajanları/Botlar

- İnternete bağlı başka bir bilgisayarı ele geçirir ve bu bilgisayarı saldırıları başlatmak veya yönetmek için kullanır
- *botnet*- koordineli bir şekilde hareket edebilen botların toplanması
- Kullanım Alanları:
  - Dağıtılmış Hizmet Reddi (DDoS) saldırılar
  - spam
  - Trafiği snif etmek
  - Keylogging
  - Yeni kötü amaçlı yazılım yaymak
  - Reklam eklentilerini ve tarayıcı yardımcı nesnelerini (BHO'lar) yükleme
  - IRC sohbet ağlarına saldırmak
  - Çevrimiçi anketleri/oyunları manipüle etme

Uzaktan Kontrol Vasıtası

- Bir botu bir solucandan ayırt eder
  - Solucan kendini yayar ve kendini aktive eder
  - Bot başlangıçta bir merkezi tesisten kontrol edilir
- Uzaktan kontrol olanağını uygulamanın tipik yolu bir IRC sunucusundadır.
  - Botlar bu sunucuda belirli bir kanala katılır ve gelen mesajları komut olarak kabul eder.
  - Daha yeni botnetler, HTTP gibi protokoller aracılığıyla gizli iletişim kanalları kullanır.
  - Dağıtılmış kontrol mekanizmaları, tek bir hata noktasından kaçınmak için eşler arası protokolleri kullanır

Yük – Bilgi Hırsızlığı
Keylogger'lar ve Casus Yazılım

Keylogger

- Saldırganın hassas bilgileri izlemesine izin vermek için tuş vuruşlarını yakalar
- Tipik olarak, yalnızca anahtar kelimelere ("login", "password") yakın bilgileri döndüren bir çeşit filtreleme mekanizması kullanır.

Spyware

- Sistemdeki geniş bir faaliyet yelpazesinin izlenmesine izin vermek için güvenliği ihlal edilmiş makineyi bozar
  - Tarama etkinliğinin geçmişini ve içeriğini izleme
  - Belirli Web sayfası isteklerini sahte sitelere yönlendirme
  - Tarayıcı ile ilgili belirli Web siteleri arasında değiş tokuş edilen verilerin dinamik olarak değiştirilme

Yük – Bilgi Hırsızlığı Yemleme (Phishing)

- Güvenilir bir kaynaktan gelen iletişim gibi görünerek kullanıcının güveninden yararlanmak için sosyal mühendislikten yararlanır
  - Bir bankacılık, oyun veya benzeri sitenin giriş sayfasını taklit eden sahte bir Web sitesine bağlantı veren spam e-postaya bir URL ekler
  - Kullanıcının hesabının kimliğini doğrulamak için acil bir işlem yapması gerektiğini önerir
  - Saldırgan, ele geçirilen kimlik bilgilerini kullanarak hesabı ele geçirir
- Yemleme kancası
  - Alıcılar saldırgan tarafından dikkatlice araştırılır
  - E-posta, alıcısına özel olarak uyacak şekilde hazırlanır ve genellikle onları gerçekliğine ikna etmek için bir dizi bilgiden alıntı yapar.

Yük –gizleme
Arka kapı (backdoor)

- *Trapdoor* olarak da bilinir
- Saldırganın erişim kazanmasına ve güvenlik erişim prosedürlerini atlamasına izin veren bir programa gizli giriş noktası
- *Bakım kancası* Programcılar tarafından programlarda hata ayıklamak ve test etmek için kullanılan bir arka kapıdır.
- Uygulamalarda arka kapılar için işletim sistemi kontrollerini uygulamak zordur.

Yük -gizleme Rootkit

- Bir sisteme gizli erişimi sağlamak için bir sisteme kurulmuş gizli programlar seti
- Bir bilgisayardaki süreçleri, dosyaları ve kayıtları izleyen ve raporlayan mekanizmaları alt üst ederek gizler
- Saldırgana yönetici (veya root) ayrıcalıkları verir
  - Programları ve dosyaları ekleyebilir veya değiştirebilir, süreçleri izleyebilir, ağ trafiği gönderip alabilir ve isteğe bağlı olarak arka kapı erişimi elde edebilir

Rootkit Sınıflandırma Özellikleri

Israrcı/kalıcı

- Sistem her önyüklendiğinde etkinleşir
- Kayıt defterinde veya dosya sisteminde saklanır

Bellek tabanlı

- yeniden başlatmadan sağ çıkamaz.
- tespit edilmesi daha zor

Kullanıcı modu

- API'lere yapılan çağrıları durdurur ve döndürülen sonuçları değiştirir

Çekirdek modu

- Çekirdek modunda yerel API'lere yapılan çağrıları kesebilir
- etkin işlemler listesinden kaldırarak kötü amaçlı bir işlemin varlığını gizler

Sanal makine tabanlı

- hafif bir sanal makine monitörü kurar ve ardından işletim sistemini bunun üzerindeki bir sanal makinede çalıştırır

Harici mod

- hedeflenen sistemin normal çalışma modunun dışında, donanıma doğrudan erişebileceği BIOS veya sistem yönetimi modunda bulunur

Kötü Amaçlı Yazılım Önlem Yaklaşımları

- Kötü amaçlı yazılım tehdidine ideal çözüm önlemedir
- Kötü amaçlı yazılımlara izin verme ilk etapta sisteme girme veya sistemi değiştirme yeteneğini engelle

Önlemenin dört ana unsuru vardır:

- Politika
- Farkındalık
- Güvenlik açığı azaltma
- Tehdit azaltma

- Önleme başarısız olursa, aşağıdaki tehdit azaltma seçeneklerini desteklemek için teknik mekanizmalar kullanılabilir:
  - Tespit etme
  - Tanımlama
  - Kaldırma

Nesiller boyu Anti-Virüs Yazılımı

Birinci nesil: basit tarayıcılar

- Kötü amaçlı yazılımı tanımlamak için kötü amaçlı yazılım imzası gerektirir
- Bilinen kötü amaçlı yazılımların tespiti ile sınırlıdır

İkinci nesil: buluşsal tarayıcılar

- Muhtemel kötü amaçlı yazılım örneklerini aramak için buluşsal kuralları kullanır
- Başka bir yaklaşım bütünlük kontrolüdür.

Üçüncü nesil: aktivite tuzakları

- Kötü amaçlı yazılımları virüs bulaşmış bir programdaki yapısından ziyade eylemleriyle tanımlayan, bellekte yerleşik programlardır.

Dördüncü nesil: tam özellikli koruma

- Birlikte kullanılan çeşitli anti-virüs tekniklerinden oluşan paketlerdir
- Tarama ve aktivite tuzağı bileşenlerini ve erişim kontrolü özelliğini içerir

Sandbox Analizi

- Emüle edilmiş bir sanal alanda (sandbox) veya sanal bir makinede potansiyel olarak kötü amaçlı kod çalıştırma
- Kodun, gerçek bir sistemin güvenliğini tehdit etmeden davranışının yakından izlenebildiği kontrollü bir ortamda yürütülmesine izin verir.
- Potansiyel olarak kötü amaçlı yazılımları bu tür ortamlarda çalıştırmak, karmaşık şifreli, polimorfik veya metamorfik kötü amaçlı yazılımların algılanmasını sağlar.
- Korumalı alan analiziyle ilgili en zor tasarım sorunu, her bir yorumlamanın ne kadar süreyle çalıştırılacağını belirlemektir.

Ana Bilgisayar Tabanlı Davranış Engelleme Yazılımı

- Bir ana bilgisayarın işletim sistemiyle bütünleşir ve kötü amaçlı eylem için program davranışını gerçek zamanlı olarak izler
  - Potansiyel olarak kötü amaçlı eylemleri, sistemi etkileme şansı bulamadan engeller
  - Yazılımı gerçek zamanlı olarak engeller, böylece parmak izi veya buluşsal yöntemler gibi virüsten koruma algılama tekniklerine göre bir avantaj sağlar

Sınırlamalar

- Tüm davranışlarının tanımlanabilmesi için kötü amaçlı kodun hedef makinede çalışması gerektiğinden, algılanıp engellenmeden önce zarar verebilir.

Çevre Tarama Yaklaşımları

- Bir kuruluşun güvenlik duvarında ve IDS'de çalışan e-posta ve Web proxy hizmetlerinde tipik olarak bulunan anti-virüs yazılımı
- Bir IDS'nin trafik analizi bileşenine de dahil edilebilir
- Herhangi bir şüpheli trafiğin akışını engelleyen izinsiz giriş önleme önlemleri içerebilir
- Yaklaşım kötü amaçlı yazılımları taramakla sınırlıdır

İki tür izleme yazılımı