BİLİŞİM SİSTEMLERİNE YÖNELİK TEHDİTLER

Öğr. Gör. Halil ARSLAN

Bilişim Sistemlerine Yönelik Tehditler

- Zararlı Yazılımlar
- Ağlara Yönelik Tehditler
- Mobil Güvenliğe Yönelik Tehditler
- Bulut Bilişim ve Tehditler
- Nesnelerin İnterneti ve Tehditler
- Sosyal Mühendislik

Zararlı Yazılımlar (Malware)

Kötü amaçlı, kötücül yazılım - Malicious Software

Bilişim sistemlerinin işlevlerini bozmak, kritik bilgileri toplamak, zarar vermek gibi kötücül amaçlı kullanılan her türlü zararlı kod, program ve yazılımları tanımlamak için kullanılan genel bir ifadedir.

Zararlı Yazılımlar (Malware)

- **Virüsler**
- **Solucanlar (Worms)**
- **Truva Atları (Trojans)**
- Casus Yazılımlar (Spyware)
- Rootkit (Kök kullanıcı takımı)
- Fidye Yazılımları (Ransomware)
- (Şantaj) Uzaktan Yönetim Aracı (RAT)
- Cryptojacking (Kripto para madenciliği)
- Arka kapı (Backdoor)
- Tarayıcı ele geçirme (Browser hijacking)
- Korunmasızlık sömürücü (Exploit)
- Klavye dinleme sistemi (Keylogger)
- Mesaj sağanağı (spam) (Yığın ileti)

Zararlı Yazılımlar (Malware)

Virüsler (Virus)

Bilişim sisteminin normal çalışmasını, kullanıcının haberi olmadan değiştirmeye çalışan, kendini gizleyen ve bir dosyaya bulaşan, bir bilgisayardan diğerine bulaşmaya çalışan, zararlı kodlar içeren bir bilgisayar programıdır. Bulaştığı dosyanın etkileşime geçmesi, çalışması ile virüs harekete geçer.

Solucanlar (Worms)

Bilişim sisteminde bir dosyaya ilişme ihtiyacı veya insan etkileşimi olmadan kendi başlarına otomatik olarak çalışabilen, başka sistemlere yayılmaya çalışan zararlı kodlar içeren bir bilgisayar programıdır. E-posta, download, reklam vb. yollar ile bilgisayara girebilirler.

Truva Atları (Trojans)

Bilinen bir yazılımın içerisine eklenmiş veya hedeflenen sistemler için yazılmış içerisinde zararlı kodlar barındıran programlardır. Eklendikleri program dosyasının çalışması ile aktif olurlar.

Arka kapı, rootkit, Banking, DdoS, Spy, Psw, proxy, clickers, vb. gibi zararları içerirler.

Zararlı Yazılımlar (Malware)

Rootkit

İşletim sistemi çekirdeğine sızarak saldırgana tam yetki veren zararlı yazılımlardır. Kernel, firmware, application, memory, bootkit, library, hypervisor vmm vb...

Ransomware (Fidye)

Bulaştığı sistem üzerinde dosyaların erişimini şifreleyip engelleyen, dosyaların yeniden kullanımı için fidye talep eden şifreli yazılımlardır. Genellikle kripto para (crypto coin) talep ederler. (WannaCry gibi..)

RAT (Remote Administration Tool - Uzaktan Yönetim Aracı)

Sistemleri uzaktan yönetip teknik destek veya sunucu yönetimi amaçlı faydalı kullanımın kötü amaçlar için yapılmasıdır.

Ağlara Yönelik Tehditler

- Hizmet Dışı Bırakma (DoS) Saldırısı
- Botnetler ve DdoS
- Port Yönlendirme
- Spoofing
- Parola Saldırıları
- ...

Ağlara Yönelik Tehditler

DoS (Denial of Service - Hizmet Dışı Bırakma) Saldırısı

Hedef sistemin kaynaklarını tüketip hizmetlerini geçici veya süresiz olarak aksatarak, görevini yerine getirememesine ve asıl kullanıcılar tarafından ulaşılamamasına neden olan erişilebilirliği hedefleyen bir siber saldırı türüdür.

Botnetler (robot network)

Saldırganlar tarafından trojan veya zararlı yazılımlar ile ele geçirilen ve uzaktan yönetilebilen bilgisayarlardan oluşturulan bir bilgisayar ağıdır. Botnet üyesi bilgisayarlar köle veya zombi olarak ifade edilirler. Botnetler tek bir birim olarak hareket etme yeteneklerine sahiptir. DdoS (Dağıtık DoS) gibi saldırılar için yaygın olarak kullanılırlar.

Tespit Yöntemleri

Virüsler

Tanım: Kendini kopyalayarak diğer dosyalara, program kodlarına ve sistem alanlarına bulaşan zararlı kod parçacıkları. Çalışmak için bir taşıyıcı programa ihtiyaç duyar ve kullanıcı etkileşimi gerektirir.

Tespit Yöntemleri:

- **İmza tabanlı tarama:** Bilinen virüs imzalarının veri tabanıyla karşılaştırma
- **Sezgisel analiz:** Virüs benzeri davranışları tespit etme
- **Davranış analizi:** Programların gerçek zamanlı davranışlarını izleme
- **Sandbox testi:** İzole ortamda dosya çalıştırma
- **Dosya bütünlük kontrolü (FIM):** Hash değerleri karşılaştırma
- **Polimorfik virus tespiti:** Şekil değiştiren virüsleri algılama

Göstergeler:

- Sistem performansında belirgin yavaşlama | Dosya boyutlarında beklenmedik artış
- Program başlatma sürelerinde uzama | Antivirüs yazılımının kendiliğinden kapanması
- Yeni dosyaların otomatik oluşması | Sabit disk aktivitesinde artış
- Sistem kaynaklarının anormal kullanımı | .exe dosyalarının açılmaması

Solucanlar

Tanım: Kullanıcı etkileşimi olmadan ağ üzerinden kendini kopyalayarak yayılan bağımsız zararlı yazılımlar. Host dosyaya ihtiyaç duymadan çalışabilir ve otomatik olarak yayılır.

Tespit Yöntemleri:

- **Ağ trafiği analizi:** Paket içeriği ve akış inceleme
- **Anormal bağlantı taraması:** Port tarama aktiviteleri
- **IDS/IPS sistemleri:** İmza ve anomali tabanlı tespit
- **Ağ davranış anomali tespiti (NBA):** Normal davranıştan sapmaları bulma
- **Güvenlik duvarı günlük analizi:** Bağlantı girişimlerini izleme
- **Bant genişliği izleme:** Trafik artışlarını gözlemleme

Göstergeler:

- Ağ trafiğinde ani ve sürekli artış | Birden fazla sistemde eş zamanlı bulaşma
- Giden bağlantılarda anormal artış | E-posta trafiğinde patlama
- Dosya paylaşım aktivitesinde artış | CPU ve bellek kullanımında artış
- Açık portlarda artış | Güvenlik duvarı loglarında tekrarlı bağlantı denemeleri

Truva Atları (Trojens)

Tanım: Meşru veya yararlı bir yazılım gibi görünen ancak arka planda zararlı işlevler gerçekleştiren programlar. Kendini kopyalamaz, kullanıcı tarafından kasıtlı olarak çalıştırılır.

Tespit Yöntemleri:

- **Uygulama beyaz liste kontrolü:** Sadece onaylı uygulamaların çalışmasına izin verme
- **Dijital imza doğrulama:** Yazılımın güvenilir kaynaklardan geldiğini kontrol etme
- **Sandbox izolasyonu:** Şüpheli dosyaları izole ortamda çalıştırma
- **Tersine mühendislik:** Program kodunu analiz etme
- **EDR sistemleri:** Uç nokta davranışlarını izleme
- **Hash analizi:** VirusTotal gibi platformlarda kontrol
- **Ağ bağlantı analizi:** C&C sunucu iletişimini tespit

Göstergeler:

- Beklenmeyen yeni program yüklemeleri | Tanımadığınız süreçlerin çalışması
- Antivirüs yazılımının devre dışı bırakılması | Güvenlik duvarı ayarlarında değişiklik
- Yeni ağ bağlantıları ve portlar | Kayıt defterinde değişiklikler
- Kullanıcı hesaplarında yetkisiz değişiklikler | Sistem konfigürasyonunda otomatik değişiklikler