|  |
| --- |
| ***Siber Güvenliğin Temelleri*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Siber Güvenlik Nedir?  -Virüsler ve türleri  -Antivirüslerin çalışma prensibi  -Ağ Tehditleri  -Tehditlerden Korunma |

**29.11.2021**

***Siber Güvenlik Nedir?***



-Bireyler için : Güvende hissetmek;kişisel verileri korumak ve gizliliği sağlamak.

-Kurumlar için : Kritik sistemlerin iş sürekliliğini sağlamak ve veri sızıntısını önlemek.

-Devletler için : Vatandaş;kurum ve devlet sistemlerinin siber tehditlere karşı korunması,veri ihlalinin önlenmesi.

-“Gizlilik + Bütünlük + Erişilebilirlik = Siber Güvenlik”

- Siber Güvenlik > Etik hackerlık&Pentester'lığı kapsar.

***Siber Güvenlik***

-Yasal Mevzuatlar

-BGYS Yönetimi

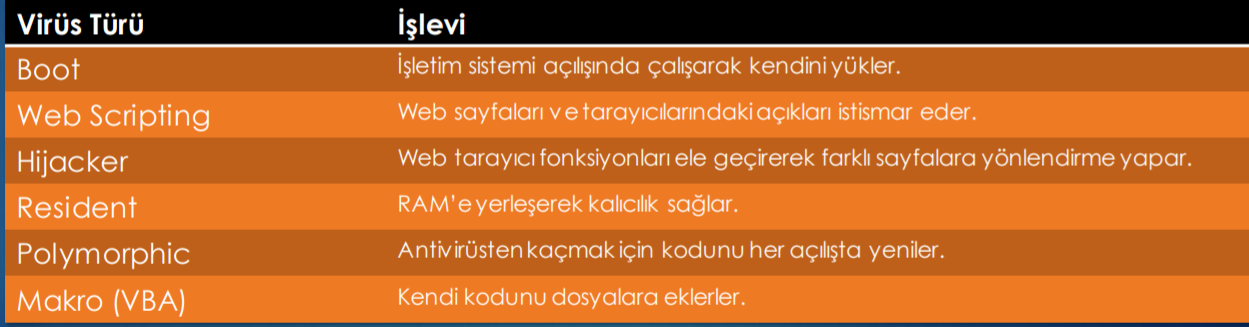
-Risk yönetimi

-Etik hackerlık& Pentesterlık

-Adli bilişim soruşturması ve delil yönetimi gibi başlıkları içerir.

***Zararlı Yazılımlar***

1-)***Virüsler***



-Kendi kendine kopyalanabilen ve yayılarak istemi değiştirebilen yazılımlardır.

-Etkileşime ihtiyaç duyarlar;çalıştırılana kadar sessiz bekleyebilirler.

2-)***Solucanlar(Worms)***



-Virüslerden farklı olarak dosya veya programlara bulaşmazlar.

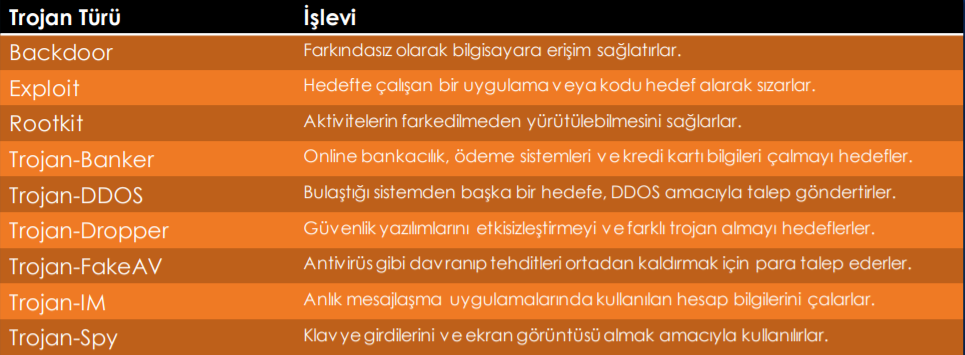
-İnsan etkileşimine veya tetikleyiciye ihtiyaç duymazlar.

-Kendini kopyalayabilir ve yayılabilirler

-Arka kapı(Backdoor) yaratma,dosya silme,veri sızdırma,zombie yapma gibi işlevleri vardır.

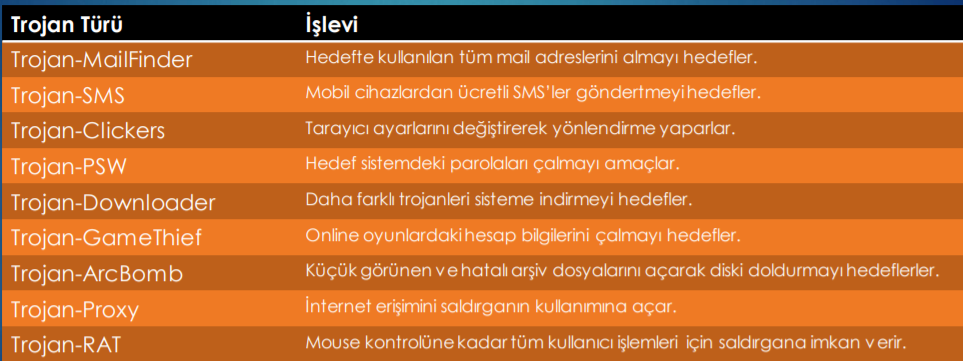
-Meşhur olanları arasında Stuxnet vardır.Nam-ı diğer "ilk siber silah"

3-)***Truva Atları(Trojan)***



- -En belirgin özelliği faydalı gibi gözükmesidir.Buna örnek olarak crack verebiliriz.

-Virüs ve solucanların tüm işlevsel özelliklerini taşırlar.



-IoT cihazların da hedef alabilirler.

-Geniş bir aileye sahiptir.

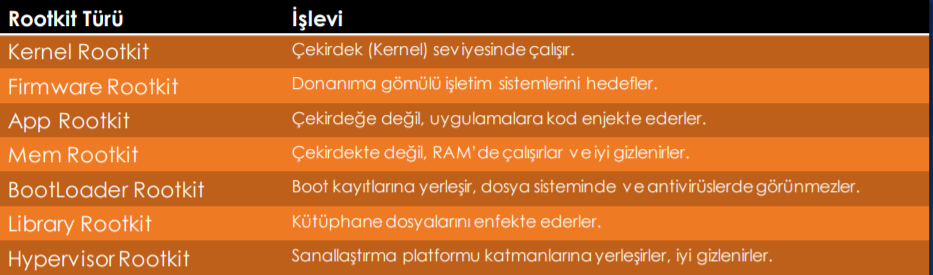
4-)***Casus yazılımlar(Spywares)***

-İşletim sistemlerine bulaşarak farkındasız olarak kullanıcının hassas bilgilerini ifşa ederler.

-Parolalar,e-mail adresleri,web tarayıcı geçmişi,log dosyaları,kullanıcı aktiviteleri gibi bilgileri edinip sahibine iletmeyi hedefler.

-Password Stealers,Keyloggers gibi faaliyetlerde bulunurlar.

5-)***Rootkit***



-İşletim istemi çekirdeğine sızdığı için en tehlikelisidir.

-Tam yetkiyle çalıştığı için eylemlerinde sınır yoktur.

-Tespitleri ve silinmeleri oldukça zordur.

-IoT cihazlarını hedef alabilir.

-Virüs,worms ve trojan'lerin tüm işlevlerini kapsar.

7-)***Fidye Yazılımları (Ransomwares)***

-Dosya sistemini hedef alarak verileri kriptolarlar.

-Verilerin çözülebilmesi için kriptop para talebi görüntülerler.

-Ağ vektörlerini kullanarak kullanıcı etkileşimsiz çalışabilirler.

-En meşhurları arasında “WannaCry” vardır.

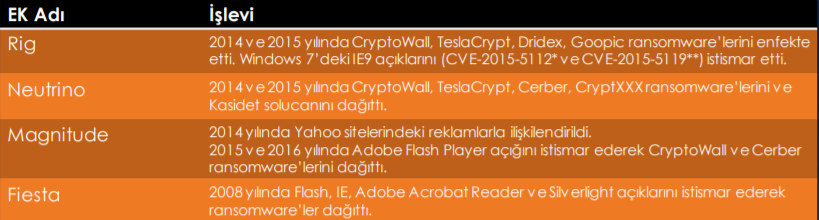
8-) ***Cryptojacking***

-Bilgisayarın kaynaklarını kullanarak saldırgan adına kripto para madenciliği(Cryptomining) yapar.

-Bilgisayar kaynakları tüketiminde anormallik yaratır.

-Gizlilik esaslı kodlanmıştır.

9-)***İstismar Kitleri (Exploit Kit –EK)***



-Popüler yazılımlardaki açıkları(vulnerability) istismar(exploit) ederler.

-Genellikle C,Perl,Python ve Ruby dilleriyle yazılırlar.

-Web sitelerinin kodlarında bulunurlar.

-Filtreleme >>> Tespit >>> İstismar şeklinde çalışırlar.

***Antivirüslerin Çalışma Prensibi***

-Antivirüsler çalışırken 3 çeşit yöntem kullanmaktadır.

1-)***Byte-Signature***

-Yazılımın(virüsün) makine dilindeki karşılığından bir bölümü alınarak tanınır.

2-)***Hash-Signature***

-Yazılımın HASH değeri alınarak tanınır.En ufak bir değişiklikte tanınamaz olacağı için risklidir.

3-)***Heuristic***

-Sezgisel tanıdır.

-Kodun içeriğinden çok davranışları izlenerek tanınmaya çalışılır.

-Performans ve zaman kaybettirebilirler.

***Owasp TOP10***



***Ağ Tehditleri***

1-)***Denial of Service(Hizmet dışı bırakma) -DOS***

-Hedef sistemin kaynaklarını tüketerek hizmet(cevap) veremez hale getirilmesidir.Sistemin kaldırabileceği yükün üstüde anlık iş talepleri göndermesiyle oluşur.

-Erişilebilirlik durumunu hedefler.Sadece web sayfalarına yönelik değildir.

-Tekil kaynaklıdır.Çoklu kaynaktan yapılanı DDOS'tur.

-MAC flooding,ICMP Smurf,TCP SYN Flood DOS ataklarına birer örnektir.

2-) ***Distributed Denial of Service(Dağıtık Hizmet Dışı Bırakma) -DDOS***

-DOS'a göre çoklu kaynakları yapılıdğı için güçlendirilmiş halidir.

-Botnet ağına düşürülmüş zombi bilgisayarların komuta edilmesiyle yapılır.

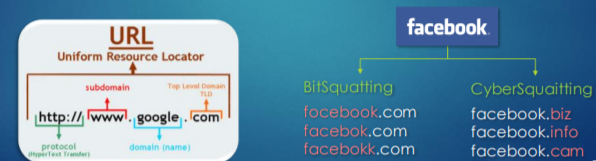
-Zombi bilgisiyarlara sadece DDOS yaptırılmaz.

3-) ***Pivoting ve Port Forwarding***

-Pivoting, ele geçirilen sistem üzerinden başka sistemlere saldırmaktır.

-Port açığı bulunan bir sunucu pivot olarak seçlilir ve açık portunda yönlendirme yapılarak diğer sistemlerin portlarına erişmek amaçlanır.

4-) ***BitSquatting ve CyberSquatting***



-Bitsquatting,var olan kurum domaninlerinin farklı ama en yakın hallerinin alınarak kötü amaçla kullanılmasıdır.

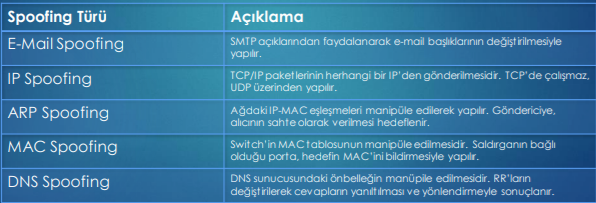
-CyberSquatting,var olan kurumların domanin adlarının aynısını ama TLD(Top Level Domain)'lerine yakın hallerini alarak kötü amaçla kullanmaktır.

5-)***Paket Manipulasyonu***

-İstek paketlerinin(Request) içeriğini değiştirerek,gelen cevap paketlerinden bigli edinmek,liste çıkarmak amaçlanır.

-Bilgisayar,sunucu,kullanıcılar,uygulamalar,servisler,paylaşımlar hakkında bilgi edinilir.

6-)***Spoofing***



- Alıcıyı,güvenilir bir kaynaktan veri aldığı yönünde manipüle etmektir.

7-) ***Session Hijacking***

-Web ortamında başarılı bir kimlik doğrulamanın taklit edilmesiyle yapılır.

-Saldırgan,oturum kimliği (Session ID) bilgisi içeren tokenları çalar ve o da oturum açar.

8-) ***Pass The Hash***

-Parola saldırı olarak da bilinir.

-Parola yerine,ağ trafiğinde şifreli(hash'i) olarak gönderilen parolanın kullanılmasıdır.

-NTLM ve Kerberos protokollerinde ki SSO(Single-Sing-On) özelliğinin istismar edilmesidir.

-Offline olarak gerçekleştirilir.

-Windowsta bu işlemleri yürüten Local Security Authority Subsystem(LSASS) uygulamasına saldırılır.

-LSSAS'ın uygulaması %SystemRoot%\System32\Lssas.exe'dir.

-Parolalara ait hash değerlerini saklar.

9-) ***Sosyal Mühendislik***

-Teknik saldırıların denenmemiş veya başarısız olması halinde,hedefe erişimi bulunan insaları manipüle etme girişimidir.

-Hedefe erişimde kolaklık sağlamaları adına insanların siber güvenlik bilgisinden faydalanılır.

-Hassas bilgi edinmek adına,insanların ilgisini çekebilecek linklere tıklatma,içerikler indirtme yazılı veya sözlü ortamlarda hassas bilgi alma,fiziksel veya dijital giriş yetkilerini elde etme gibi amaçlar doğrultusunda yapılır.

***Tehditlerden Korunma***

***Başlıca Bireysel Önlemler***

-Tüm platformlarınızda ücretli antivirüs yazılımları kullanın ve değerlendirerek tercih ediniz.

-İnternet tarayıcılarınıza antivürüs eklentileri(extension,add-on) yükleyin.

-Kaynaklarınızı monitör edin ve ağ trafiğinizi gözlemleyin.

-Güncelleştirmeleri(OS ve APP) ertelemeyin ve buna yüksek önem gösterin.

-Yedeklemeden kaçınmayın;bunu sık yapın ve offline olarak saklayın.

-Yüksek haklara sahip kullanıcıları kullanmaktan kaçının ve UAC'i kapatmayın.

-Sabit ve taşınabilir depolama birimlerinizde disk encryption kullanın.

-İşletim sistemlerinizde security hardening(Güvenlik güçlendirme) uygulayın.

***Başlıca Kurumsal Önlemler***

-Bilgisayar kullanan tüm personele bilgi güvenliği ve farkındalık eğitimleri verin.

-Merkezi antivirüs uygulamaları kullanın ve kullanıcı etkileşimsiz olarak dağıtın.

-Güncelleştirmeleri merkezileştirin ve kullanıcı etkileşimsiz olarak zorlayın.

-IPS,IDS,DLP,AV gibi özellikli donanımsal güvenlik duvarları kullanın.

-Güvenlik ve güncelleştirme poliçelerinizi mantık hatasız uygulayın.

-Yazma izinlerini doğru verin.

-Yedeklemeleri otomatik,zamanlı,merkezi ve offline özellikte gerçekleştirin.

-ISO27001 ve BGYS önlemlerini "gerçek" ortamda uygulayın.

-BYOD(Bring Your Own Device)'dan mümkün oldukça kaçının ve NAP kullanın.