SİBER TEHDİT İSTİHB. VE TEHDİT AVCILIĞI

GİRİŞ

- **IoC (Indicator of Compromise)**
  - ihlal göstergesidir , zararlı ve kötü amaçlı yazılımları tespit edilmesinde kullanılır.
  - **IoC Olabilecek Veriler :**

I. Normal dışı DNS sorguları
II. Normal dışı processler
III. Normal dışı uygulamalar
IV. Kaynaklara normal üstü sayılarda erişimler
V. Yönetici ve yetkili kullanıcı hesapları aktiviteleri
VI. Normal dışı dosya indirme yada güncelleme
VII. Zararlı yazılımlar tarafından kullanılan Ip ve domain adresleri

VIII. Nadiren kullanılan yada kullanılmayan portların kullanımı
IX. Oltalama adreslerine erişim
X. Zararlı yazılım hash veya imzası
XI. Normal dışı boyutlarda HTTP istek-cevapları
XII. Yapılandırma dosyalarının, kayıtların veya cihaz ayarlarının yetkisiz olarak değiştirilmesi
XIII. Yüksek boyutlarda giriş deneme sayısı

- **CC (Command and Control)**

- Ele geçirilen sistemlere uzaktan komut göndermek için sunucu/bilgisayardır

Zararlı aktiviteyi saklamak için farklı servislerde kullanılabilir.

i. Dosya paylaşım servisleri
ii. Ortak kullanım servisleri
iii. Sosyal medya platformlarını API'leri
iv. Webmail servisleri
v. Legit sitelerin kullanımı

- **LOG**
  - Sistem ve ağlardaki iz kayıtlarıdır.

Log Kaynakları

1. İşletim sistemleri
2. Veritabanı Yönetim Sistemler
3. Sanallaştırma Teknolojileri
4. Güvenlik Cihazları
5. Ağ ve Sistem Ürünleri
6. Web Uygulama Servisleri
7. Kimlik Doğrulama Sistemleri
8. Domain Controller

- **SIEM (Security Information and Event Managemenet)**

- Güvenlik bilgileri ve olay yönetimidir
- Sistemlerde ki verileri , logları analiz etmek için toplayan güvenlik cihazlarıdır
- sistem ve ağlarda ki anormallikleri tespit etmeye ve geri dönük incelemeler yapmayı sağlar
- Üst seviye siem'ler (IBM qradar,splunk,fortisiem,logrhythm) gelen verileri parse etme ve incelenebilir formata dönüştürmeyi sağlar

- **OSINT (Open Source Intelligence)**
  - Açık kaynak istihbaratıdır
  - sosyal medya , radyo , arama motorları , whois , reverse dns , shodan yani kısaca açık ulaşılması kolay yerler

VIRUSTOTAL

- zararlı yazılımları onlıne tespit etmek ve hakkında bilgi alma yeridir.
- sistemin çalışma mantığı file,url yada direkt ip filan olarak dosyayı gösterince dosyayı açıp 62 tane antivirüs programından geçirip kontrol eder ve detaylı olarak çıktısını çıkarır

MITRE

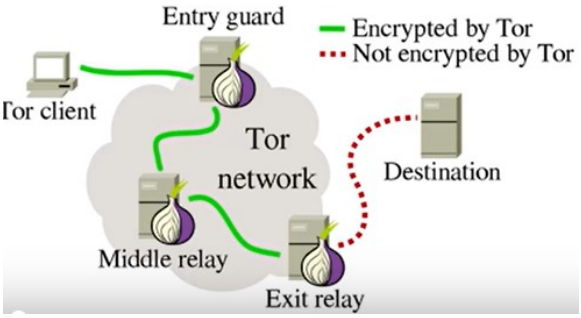
- gerçek senaryolar ile hazırlanmış tehdit sürecini tamamen anlatan teknik , taktik , prosedürleri kısace bir ansiklopedi gibi
- www.mitraattcak.com

ID	İsim	Açıklama
TA0001	Initial Access	Saldırganın sisteme ilk erişim sağlama teknikleri
TA0002	Execution	Zararlı kodun sistemde yürütülme teknikleri
TA0003	Persistence	Saldırganın sistemde kalıcılık sağlama teknikleri
TA0004	Privilege Escalation	Saldırganın sistemde yetki yükseltme teknikleri
TA0005	Defense Evasion	Güvenlik tedbirlerinin atlatılması teknikleri
TA0006	Credential Access	Sistemde kullanılan kimlik bilgilerinin ele geçirilmesi teknikleri

ID	İsim	Açıklama
TA0007	Discovery	Saldırganın sızdığı sistemi tanıma ve keşfetme teknikleri
TA0008	Lateral Movement	Ağdaki diğer sistemlere erişme teknikleri
TA0009	Collection	Sistemdeki kritik bilgilerin toplanması teknikleri
TA0011	Command and Control	Komuta kontrol sunucularıyla iletişime geçme teknikleri
TA0010	Exfiltration	Ele geçirilen bilgilerin sistemden çıkarılması teknikleri
TA0040	Impact	Sistemi bozmak ve manipülasyon için kullandığı teknikler

DEEBWEB

- netin karanlık yüzü ve arama motorları endeksli değil
- girişler için tor(the onion router) denen özel ağ ve tarayıcı kullanılır.
  - anonimlik ve şifreli haberleşme sağlar



  - ileri zararlı yazılımların çoğu tor altyapısını kullanmaktadır sebebi ise devletlerin bunları engellemek için aldığı ip , domain gibi önlemleri tor altyapısı kullanrak anonimlik kazanmasıdır.

Temel olarak 2 yöntem görmekteyiz:

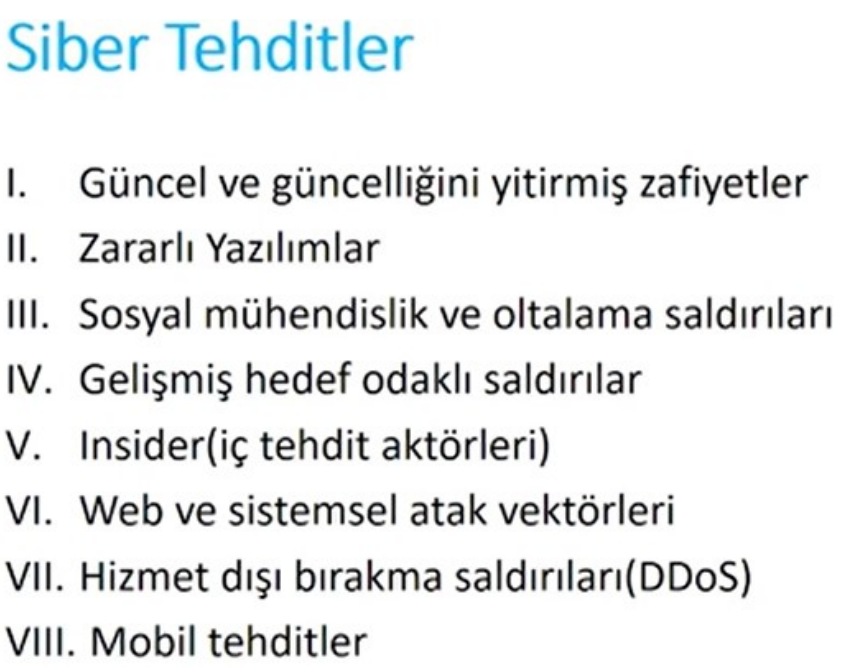
1. Zararlı yazılım bulaştığı sisteme tor altyapısı kurup tor ağı üzerinden komuta kontrol merkezi ile haberleşir.
2. Zararlı yazılım; Tor altyapısı kurulu bir Proxy üzerinden Tor ağındaki komuta kontrol merkezi ile haberleşir.

HONEYPOT (BALKÜPÜ)

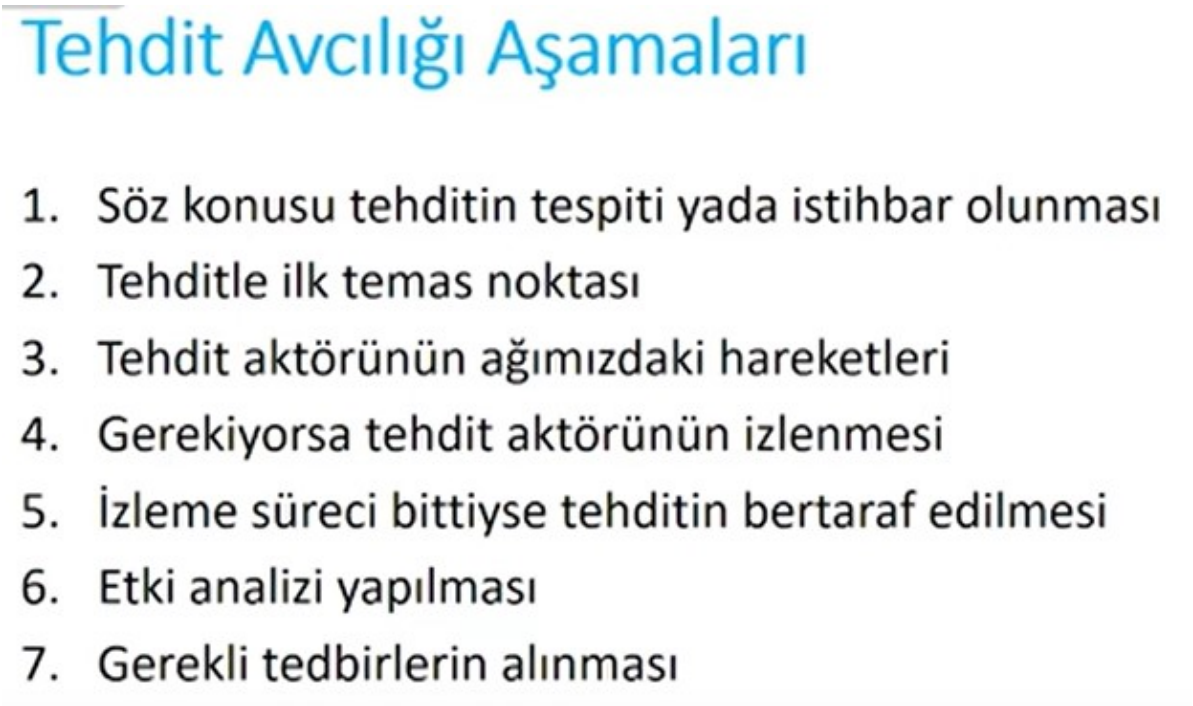
- Saldırganların sisteme ilgisini çekmek için kurulan bir tuzak. düşük etkileşimli ve yüksek etkileşimli olarak ikiye ayrılır. düşükte kontrol saldırgana verilmez ama yüksekde saldırganın kontrolü ele almasına izin verir.
- T-pot : içerisinde docker teknolojisi kullanarak farklı farklı balküpü bulunduran framework , kurulup saldırılar , izlenebilir. bazı balküpleri :
  - tanner : web balküpüdür , web sunucusu gibi davranır ve saldırganları dener
  - dionaea : zararlı yazılımları yakalamada kullanılır. atak senaryolarını tespit eder

TEHDİT AVCILIĞI

- Sistemde gizlenen tehditleri proaktif olarak arama



- Tehditin yada saldırının aşamaları önemlidir neler yapmış ve ne yapmak istiyor gibi bilgiler hayatidir. Direkt iletişimini kesmek yanlış olur öncesinde önlemler alınarak izlenmelidir.



- SOC (SECURITY OPERATİON CENTRE)
  - Güvenlik operasyonları merkezi. Sistemin kalbidir , güvenlik durum kontrolleri burada yapılır ve soz analistleri , tehdit isth. analistleri , tehdit avcıları ve güvenlik ekipleri bulunur.
  - Görevleri : olay tespit , analiz , raporlama , koordinasyon ve ileri görüşlülük ile önden koruma

- ALANLAR :
  - **Sızma testi Uzmanlığı** : sistemdeki zaafiyetler ve oluşabilecek tehditlerin tespitini sağlar
  - **Olay müdahale uzmanlığı** : gerçekleşen saldırıdan sonra inceleme ve sabep sonuçlarını çıkararak önlemleri almayı sağlar
  - **SOC analistliği** : gelen istihbarat ve ihbarları değerlendirerek incelemeye alanlar
  - **Zararlı yazılım analizi uzmanlığı** : SOC ile gelen bilgileri değerlendirerek inceleme ve zararlı yazılımı inceleme

- **Tehdit istihbaratı uzmanlığı** : genel ihbar inceleme ve değerlendirme

- Windows event log (Olay görüntüleyici)
  - yazılım ve olayları denetleyip izlemeyi sağlar
  - 3 farklı event log vardır : application , system , security
    - Application : uygul. ve kullanıcı prog. gelen loglardır. Host-based güvelik araçları (anti-virüsler) genelde büyük kısmı oluşturur.
    - System : Farklı bileşenlerden gelen loglardır.
    - Security : Doğrulama ve güvenlik işlemleri logları tutar. Local ve Group policy ayarları ile security logları ayarlanabilir

Event Log Konumları

Event Log	Event Log Konumu
Application(Uygulama)	%SYSTEMROOT%\System32\Winevt\Logs\Application.evtx
System(Sistem)	%SYSTEMROOT%\System32\Winevt\Logs\System.evtx
Security(Güvenlik)	%SYSTEMROOT%\System32\Winevt\Logs\Security.evtx

Neden Önemli?

1. Başarılı ve başarısız logonları izlemek
2. Başlatılan , durdurulan ve oluşturulan servisleri izlemek
3. Belli uygulamaların kullanımını izlemek
4. Denetim politikasındaki değişiklikleri izlemek
5. Kullanıcı izinlerindeki değişiklikleri izlemek
6. Kurulan uygulamalardan oluşan olayların izlenmesi(anti-virüs)

Event ID'ler (Logon)

Event ID	Açıklama
4624	Başarılı Logon
4625	Başarısız Logon
4634	Başarılı Logoff
4648	Açık kimlikle Logon
4672	Özel ayrıcalık atanması
4768	Kerberos Ticket(TGT) isteği
4769	Kerberos servis ticket isteği
4778	Oturuma tekrar bağlantı sağlaması
4779	Oturumla bağlantı koparma

Event ID	Açıklama
4720	Hesap oluşturma
4722	Hesap etkinleştirme
4724	Parola sıfırlama girişimi
4728	Global group'a kullanıcı ekleme
4732	Local group'a kullanıcı ekleme

Logon Types

Logon Type	Logon Title	Açıklama
2	Interactive	Kullanıcının fiziksel olarak bilgisayara giriş yapması.
3	Network	Kullanıcı veya bilgisayarın networke giriş yapması
4	Batch(Grup)	İşlemlerin bir kullanıcı adına yürütüldüğü toplu işler (Scheduled Tasks)
5	Service	Service Control Manager tarafından başlatılan servisler(Telnet)
7	Unlock	Sistemin kilidinin açılması(ekran koruyucu)
8	NetworkClearText	Clear-text kimlik bilgileri gönderilmesi(basic auth.)
9	NewCredentials	Credential klonlanması ve yeni credentialler elde edilmesi (Runas)
10	RemoteInteractive	Uzaktan yönetim servisleri ile giriş (Terminal services ,RDP)
11	CachedInteractive	Cache'deki credentiallerin kullanılarak giriş

Parola Saldırısı Avı

Event ID	Logon Type	Açıklama
4625	3	Event ID 4625 (failed logon) Logon Type 3 (network logon) Belli bir zaman aralığında yüksek sayıda belirtilen Event ID ile Logon Type tespit edilmesi halinde bir Password Spraying Attack gerçekleşmiş olabileceği düşünülebilir.

- **Pass The Hash Avı** : hash bir metnin bir daha geri döndürülemeyecek şekilde şifrelenmesidir böylece güvenli olduğundan bilgisayar parolaları ram içinde hashleyerek tutar. Saldırganlar ramlere ulaşarak bu hashleri ele geçirerek parolasız olarak sistemlerde yetki yükseltebilir

Event ID	Logon Type	Açıklama
4624	3	Event ID 4624(Başarılı Logon) Logon Type 3(network logon)

- PsExec Avcılığı
  - Uzak bilgisayarlarda komut çalıştırmamıza yarayan araçtır
  - Yönetici kimlik bilgilerini kullanarak SMB bağlantısı kurar
  - PSEXESVC.EXE alıcı processinin hedef sistemin ADMIN$ paylaşımına ekler
  - Named Pipe kullanarak girdi ve çıktıları gönderir

Event ID	Açıklama
5145	Paylaşım isteği yakalanması(ADMIN$ ve IPC$ odaklanmalıyız)
5140	Paylaşıma başarılı erişim
4697/7045	Servis oluşturma
4688	Yeni Process oluşturma (Sysmon EID 1)

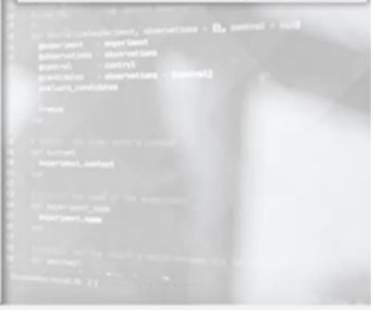
- Sysmon

- Sistem monitörüdür , logları etkinlikleri izleme ve kaydetmekle görevlidir

Event description	Event ID
Process Create	1
File creation time changed	2
Network connection detected	3
Sysmon service state change	4
Process terminated	5
Driver loaded	6
Image loaded	7
CreateRemoteThread detected	8
RawAccessRead detected	9
Process accessed	10

Event description	Event ID
File created	11
Registry object added or deleted	12
Registry value set	13
Registry object renamed	14
File stream created	15
Sysmon configuration change	16
Named pipe created	17
Named pipe connected	18
WMI filter	19
WMI consumer	20

Event description	Event ID
WMI consumer filter	21
DNS query	22
Error	255



- ELK : ElasticSearch , Logstash , Kibana
  - ElasticSearc : arama ve indeksleme motorudur , Apache Lucenee altyapısı kullanır , açık kaynaklıdır
  - Logstash : Kaynaklardan verileri toplayan , bu verileri işledikten sonra indekslemek üzere elastiksearch motoruna ilete yapıdır , verileri toplar ve anlamlı hale getirir
  - Kibana : Önceki adımları kullanışlı web arayüzü haline gelmiş sistemdir
  - Tüm bunlar verilerin alınması , ayrıştırılması , depolanması gibi kolaylıklar sağlar
  - Tüm kaynaklardan gelen loglar , endpoint ürünlerden gelen loglar , Balküpünden gelen veriler , ham olarak gelen tehdit istihbaratı verisi , işlenmiş tehdit istihbatı verisi , incelemeye tabi tutulabilecek veriler

ZARARLI YAZILIM (MALWARE) ANALİZ TEMELLERİ

- Ransomware (Fidye Yazılımı)
  - bilgisayar sistemindeki verileri , erişimleri engellemek için bunları şifreleyerek fidye talep etme.

    - Wannacry , Ryuk , DJVU , Bitlocker

- Worm (Solucan)
    - Bulaştığı sistemleri kopyalarak çoğaltan ve sıçrayan sistemler
    - Stuxnet , Voyager , Zotob

- Adware (Reklam Yazılımı)
    - Bulaşılan cihazlarda pazarlama için faaliyetleri toplar
    - Firebal , DollarRevenue , Deskad

- Trojan (Truva Atı)
    - İyi niyetli yazılım gibi görünen girince zararlı olan tür
    - DarkComet , Zeus , FlashBack , Cerberus

- Spyware (Casus Yazılım)
    - Sistemde casusluk faaliyeti gösteren geniş çatısı olan bir genel adlandırma
    - Zlob , BlazeFind , PseudoManuscrypt

- Mobile Malware (Mobil Zararlı Y.)
    - AlienBot , Cerberus , Anubis , Hydra

- Rootkit
    - Hedef sisteme erişim ve yönetim sağlaması amacıyla oluşturulan yazılımlar
    - Stoned Bootkit , Rovnix , Olmasco

HAFIZA ANALİZİ (MEMORY ANALYSİS)

- Malwareleri bulmanın birçok yolu vardır ancak yükselişte olan yöntem budur.tercih edilme sebepleri
    - geleneksel yöntemlerin yetersizliği
    - daha proaktif (canlı) şekilde malware izleme
    - kalıcılık yöntemlerinin tespiti
    - malware amaçlarının tespiti
    - malwarenin kaçınma yöntemlerini daha kolay tespit etme (shellcade injection , dll and reflective dll injection , process hollowing , api hooking)

- VOLATİLİTY
    - Hafıza imajı analizidir
    - Parametreleri : imageinfo , pslist , cmdscan , connscan , pstree , dlllist , iehistory , malfind , yarascan , netscan

---

** shellcade injection → saldırganın sisteemimizde kodları çalıştırması

** dll and reflective dll injection → bir dll dosyasına processin adres alanını ekleyip daha sonra çalışmasını sağlayarak kaçma tekniğidir

** process hollowing → bir dosyanın içini boşaltıp zararlı yazılımları yüklemek

** imageinfo → imajın hangi işletime ait oludupunu belirten profil

** pslist → Sistemde çalışan süreçleri listeler ve bilgiler verir

** cmdscan → komut isteminde çalışan komutları listeler

** connscan → sistemin ağ bağlantılarını görmeyi sağlar

** pstree → processlerin ağaç şeklinde birbiri ilişkileriyle görmeyi sağlar

** dlllist → çalışan processlerin çağırdığı dllleri listeler

WEBSHELL

- Siber saldırı başarıyla gerçekleştikten sonra web sunucusuna uzaktan erişmeye yarayan kod parçası

- Desteklenen herhangi bir yazılım dili ile geliştirilebilir.
- Sistemlere Yükleme : sql injection , Remote code execution , rfı ve lfı , açık yönetim servisleri , sosyal mühendislik saldırıları

B374K

- PHP tabanlı , görsel arayüzlü webshelldir

Webshell Tespiti : Anti-virüsler , sistemde anormal kullanım süreleri , dosyaları anormal zaman damgaları , dosyalarda şüpheli kelimeler , loglarla trafikten tespit , şüpheli oturum açmalar

Webshell Avcılığı

- LOKI IOC Scanner , Neopi , BackdoorMan , PHP-Malware-Finder
- bunların bir tanesini değilde hepsini kullanmak daha iyidir birinin bulamadığını diğeri bulur.

** Neopi → farklı istatistiksel metodlar kullanır ve python scriptidir.

** LOKI IOC Scanner → ücretsiz ve basit mantıkla çalışır