

Giriş Karışık (Intro Mix)

Bknz: OSI Katmanları

Hizmet Engelleme Neden Yapılır?

Finansal kazanç, siyasal manifestolar, Spam e-posta bildirimi (botnet), Gövde gösterisi, diğer saldırıları gizleme (log kirlenmesi), ihtiyaç oluşturma (anti-ddos)

DoS, tek kaynaktan hedefe (exploitable -> makineye gönderilir ve crash olur. | Kolay engellenebilir. | Kolay hasar verilebilir.)

DDoS, farklı kaynaklardan tek hedefe (korunumu zor, anonimlik için daha iyi)

Botnet (zombi pc)

1. Zararlı yazılımlar (virüs, rat, trojan)

Film oyun siteleri, uygulama edinme portalları, yazılım ve uygulama güncelleme servisi, web portalları

1. Silahlı exploitler (wanna cry)
2. Ev ağı ve IoT cihazları (mirai botnet)

Bknz: HomeGateway vs Modem

Mirai (bütün ipleri tarayalım, default panellere, default giriş bilgisi)

Botnet mining

WireX Android Botnet (1 günde bütün public ip değişiyor durdurulması zor)

pDoS

Arp, broadcast storm

ICMP Fragmentation

Layerlar boyunca DDoS'lar

Layer 7

Get Flood

Post Flood

Yük Saldırıları (AB Tool)

Güvenlik Zafiyetleri ve Exploitler

Slow HTTP

DNS Genişletme (DNS Amplification)

Siber Ölüm Zinciri

1- Keşif(Reconnaissance)

Aktif - Pasif Bilgi Toplama

2- Silahlanma(Weaponization)

Silahın keşif doğrultusunda geliştirildiği aşama.

3- İletme(Delivery)

APT kodunun kurbanı sömürmek için hedef bilgisayara geçmesidir. Phishing ile zararlı yazılım bulaştırılır.

Genelde en zayıf halka seçilerek spear phishing gerçekleştirilir. Genelde word ve pdf gibi ek içermektedir.

Ek ile apt kurum içi ağa erişir.

4- Sömürme(Exploitation)

Hedef sistemde zafiyet varsa bu işlemde zafiyet sömürülür ancak çoğu apt saldırısı phishing ile gerçekleştirildiğinde içeride çalışması yeterlidir.

5- Installing

Varlığa kötü amaçlı yazılım yüklemek.

6- Komuta ve Kontrol(Command and Control)

İletişim APT kodlarını hedef ağa yerleştirir. APT kodunu tamamen ve daha derin bir şekilde yönetmesine, veri göndermesine ve logları silmesine olanak sağlar.

7- Hedeflenen Eylem(Action on Objectives)

Veri çalma, değiştirme, silme, başka sisteme sıçrama...

Zafiyet Analizi Testleri ve Türleri

Web

WAN

LAN

WiFi

DoS / DDoS

Sosyal Mühendislik

Yazılım Analizi

Mobil Uygulama Analizi

Fiziksel Testler

Red Teaming

CIA

Gizlilik (Confidentiality)

Bütünlük (Integrity)

Erişilebilirlik (Availability)

nc -lvp 6666

Sql

Directory path traversal


Lfi

Valhalla

Loki - signature based

Naxtron-systems.com/valhalla

Valhalla Rule Feeder



Valhalla, Loki ile aynı şirketin sunmuş olduğu bir ürün. Ücretsiz olarak güncel YARA kuralları almamızı sağlıyor. Valhalla'da güncel olarak +13000 Yara kuralı bulunmaktadır. Günlük Olarak Yara kuralları güncellenir. Get Access API key olmadan sadece DEMO API key ile gelen YARA kurallarını kullanabilirsiniz. Get Access API key abone olunan şirketlere sağlanmaktadır.

```
from valhallaAPI.valhalla import ValhallaAPI
```

```
import os.path
```

```
save_path = 'C:/Users/Pwnlab/Desktop/loki/signature-base/yara'
```

```
api = ValhallaAPI(api_key = "{api_key}")
```

```
save_path = api.get_rules_text()
```

```
with open('valhalla-rules.yar', 'w') as vh:
```

```
    vh.write(save_path)
```

Tüm bu işlemleri yaptıktan sonra Linux veya Windows tarafında bir crontab(cronjob) ekleyerek güncel kurallardan anlık olarak beslenebiliriz.

```
0 03 1-31 * * /usr/bin/python3 /home/loki/valhalla/Desktop/APIscript.py
```

Ayın her günü gece saat 03:00'da API kod betiğimiz çalışarak, /yara dizinin altına en güncel YARA kural setini yazdıracaktır.

NOT: Loki'de YARA kurallarının aynısı aynı dizine yazılmış olsa bile, algoritması sayesinde sadece bir tanesini çalıştıracaktır ve performans kaybının önüne geçecektir.

crontab.guru

IoC (Indicator of Compromise), bir olay incelendikten sonra o zararlı hakkında çıkartılan;

- IP adresleri
- Kötü amaçlı yazılım dosyaları
- MD5 Hash'leri
- Botnet vb. Komutları
- C2 URL & Domain

Ve daha fazlasından oluşur. IoC'lerin analistlere olay analizi sırasında büyük kolaylık sağlar. IoC'lerin amacını kısaca böyle açıklayabiliriz.



Sandbox Nedir?

Sistemi ve platformu etkilemeden program çalıştırılmasını sağlayan yalıtılmış test ortamıdır.

Any.run

Cuckoo - cuckoo ubuntu host only - win7 agent ile haberleşiliyor

bazaar.abuse.ch - MalwareBazaar

virusshare.com - malwares

Size, event id logs, CSRR.exe, SMSS.exe