

Campfire-1, evtx、pf(EvtxECmd、Timeline Explorer、PECmd)

Sherlock Scenario

In this Sherlock, you will familiarize yourself with Sysmon logs and various useful EventIDs for identifying and analyzing malicious activities on a Windows system. Palo Alto's Unit42 recently conducted research on an UltraVNC campaign, wherein attackers utilized a backdoored version of UltraVNC to maintain access to systems. This lab is inspired by that campaign and guides participants through the initial access stage of the campaign.

* * *

About Campfire-1

In this Sherlock activity, players will examine artefacts and logs from a Domain Controller, as well as endpoint artefacts from where Kerberoast attack activity originated. We will explore what to look for to properly identify Kerberoasting attack activity and how to avoid false positives given the complexity of Active Directory.

因win11直下載失敗，改由linux下載並轉到win11

指令：`wget.exe -r -np http://192.168.64.2:8000/Triage/`

文件：眾多pf檔、2個evtx)

使用工具：EvtxECmd、Timeline Explorer、PECmd

工具參考：

- <https://ericzimmerman.github.io/#index.md>
- <https://github.com/EricZimmerman/evtx>
- <https://github.com/EricZimmerman/PECmd>

指令：

```
- EvtxECmd.exe -f "C:\Users\TS0\Downloads\192.168.64.2+8000\Triage\Domain
Controller\SECURITY-DC.evtx" --csv "C:\Users\TS0\Downloads\log" --csvf
SECURITY-DC-OutputFile.csv
- EvtxECmd.exe -f
"C:\Users\TS0\Downloads\192.168.64.2+8000\Triage\Workstation\Powershell-
Operational.evtx" --csv "C:\Users\TS0\Downloads\log" --csvf Powershell-
Operational-OutputFile.csv
```

* * *

`PECmd.exe -d`

```
"C:\Users\TS0\Downloads\192.168.64.2+8000\Triage\Workstation\2024-05-21T033012_triage_asset\C\Windows\prefetch" --csv
"C:\Users\TS0\Downloads\log" --csvf foo.csv --json
C:\Users\TS0\Downloads\log\json
```

Task 1

Analyzing Domain Controller Security Logs, can you confirm the date & time when the kerberoasting activity occurred?

我看kerber的event id = 4769

Time Created	Payload Data1	Payload Data2
=	⌵	⌵
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: krbtgt
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:05:54	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:06:15	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:06:15	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:12:05	Target: FORELA.LOCAL\alonzo.spire@FORELA.LOCAL	ServiceName: FORELA-WKSTN001\$
2024-05-21 03:12:05	Target: FORELA.LOCAL\alonzo.spire@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:13:02	Target: FORELA.LOCAL\alonzo.spire@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:15:12	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:18:09	Target: FORELA.LOCAL\alonzo.spire@FORELA.LOCAL	ServiceName: MSSQLService
2024-05-21 03:18:51	Target: FORELA.LOCAL\Administrator@FORELA.LOCAL	ServiceName: DC01\$
2024-05-21 03:20:24	Target: FORELA.LOCAL\DC01\$@FORELA.LOCAL	ServiceName: DC01\$

2024-05-21 03:18:09

Task 2

What is the Service Name that was targeted?

同上：MSSQLService

Task 3

It is really important to identify the Workstation from which this activity occurred. What is the IP Address of the workstation?

Payload

Cell contents

```
{"EventData":{"Data":[{"@Name":"TargetUserName","#text":"alonzo.spire@FORELA.LOCAL"},{"@Name":"TargetDomainName","#text":"FORELA.LOCAL"},{"@Name":"ServiceName","#text":"MSSQLService"},{"@Name":"ServiceSid","#text":"S-1-5-21-3239415629-1862073780-2394361899-1105"},{"@Name":"TicketOptions","#text":"0x40800000"}, {"@Name":"TicketEncryptionType","#text":"0x17"}, {"@Name":"IpAddress","#text":"::ffff:172.17.79.129"}, {"@Name":"IpPort","#text":"58107"}, {"@Name":"Status","#text":"0x0"}, {"@Name":"LogonGuid","#text":"59f3b9b1-65ed-a449-5ac0-8ea1f68478ee"}, {"@Name":"TransmittedServices","#text":"-"}]}}
```

Format Replace: ☐ CRLF ☐ CR ☐ LF ☒ Comma ☐ Tab Font size 12

☒ Payload Data2 Contains MSSQLService

172.17.79.129

Task 4

Now that we have identified the workstation, a triage including PowerShell logs and Prefetch files are provided to you for some deeper insights so we can understand how this activity occurred on the endpoint. What is the name of the file used to Enumerate Active directory objects and possibly find Kerberoastable accounts in the network?

更換至 Powershell-Operational.evtx


Powershell-Operational-OutputFile.csv

×

SECURITY-DC-Outpu

Enter text to search...

Find

cord Id	Time Created	Payload Data1
	=	
147	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
148	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
149	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
150	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
151	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
152	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
153	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
154	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
155	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
156	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
157	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
158	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
159	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
160	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
161	2024-05-21 03:16:32	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
162	2024-05-21 03:17:23	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
163	2024-05-21 03:17:23	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
164	2024-05-21 03:17:23	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
165	2024-05-21 03:17:25	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
166	2024-05-21 03:17:25	Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
134	2024-05-21 03:16:11	Severity = Warning

⏪

C:\Users\TSO\Downloads\log\Powershell-Operational-OutputFile.csv

powerview.ps1

Task 5

When was this script executed?

同上，第一筆紀錄：

2024-05-21 03:16:32

Task 6

What is the full path of the tool used to perform the actual kerberoasting attack?

這裡要看pf，找USER執行檔案的

a column header here to group by that column	
Run Time	Executable Name
=	USER
2024-05-21 03:13:01	\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\OOBE\USEROOB
2024-05-21 03:18:08	\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\DOWNLOADS\



Run Time

Is same day

2024-05-21 00:00:00

And

Executable Name

Contains

USER

C:\USERS\ALONZO.SPIRE\DOWNLOADS\RUBEUS.EXE

Task 7

When was the tool executed to dump credentials?

同上

2024-05-21 03:18:08