Unit42 - htb

Questions

How many Event logs are there with Event ID 11?

```
Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=11} | Measure-Object -Line
```

```
Lines Words Characters Property
----- ----- ---------- --------
   56
```

Answer: 56

Whenever a process is created in memory, an event with Event ID 1 is recorded with details such as command line, hashes, process path, parent process path, etc. What is the malicious process that infected the victim's system?

Primeiro verifiquei quantos logs de id 1 tinham :

```
Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=1}
```

```
   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
14/02/2024 00:41:58              1
14/02/2024 00:41:57              1
14/02/2024 00:41:57              1
14/02/2024 00:41:57              1
14/02/2024 00:41:56              1
14/02/2024 00:41:45              1
```

Como eram poucos os enumerei manualmente, até achar o log com o processo pai não comum :

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
```

```
Operational.evtx";ID=1})[1].Properties[20]
```

```
Value
-----
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
```

Answer: Preventivo24.02.14.exe.exe

Which Cloud drive was used to distribute the malware?

Primeiro verificamos quais eventos de ID 22(eventos de consultas DNS) temos :

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=22} -Oldest) | Format-Table -AutoSize -Wrap
```

```
   ProviderName: Microsoft-Windows-Sysmon

TimeCreated          Id LevelDisplayName Message
-----------          -- ---------------- -------
14/02/2024 00:41:26 22
14/02/2024 00:41:45 22
14/02/2024 00:41:58 22
```

Também podemos ver em que momento foram criados.

Como temos 3 podemos enumerar manualmente.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=22})[1,2].Properties | Format-Table -AutoSize -
Wrap
```

```
Value
-----
-
2024-02-14 03:41:43.924
817bddf3-3514-65cc-0802-000000001900
4292
d.dropbox.com
0
type:  5 d.v.dropbox.com;type:  5
d-edge.v.dropbox.com;162.125.8.20;205.251.192.57;2600:9000:5300:3900::1;
C:\Program Files\Mozilla Firefox\firefox.exe
DESKTOP-887GK2L\CyberJunkie
-
2024-02-14 03:41:25.269
817bddf3-3514-65cc-0802-000000001900
4292
uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com
0
type:  5 edge-block-www-env.dropbox-dns.com;::ffff:162.125.81.15;198.51.44.6;2620:4d:4000:6
259:7:6:0:1;198.51.45.6;2a00:edc0:6259:7:6::2;198.51.44.70;2620:4d:4000:6259:7:6:0:3;198.51
.45.70;2a00:edc0:6259:7:6::4;
C:\Program Files\Mozilla Firefox\firefox.exe
DESKTOP-887GK2L\CyberJunkie
```

os eventos de índice 1 e 2 fazem referência consultas ao `dropbox`. Vendo o horário em que a requisição foi feita, podemos fazer relação se algum arquivo foi criado nesse horário com os log de id 11(log de criação de arquivo).

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=11;StartTime="14/02/2024 00:41:26";EndTime="14/02/2024 00:41:27"} -Oldest) | Format-Table -AutoSize -Wrap
```

```
   ProviderName: Microsoft-Windows-Sysmon

TimeCreated          Id LevelDisplayName Message
-----------          -- ---------------- -------
14/02/2024 00:41:26 11
14/02/2024 00:41:26 11
14/02/2024 00:41:26 11
14/02/2024 00:41:26 11
```

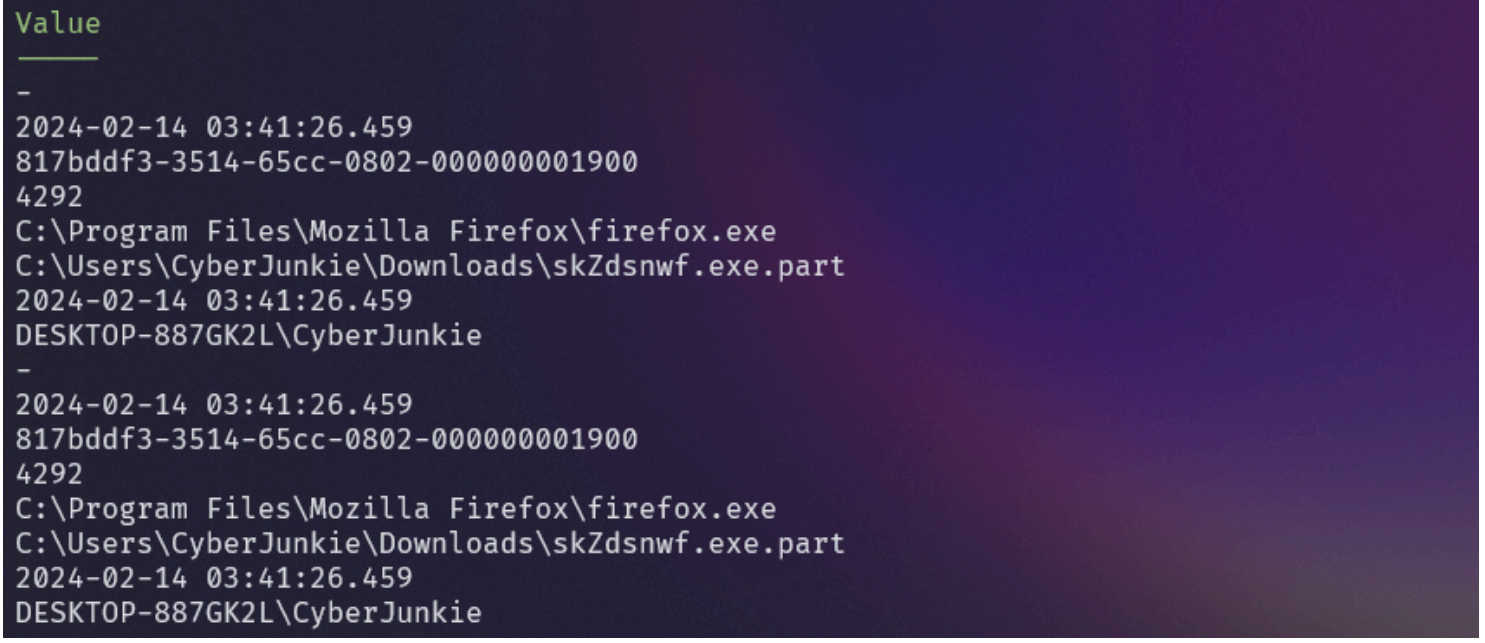
Aqui temos 4 eventos de criação de arquivo que foram feitas nesse horário.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=11;StartTime="14/02/2024 00:41:26";EndTime="14/02/2024 00:41:27"})[0].Properties | Format-Table -AutoSize -Wrap
```

```
Value
-----
-
2024-02-14 03:41:26.459
817bddf3-3514-65cc-0802-000000001900
4292
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
2024-02-14 03:41:26.459
DESKTOP-887GK2L\CyberJunkie
```

O evento de índice 1 indica o download do arquivo malicioso.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=11;StartTime="14/02/2024 00:41:26";EndTime="14/02/2024 00:41:27"})[1,2].Properties | Format-Table -AutoSize -Wrap
```



os logs de índice 1 e 2 indicam o download de parts de um arquivo.

Assimilando o horário de criação desses arquivos com o horário de consulta dns, podemos saber de onde veio.

Answer: dropbox

The initial malicious file time-stamped (a defense evasion technique, where the file creation date is changed to make it appear old) many files it created on disk. What was the timestamp changed to for a PDF file?

Podemos pesquisar pelo id de evento 2

```
Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=2;} | Measure-Object -Line
```

Como são 16, seria demorado para verificarmos manualmente.

Vamos criar um script para podemos saber qual é o log certo.

```
for($i = 0;$i -lt 16;$i++){

$logs = (Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=2;})[$i].Properties[5].Value | Select-String -Pattern 'pdf';
```

```
$logs ? (Write-Host "$logs - Id do evento : $i") : ($null)

}
```

```
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\Tem
pFolder\~.pdf - Id do evento : 7
```

Nesse script verificamos se o nome do arquivo modificado contém `pdf` e jogamos em uma variável. Depois verificamos se a variável não está vazia, caso não esteja vazia printamos o nome do arquivo e o id do evento. Agora sabemos o id do evento certo.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=2;})[7].Properties[6] | Format-Table -AutoSize -
Wrap
```

O índice 6 se refere a data para o qual foi modificada.

Answer: 2024-01-14 08:10:06

The malicious file dropped a few files on disk. Where was "once.cmd" created on disk? Please answer with the full path along with the filename.

Podemos filtrar pelos eventos de id 11 e pelo nome `once.cmd`

```
for($i = 0;$i -lt 56;$i++){

        $logs = (Get-WinEvent -FilterHashtable @{Path=".\Microsoft-
Windows-Sysmon-Operational.evtx";ID=11;})[$i].Properties[5].Value |
Select-String -Pattern 'once.cmd';

        $logs ? (Write-Host "$logs - Id do evento : $i") : ($null)
}
```

```
C:\Games\once.cmd - Id do evento : 17
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\Win
dowsVolume\Games\once.cmd - Id do evento : 34
```

Obtivemos 2 resultados. Agora podemos conferir qual a imagem que os criou.

Como são só 2 eventos podemos fazer manualmente.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=11;})[34].Properties
```

```
Value
-----
-
2024-02-14 03:41:58.404
817bddf3-3684-65cc-2d02-000000001900
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn
1.1.2\install\F97891C\WindowsVolume\Games\once.cmd
2024-02-14 03:41:58.404
DESKTOP-887GK2L\CyberJunkie
```

O evento de índice 34 foi criado pelo malware.

Answer: `C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd`

The malicious file attempted to reach a dummy domain, most likely to check the internet connection status. What domain name did it try to connect to?

Já vimos isso antes, podemos ver as tentativas de resolução DNS.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=22})[0].Properties | Format-Table -AutoSize -
Wrap
```

```
Value
-----
-
2024-02-14 03:41:56.955
817bddf3-3684-65cc-2d02-000000001900
10672
www.example.com
0
::ffff:93.184.216.34;199.43.135.53;2001:500:8f::53;199.43.133.53;2001:500:8d::53;
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
```

Answer: `www.example.com`

Which IP address did the malicious process try to reach out to?

Podemos buscar pelo evento de id 3.

Como só tem 1 podemos vê-lo manualmente

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-
Operational.evtx";ID=3}).Properties | Format-Table -AutoSize -Wrap
```

```
Value
-----
technique_id=T1036,technique_name=Masquerading
2024-02-14 03:41:57.159
817bddf3-3684-65cc-2d02-000000001900
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
tcp
True
False
172.17.79.132
-
61177
-
False
93.184.216.34
-
80
-
```

Answer: `93.184.216.34`

The malicious process terminated itself after infecting the PC with a backdoored variant of UltraVNC. When did the process terminate itself?

Podemos verificar pelo id de evento 5.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=5}) | Format-Table -AutoSize -Wrap
```

```
   ProviderName: Microsoft-Windows-Sysmon

TimeCreated          Id LevelDisplayName Message
-----------          -- ---------------- -------
14/02/2024 00:41:58  5
```

Como só tem uma podemos verificar manualmente.

```
(Get-WinEvent -FilterHashtable @{Path=".\Microsoft-Windows-Sysmon-Operational.evtx";ID=5}).Properties | Format-Table -AutoSize -Wrap
```

```
Value
-----
-
2024-02-14 03:41:58.795
817bddf3-3684-65cc-2d02-000000001900
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
```

Answer: `2024-02-14 03:41:58`