Arctic Wolf Labs Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN

arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/

by Steven Campbell, Akshay Suthar, and Stefan Hostetler

October 24, 2024

FOG
RANSOMWARE

Key Takeaways

- Arctic Wolf has observed an influx of at least 30 Akira and Fog intrusions across a variety of industries since early August, each involving SonicWall SSL VPN early in the cyber kill chain.
- Malicious VPN logins originated from IP addresses associated with VPS hosting, providing defenders with a viable mechanism for early detection and prevention.
- None of the affected SonicWall devices were patched against CVE-2024-40766, which SonicWall indicates is potentially under active exploitation.
- Shared IP infrastructure was seen across several Akira and Fog intrusions.
- A short interval between initial SSL VPN account access and ransomware encryption was observed, often within the same day.

Summary

In early August, Arctic Wolf Labs began observing a marked increase in Fog and Akira ransomware intrusions where initial access to victim environments involved the use of SonicWall SSL VPN accounts. Based on victimology data showing a variety of targeted industries and organization sizes, we assess that the intrusions are likely opportunistic, and the threat actors are not targeting a specific set of industries.

On September 6, 2024, SonicWall indicated that CVE-2024-40766 was potentially under active exploitation. While we do not have definitive evidence of this vulnerability being exploited in the intrusions we investigated, all SonicWall devices involved were running firmware versions affected by it. Although credential-based attacks can't be ruled out in some intrusions, the trend of increased threat activity against SonicWall devices highlights the necessity of maintaining firmware updates and implementing external log monitoring.

We are sharing details of the observed ransomware activity to help organizations defend themselves effectively against these threats. Please note that we may add further details to this blog article as we uncover additional information, as our investigation into these activities is still ongoing.

What we Know About the Intrusions

Prior to the month of August 2024, Fog and Akira ransomware intrusions investigated by Arctic Wolf Incident Response involved a variety of firewall brands. However, new caseload since early August shows a skew towards SonicWall in new intrusions where Akira and Fog ransomware encryptor payloads were deployed, spanning across 30 new ransomware intrusions between the start of August until the time of this writing (mid-October 2024). Akira ransomware was deployed in approximately 75% of these intrusions and Fog ransomware was deployed in the remaining 25%. The duration between initial SSL VPN access to acting on ransom/encryption objectives was as short as 1.5 to 2 hours in some intrusions, while in other intrusions the interval was closer to 10 hours.

Initial Access

In the firewall logs reviewed by Arctic Wolf Labs, there was no definitive evidence confirming exploitation of any known remote code execution vulnerabilities. On the other hand, none of the SonicWall devices in the reviewed intrusions were shown to be running new enough firmware versions to prevent exploitation of CVE-2024-40766. Additionally, in intrusions where firewall telemetry was available, malicious SonicWall SSL VPN login events were observed that originated from VPS (Virtual Private Server) hosting providers.

In almost all intrusions, connections to the VPNs originated from hosting-related ASNs. In two separate sets of intrusions, we observed Akira ransomware affiliates logging in to the victims' SonicWall VPNs using the same VPS IP addresses as identified in separate Fog intrusions (AS64236 – UnReal Servers, LLC and AS32613 – Leaseweb Canada Inc.).

Similar to our findings on September 6, 2024, compromised SSL VPN accounts were local to the SonicWall devices themselves and were not integrated with a centralized authentication solution such as Microsoft Active Directory. Arctic Wolf Labs was not able to confirm any instances where multi-factor authentication (MFA) was enabled among compromised accounts.

In several instances, victim organizations' SSL VPN services were running on the default port of 4433. In intrusions where firewall logs were captured, message event ID 238 (WAN zone remote user login allowed) or message event ID 1080 (SSL VPN zone remote user login allowed) were observed. Following one of these messages, there were several SSL VPN INFO log messages (event ID 1079) indicating that login and IP assignment had completed successfully. Threat actors commonly sought to delete firewall logs upon gaining access to compromised environments.

```
id=firewall sn=REDACTED time=REDACTED fw=REDACTED pri=6 c=0 m=1080 msg="SSL VPN zone
remote user login allowed" sess="sslvpnc" n=8 usr=REDACTED src=77.247.126.158::X3
dst=REDACTED proto=tcp note=REDACTED_USERNAME fw_action="NA"
id=firewall sn=REDACTED time=REDACTED fw=REDACTED pri=6 c=0 m=1079 msg="User REDACTED
login" sess="sslvpnc" n=22 fw_action="NA"
id=firewall sn=REDACTED time=REDACTED fw=REDACTED pri=6 c=0 m=1079 msg="Client
REDACTED is assigned IP:REDACTED_INTERNAL_IP_ADDRESS" n=24 fw_action="NA"
```

Encryption

As previously observed with Fog, there was rapid encryption in the intrusions. In some intrusions, the duration between initial access to data encryption took place over several hours. Threat actors demonstrated focus on storage of virtual machines and their backups.

Data Exfiltration

Based on command line activities observed during exfiltration, we can begin to see what data these ransomware affiliates were most interested in. General folders containing applications, staff documents, or generic files were only exfiltrated up to six months' worth of data. Whereas, folders containing potentially more sensitive information, such as documents from human resources or accounts payable departments had up to 30 months worth of data exfiltrated.

Conclusion

Based on intrusions investigated by Arctic Wolf since early August, a significant amount of activity was observed involving Fog and Akira ransomware in environments using the SonicWall SSL VPN service. Visibility gaps hampered analysis of firewall logs across a subset of intrusions, while others suggested that existing accounts had been compromised.

We do not have definitive evidence that the threat actors exploited remote code execution vulnerabilities such as CVE-2024-40766 to compromise SonicWall appliances. In some instances, VPN credentials may have been obtained through another means, such as data breaches, for example. Nonetheless, as we've indicated previously in our September security bulletin, our findings suggest that defenders should prioritize remediation of this vulnerability to rule out potential exploitation.

There have been several notable developments in the threat landscape since our initial Fog ransomware publication in June 2024. The Fog affiliates we have visibility into are now exfiltrating data, as is common practice in most ransomware intrusions. Additionally, victimology of intrusions involving Fog ransomware have diverged from the education sector, indicating a more opportunistic approach than previously observed.

Both Akira and Fog affiliates have shown an interest in compromising SSL VPN accounts on SonicWall appliances, rapid encryption of VM storage data, and exfiltration of sensitive data to increase the likelihood of a ransom payment. Across the latest influx of intrusions we examined, a short duration was observed between initial access and action on objectives, leaving minimal time for defenders to thwart their activities.

To effectively protect against these and other emerging ransomware threats, defenders should prioritize keeping firmware up to date on perimeter network appliances, monitoring for VPN logins from hosting providers that are not expected in their environments, ensuring that secure off-site backups are in place, and monitoring for common post-compromise activities across endpoints.

How Arctic Wolf Protects its Customers

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

Arctic Wolf Labs has leveraged threat intelligence around Akira and Fog ransomware activity to implement new detections in the Arctic Wolf Platform to protect Managed Detection and Response (MDR) customers. As we discover new information, we will enhance our detections to account for additional indicators of compromise and techniques leveraged by these threat actors.

Appendix

Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	Sub-techniques or Tools
Initial Access	T1133: External Remote Services	
	T1078: Valid Accounts	• Compromised VPN Credentials • T1078.002: Domain accounts
Discovery	T1046: Network Service Discovery	• SoftPerfect Network Scanner • Advanced Port Scanner
	T1482: Domain Trust Discovery	• NLTest • AdFind
Lateral Movement	T1021: Remote Services	• T1021.001: Remote Desktop Protocol • T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	• PsExec
Credential Access	T1555: Credentials from Password Stores	• PowerShell script (Veeam-Get-Creds.ps1) to obtain passwords from the Veeam Backup and Replication Credentials Manager
	T1003: OS Credential Dumping	• Mimikatz • Secretsdump.py • DPAPI Domain Backup Key Extraction
Execution	T1059: Command and Scripting Interpreter	• T1059.003: Windows Command Shell
Command and Control	T1219: Remote Access Software	• AnyDesk • Putty • MobaXterm

Collection	T1560: Archive Collected Data	• T1560.001: Archive via Utility • 7-Zip • WinRAR
Exfiltration	T1567: Exfiltration Over Web Service	• T1567.002: Exfiltration to Cloud Storage • Rclone
	T1048: Exfiltration Over Alternative Protocol	• T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol • WinSCP • FileZilla
Impact	T1486: Data Encrypted for Impact	• Akira Payload • Fog Payload
	T1490: Inhibit System Recovery	• vssadmin.exe used to delete volume shadow copies on the system.

Tools

Name	**Description**
PsExec	A tool that allows threat actors to execute processes on other systems with full interactivity for console applications. The threat actors leveraged PsExec to move laterally and execute commands.
Advanced IP Scanner	Free network scanner. The threat actors used Advanced IP Scanner to discover network devices.
Advanced Port Scanner	Free port scanner. The threat actors used Advanced Port Scanner to discover network services.
SoftPerfect Network Scanner	Network administration tool for Windows, macOS, and Linux. The threat actors used SoftPerfect to discover network services.
AnyDesk	Remote desktop application. Threat actors used it for remote access
MobaXterm	Remote access toolset, that includes a Windows SSH client. Used for persistence.
WinRAR	File archiver utility. Threat actors used it to create archive files for exfiltration.
Mimikatz	Open-source tool that can be used to gain access to hashes, passwords, and Kerberos tickets. Used for credential access.
Rclone	Command line program used to sync files and directories to cloud storage providers. The threat actors used Rclone to exfiltrate data.

Veeam-Get-Creds.ps1	An open-source PowerShell script used by the threat actors to obtain passwords from the Veeam Backup and Replication Credentials Manager.

Indicators of Compromise (IoCs)

Indicator	Type	Description
.fog	File Extension	Fog ransomware extension
.flocked	File Extension	Fog ransomware extension
.akira	File Extension	Akira ransomware extension
7z2407-x64.exe	File Name	7-zip
AIPScanner.exe	File Name	Advanced IP Scanner
netscan_n.exe	File Name	SoftPerfect Network Scanner
adfind.exe	File Name	AdFind
sys.exe	File Name	Renamed rclone
readme.txt	File Name	Fog ransom note
mimikatz.exe	File Name	Mimikatz
1.bat	File Name	Potential ransomware deployment script
akira_readme.txt	File Name	Akira ransom note
esxi6	File Name	Akira ESXI ransomware binary
.loc	File Name	Fog ESXI ransomware binary
kali	Hostname	Threat Actor hostname
WORKSTATION	Hostname	Threat Actor hostname
77.247.126[.]158	IPv4 Address	TA connection to VPN

208.115.232[.]194	IPv4 Address	TA connection to VPN
184.107.5[.]46	IPv4 Address	TA connection to VPN
66.181.33[.]32	IPv4 Address	TA connection to VPN
185.235.137[.]150	IPv4 Address	TA connection to VPN
45.11.59[.]16	IPv4 Address	TA connection to VPN
79.141.173[.]238	IPv4 Address	AnyDesk connection IP
57.128.101[.]78	IPv4 Address	AnyDesk C2 IP
194.33.45[.]167	IPv4 Address	Exfiltration IP
23.227.162[.]18	IPv4 Address	Exfiltration IP
45.86.208[.]146	IPv4 Address	FileZilla Exfiltration IP
3477a173e2c1005a81d042802ab0f22cc12a4d55	SHA-1	Advanced Port Scanner
86233a285363c2a6863bf642deab7e20f062b8eb	SHA-1	Advanced IP Scanner
ce4758849b53af582d2d8a1bc0db20683e139fcc	SHA-1	Advanced IP Scanner
67396e1aacacb6efbca51f4c03d2017af78c9842	SHA-1	Angry IP Scanner
806a232379ad0af437d4bc5b87fb42065dbf82d4	SHA-1	SoftPerfect Network Scanner
e6b34a589e61b155ab70f11f8f7393316c9a3189	SHA-1	SoftPerfect Network Scanner
1d345799307c9436698245e7383914b3a187f1ec	SHA-1	Rclone
ce8de59e2277e9003f3a9c96260ce099ca7cda6c	SHA-1	WinRAR
15035d9f218a4629a8449829eba85b40806f4f59	SHA-1	WinRAR
7931b85054c29be4cc3c9250a5dc4a821a44604	SHA-1	WinRAR

c26cfb9f9910fe585630940a777022702257548d	SHA-1	WinRAR
8ea2bf726044e98479076d0e64327f7ae7a6e5f2	SHA-1	FileZilla
99ed6135defff6e675d626f742389d6280abdb60	SHA-1	FileZilla
c1f271e5ced7a5badf62042ab882584e45aeab37	SHA-1	WinSCP
8e81daa8c88a1e40c60332917c4ad5fa57acbb23	SHA-1	PuTTY
75d7d147f66004c7131ad0d0fa5603451be45ba	SHA-1	OpenSSH
f5ca50ee8bc9d01760c7d0d4fc0c814cbbf26bc9	SHA-1	MobaXterm – SSH tool
03f193a9385cf8fe2429e14aab4862b1627ff9d5	SHA-1	MobaXterm – SSH tool
57aed4cf2972b51e0a7d37e9ca0c4b1b6985e1f1	SHA-1	MobaXterm – SSH tool
2aab7f60262db7589d83fd7d13c968a6b93f75b9	SHA-1	MobaXterm – SSH tool
e7fb4bf69be5ac4583c0c02e26a17bd3cdef4c02	SHA-1	AnyDesk
6ae600ccff0741ce420bbd372c931b951094121f	SHA-1	AnyDesk
c144446dc23c86c7c9b26ce87c3176866372f6d1	SHA-1	AnyDesk
363068731e87bcee19ad5cb802e14f9248465d3	SHA-1	AV/EDR killer
AS29802	AS Number	Hivelocity Inc. – Used for SSL VPN login
AS43641	AS Number	Sollutium Eu Sp Z.O.O. – Used for SSL VPN login
AS58061	AS Number	Scalaxy B.V. – Used for SSL VPN login
AS59711	AS Number	Hz Hosting Ltd – Used for SSL VPN login
AS62240	AS Number	Clouvider Limited – Used for SSL VPN login
AS202015	AS Number	Hz Hosting Ltd – Used for SSL VPN login
AS395092	AS Number	Shock Hosting Llc – Used for SSL VPN login
AS64236	AS Number	UnReal Servers, LLC – Used for SSL VPN login

AS32613	AS Number	Leaseweb Canada Inc. – Used for SSL VPN login

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 ransomware threat actors.

Network

During our investigations, we observed threat actors logging into SonicWall SSL VPN accounts via a handful of hosting-related ASNs. In situations where organizations don't have a valid business reason to allow logins from these specific ASNs, login attempts can be blocked outright, or otherwise used for detection purposes. IP classification services may provide avenues for blocking logins from hosting-related ASNs altogether, although some exceptions may be needed depending on the use of legitimate services such as SASE providers.

Endpoint

The Veeam-Get-Creds.ps1 PowerShell script includes the following strings:

```
[System.Security.Cryptography.ProtectedData]::Unprotect
[System.Security.Cryptography.DataProtectionScope]::LocalMachine
SqlDatabaseName
```

Detecting occurrences of all 3 strings in PowerShell script block logging may be able to identify usage of this tool.

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 Labs 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

Steven Campbell

Steven Campbell is a Lead Threat Intelligence Researcher at Arctic Wolf Labs and has more than eight years of experience in intelligence analysis and security research. He has a strong background in infrastructure analysis and adversary tradecraft.

Akshay Suthar

Akshay Suthar is a Lead Threat Intelligence Researcher at Arctic Wolf Labs focused on researching adversary tradecraft and malware analysis. He has more than seven years of experience in a multitude of domains including threat intelligence research, detection engineering, and intrusion analysis.

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.