Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

ArcaneDoor a Novel Espionage Campaign Exploits Cisco Zero-Days

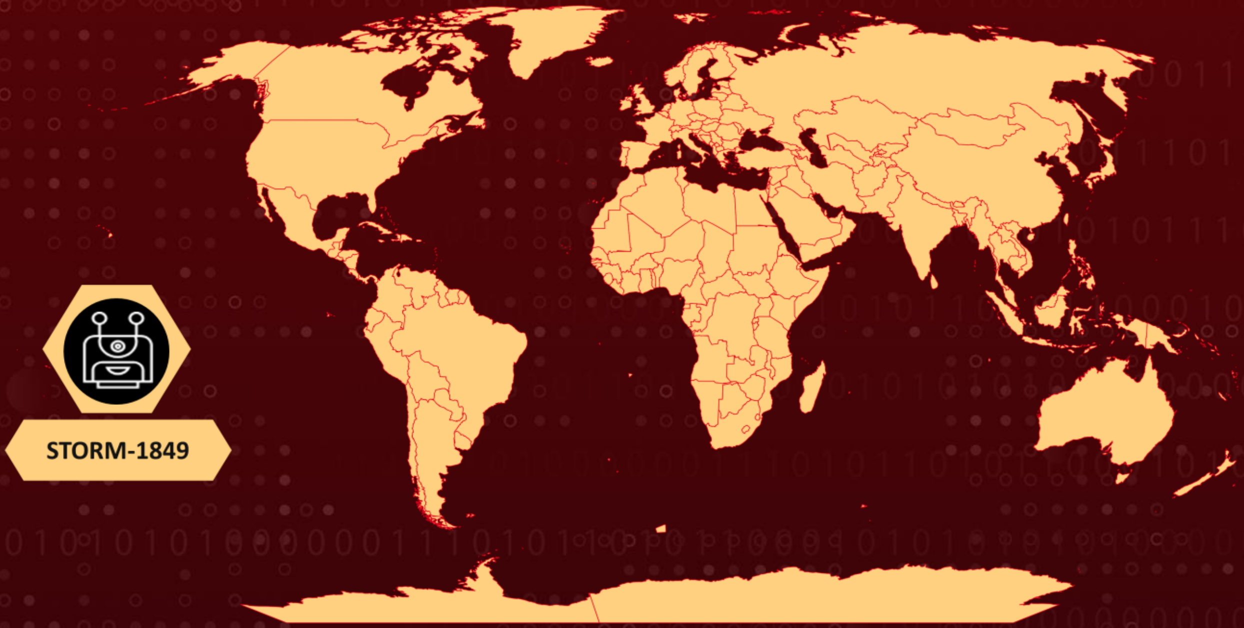
Date of Publication	Admiralty Code	TA Number
April 25, 2024	A1	TA2024163

Summary

Attack Commenced: November 2023
Campaign: ArcaneDoor
Threat Actor: STORM-1849 (aka UAT4356)
Attack Region: Worldwide
Targeted Industries: Government, Critical Infrastructure, Telecommunication, Energy

Attack: ArcaneDoor, an intricately crafted cyber espionage endeavor, orchestrated by state-affiliated operatives under the moniker STORM-1849, has been strategically aimed at governmental and critical infrastructure networks on a global scale since November 2023. Leveraging two undisclosed vulnerabilities found within Cisco ASA and FTD firewalls.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20353	Cisco ASA and FTD Denial of Service Vulnerability	Cisco ASA Software and FTD Software	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20359	Cisco ASA and FTD Privilege Escalation Vulnerability	Cisco ASA Software or FTD Software	✓	✓	✓

Attack Details

#1 The cyber espionage campaign known as ArcaneDoor has been meticulously orchestrated, with the primary aim of breaching the perimeter network defenses used by governmental and critical infrastructure entities.

#2 Spearheaded by state-backed operatives identified as STORM-1849 (also known as UAT4356), this nefarious campaign has exploited two previously undocumented vulnerabilities within Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls since November 2023, enabling infiltration into government networks worldwide.

#3 These vulnerabilities provided the means for threat actors to deploy previously undiscovered malware components, establishing persistent access to compromised ASA and FTD devices. Operating under the cover of STORM-1849, the perpetrators introduced two distinct backdoor components into their arsenal: "Line Runner" and "Line Dancer."

#4 Of these, "Line Dancer" is a pivotal component—a memory-resident shellcode interpreter facilitating the uploading and execution of arbitrary shellcode payloads, thereby affording adversaries a versatile means of interaction within compromised systems.

#5 These malicious tools were collectively used to execute a spectrum of malevolent activities, including configuration tampering, reconnaissance, capture and exfiltration of network traffic, and potentially, lateral movement within targeted environments.

#6 The unmasking of the ArcaneDoor espionage campaign serves as a testament to the formidable prowess of the STORM-1849 actor, who has demonstrated a tailored approach to tool development indicative of a deep-seated commitment to espionage and an intimate understanding of the targeted devices—a hallmark of sophisticated state-sponsored actors.

Recommendations

Patch Management: Implement a rigorous patch management strategy to promptly apply security patches and updates to all network devices, especially Cisco ASA and FTD firewalls, to mitigate the risk of exploitation by zero-day vulnerabilities.

Review Device Disk: Inspect the disk0 device for any unusual zip files that may indicate the presence of LineRunner. A set of commands has been recommended to confirm the existence of malware on the device.

Validate System Integrity: Execute the command "show memory region | include lina" and scrutinize the output for signs of tampering. If the output reveals multiple memory regions with permissions set to r-xp, particularly if any one of them measures exactly 0x1000 bytes, it suggests potential tampering. Prompt invocation of the incident response process is further recommended in such cases.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1037 Boot or Logon Initialization Scripts	T1040 Network Sniffing	T1041 Exfiltration Over C2 Channel	T1055 Process Injection
T1059 Command and Scripting Interpreter	T1070.004 File Deletion	T1071.001 Web Protocols	T1102.003 One-Way Communication

T1140 Deobfuscate/Decode Files or Information	T1556 Modify Authentication Process	T1557 Adversary-in-the-Middle	T1562.001 Disable or Modify Tools
T1653 Power Settings	T1498 Network Denial of Service	T1068 Exploitation for Privilege Escalation	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	192[.]36[.]57[.]181, 185[.]167[.]60[.]85, 185[.]227[.]111[.]17, 176[.]31[.]18[.]153, 172[.]105[.]90[.]154, 185[.]244[.]210[.]120, 45[.]86[.]163[.]224, 172[.]105[.]94[.]93, 213[.]156[.]138[.]77, 89[.]44[.]198[.]189, 45[.]77[.]52[.]253, 103[.]114[.]200[.]230, 212[.]193[.]2[.]48, 51[.]15[.]145[.]37, 89[.]44[.]198[.]196, 131[.]196[.]252[.]148, 213[.]156[.]138[.]78, 121[.]227[.]168[.]69, 213[.]156[.]138[.]68, 194[.]4[.]49[.]6, 185[.]244[.]210[.]65, 216[.]238[.]75[.]155, 5[.]183[.]95[.]95, 45[.]63[.]119[.]131, 45[.]76[.]118[.]87, 45[.]77[.]54[.]14, 45[.]86[.]163[.]244, 45[.]128[.]134[.]189, 89[.]44[.]198[.]16, 96[.]44[.]159[.]46, 103[.]20[.]222[.]218, 103[.]27[.]132[.]69, 103[.]51[.]140[.]101, 103[.]119[.]3[.]230,

TYPE	VALUE
IPv4	103[.]125[.]218[.]198, 104[.]156[.]232[.]22, 107[.]148[.]19[.]88, 107[.]172[.]16[.]208, 107[.]173[.]140[.]111, 121[.]37[.]174[.]139, 139[.]162[.]135[.]12, 149[.]28[.]166[.]244, 152[.]70[.]83[.]47, 154[.]22[.]235[.]13, 154[.]22[.]235[.]17, 154[.]39[.]142[.]47, 172[.]233[.]245[.]241, 185[.]123[.]101[.]250, 192[.]210[.]137[.]35, 194[.]32[.]78[.]183, 205[.]234[.]232[.]196, 207[.]148[.]74[.]250, 216[.]155[.]157[.]136, 216[.]238[.]66[.]251, 216[.]238[.]71[.]49, 216[.]238[.]72[.]201, 216[.]238[.]74[.]95, 216[.]238[.]81[.]149, 216[.]238[.]85[.]220, 216[.]238[.]86[.]24

Patch Links

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

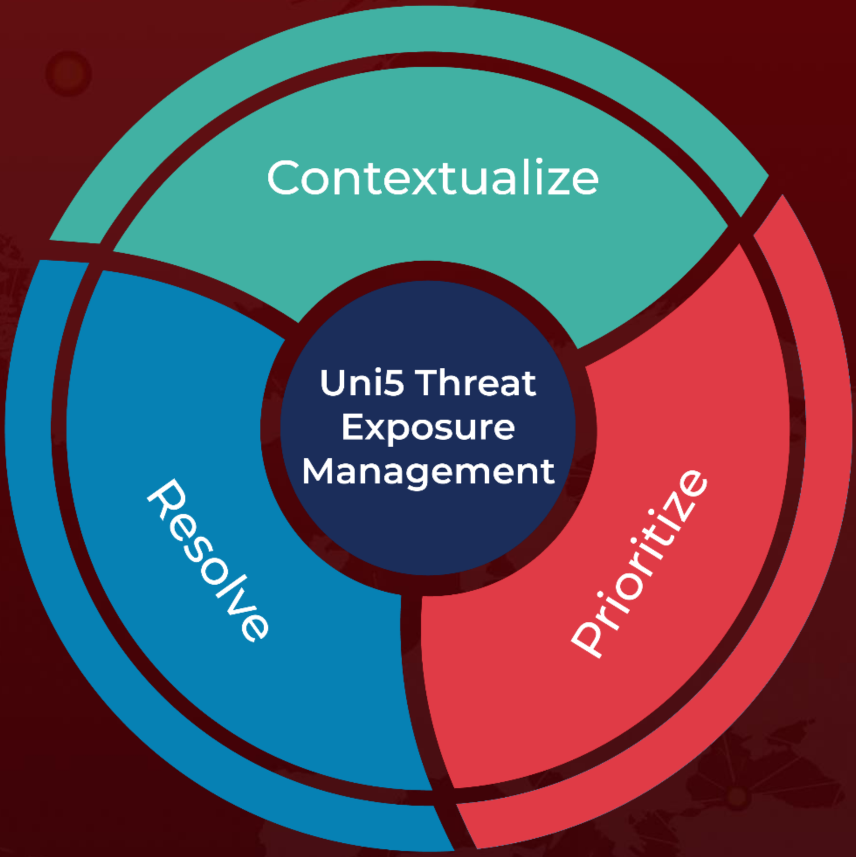
References

https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 25, 2024 • 6:00 AM

More at www.hivepro.com