Date of Publication
September 1, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

25 to 31 AUGUST 2025

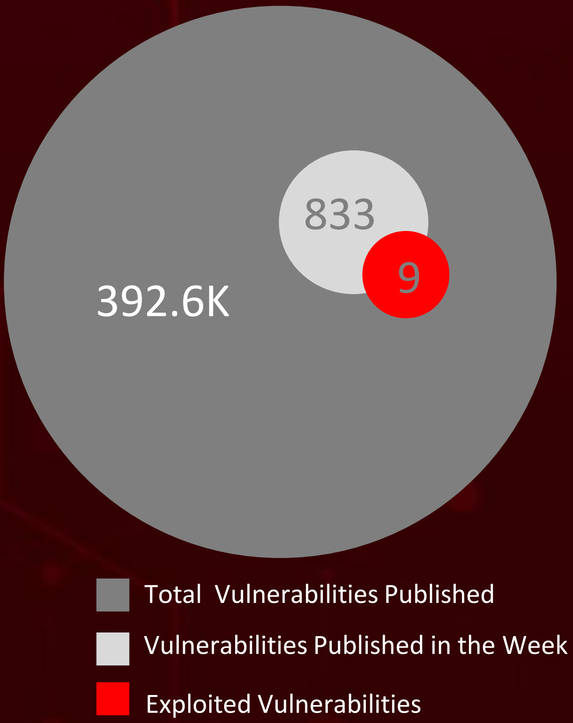
Table Of Contents

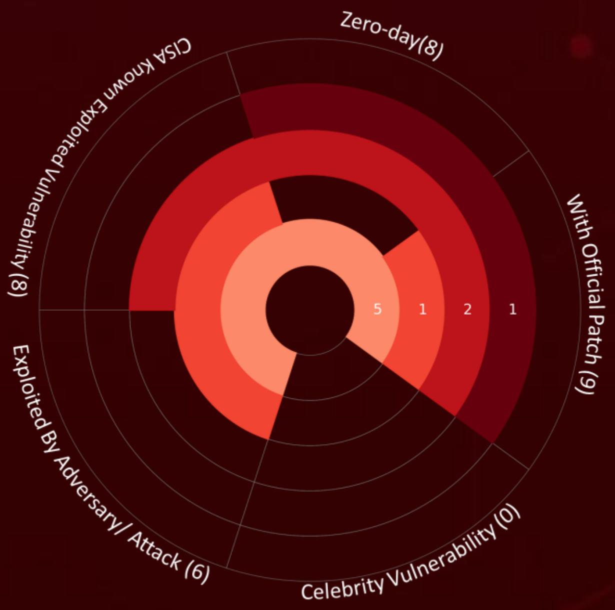
Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **two** major attacks were detected, **nine** critical vulnerabilities were actively exploited, and **three** threat actors were closely monitored, reflecting an alarming escalation in malicious activities.

Citrix disclosed three critical NetScaler ADC and Gateway flaws (**CVE-2025-7775**, CVE-2025-7776, CVE-2025-8424), with CVE-2025-7775 actively exploited for unauthenticated RCE/DoS. As no workarounds exist, immediate patching of affected systems to the fixed versions is required to prevent compromise.

Additionally, **Salt Typhoon**, a Chinese state-backed group, has expanded globally, hitting 600+ organizations in 80 countries by exploiting known vulnerabilities, with telecoms and critical sectors heavily targeted. **Storm-0501** has shifted from traditional ransomware to cloud-native attacks, exploiting identity gaps to escalate privileges, exfiltrate data, delete backups, and execute ransomware directly in the cloud. These rising threats pose significant and immediate dangers to users worldwide.





High Level Statistics

2

Attacks Executed

- SHAMOS
- MixShell

9

Vulnerabilities Exploited

- CVE-2025-7775
- CVE-2024-21887
- CVE-2023-46805
- CVE-2024-3400
- CVE-2023-20273
- CVE-2023-20198
- CVE-2018-0171
- CVE-2025-54948
- CVE-2025-54987

3

Adversaries in Action

- Cookie Spider
- Salt Typhoon
- Storm-0501

Insights

Storm-0501 now executes ransomware directly in the cloud, exploiting identity gaps to steal data, delete backups, and enforce ransom demands.

COOKIE SPIDER's latest campaign used SHAMOS, a stealthy AMOS variant, spread via malvertising and fake support sites to steal sensitive macOS user data and deliver additional payloads.

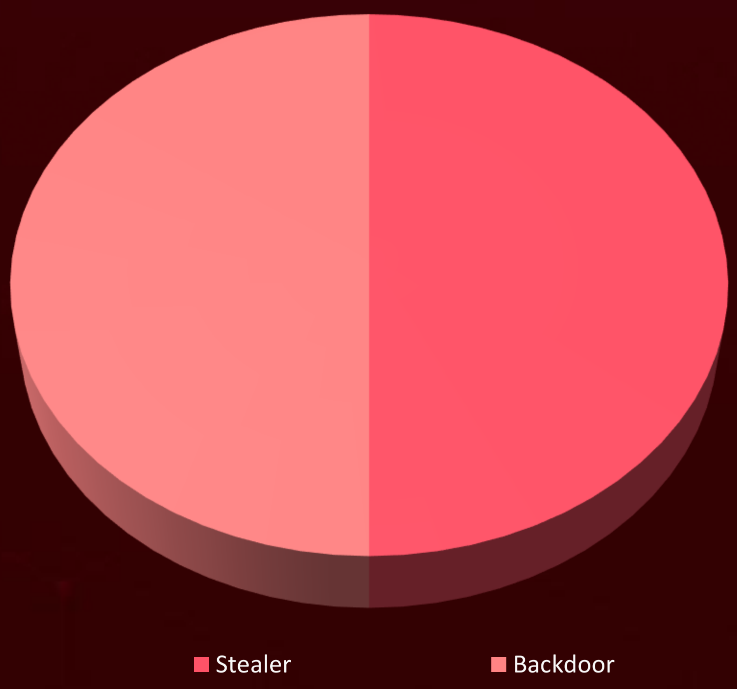
Salt Typhoon, a Chinese state-backed group, is exploiting known flaws to hit 600+ organizations across 80 countries, targeting telecoms and critical sectors.

Citrix warns of three critical NetScaler bugs, including zero-day CVE-2025-7775 under active RCE/DoS exploitation.

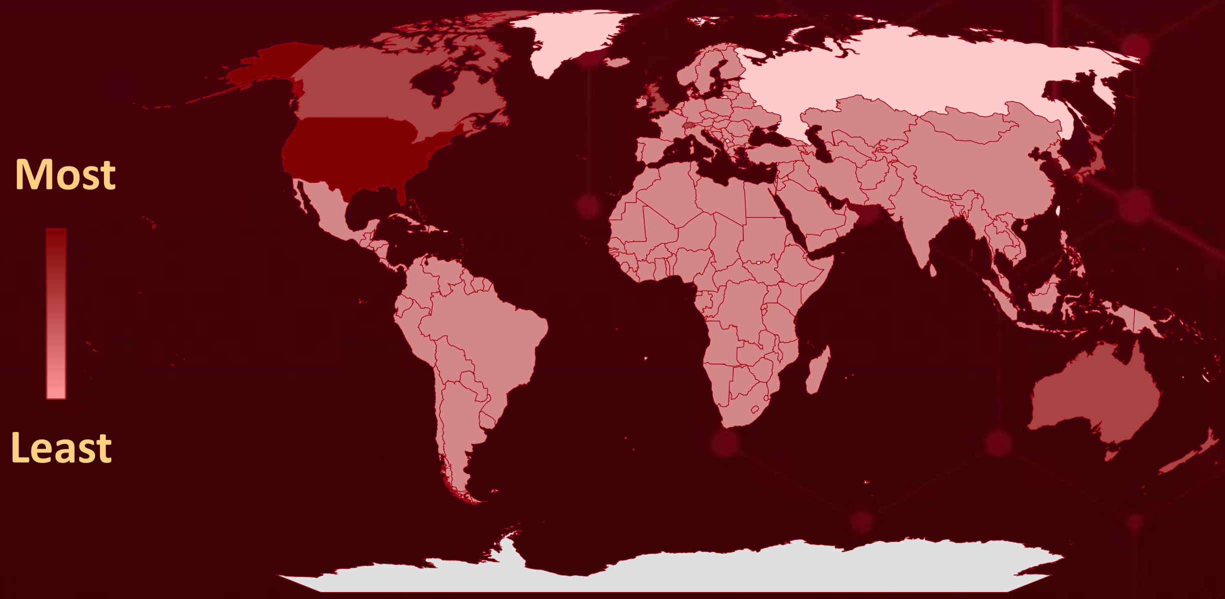
The ZipLine campaign targets U.S. supply chain manufacturers with social engineering, using trusted pretexts and ZIP archives to deliver the in-memory malware MixShell.

Trend Micro zero-day in Apex One allows RCE without login; immediate patching is strongly advised.

Threat Distribution



Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

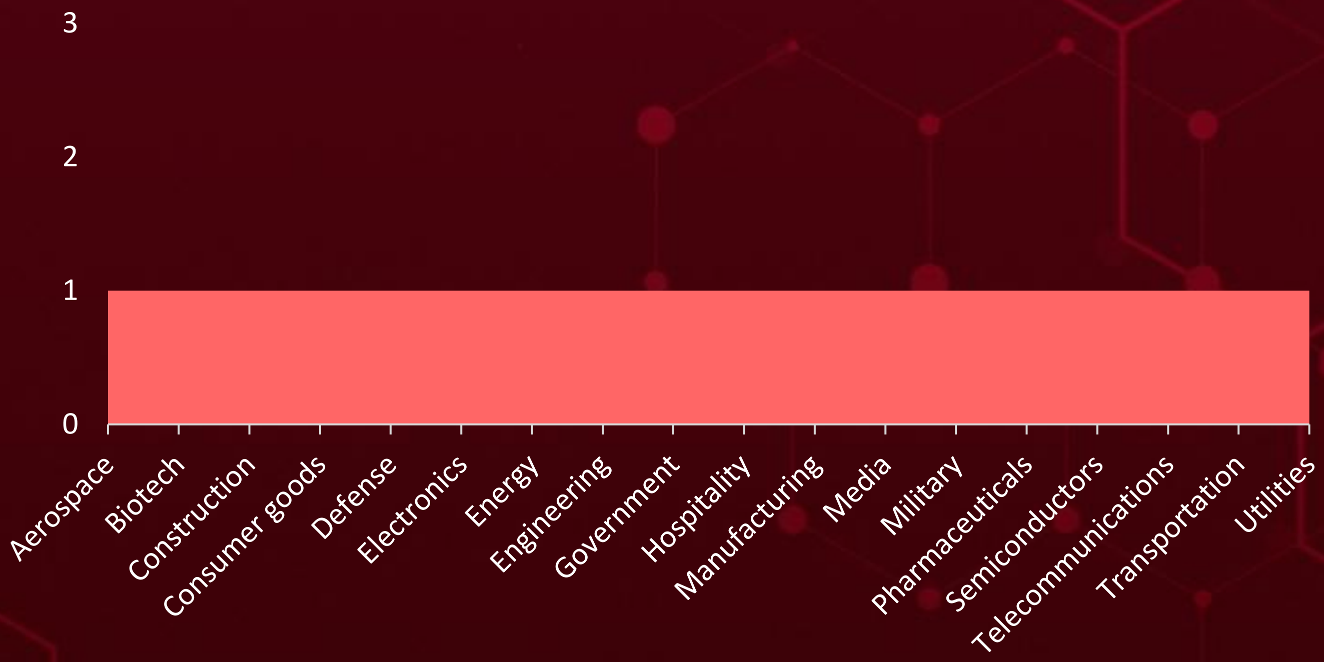
Countries
United States
New Zealand
Switzerland
Australia
Singapore
Canada
Japan
United Kingdom
Papua New Guinea
Malawi
Sudan
Austria
Myanmar
Azerbaijan
Senegal
Bahamas
Uganda
Bahrain
Mexico
Bangladesh
Nigeria
Barbados
Romania
Belarus

Countries
Somalia
Belgium
Timor-Leste
Belize
Liechtenstein
Benin
Malta
Bhutan
Mongolia
Bolivia
Netherlands
Bosnia and Herzegovina
Oman
Botswana
Poland
Brazil
Samoa
Brunei
Argentina
Bulgaria
Spain
Burkina Faso
Syria
Burundi

Countries
Tunisia
Cabo Verde
Zimbabwe
Cambodia
Luxembourg
Cameroon
Maldives
Algeria
Mauritania
Central African Republic
Moldova
Chad
Morocco
Chile
Nauru
China
Nicaragua
Colombia
North Macedonia
Comoros
Palau
Congo
Peru
Costa Rica

Countries
Cyprus
Slovenia
Czech Republic (Czechia)
South Korea
Denmark
St. Vincent & Grenadines
Djibouti
Sweden
Dominica
Tanzania
Dominican Republic
Tonga
DR Congo
Turkmenistan
Ecuador
Albania
Egypt
Afghanistan
El Salvador
Lithuania
Equatorial Guinea
Madagascar
Eritrea

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	**T1555** Credentials from Password Stores	**T1078** Valid Accounts
T1583 Acquire Infrastructure	**T1204** User Execution	**T1005** Data from Local System	**T1566** Phishing	**T1027** Obfuscated Files or Information
T1204.001 Malicious Link	**T1588** Obtain Capabilities	**T1203** Exploitation for Client Execution	**T1588.005** Exploits	**T1566.001** Spearphishing Attachment
T1133 External Remote Services	**T1059.001** PowerShell	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SHAMOS	SHAMOS is a macOS malware variant of the Atomic macOS Stealer (AMOS), distributed by the cybercriminal group COOKIE SPIDER. It spreads through malvertising and fake support websites, tricking users into running one-line terminal commands that install the stealer. Once active, it evades detection, establishes persistence, and exfiltrates sensitive data like credentials, notes, and crypto wallet files.	Malvertising and fake support websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	macOS
ASSOCIATED ACTOR			**PATCH LINK**
COOKIE SPIDER			-

IOC TYPE	VALUE
SHA256	4549e2599de3011973fde61052a55e5cdb770348876abc82de14c2d99575790f, b01c13969075974f555c8c88023f9abf891f72865ce07efbcee6c2d906d410d5, a4e47fd76dc8ed8e147ea81765edc32ed1e11cff27d138266e3770c7cf953322, 95b97a5da68fcb73c98cd9311c56747545db5260122ddf6fae7b152d3d802877

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MixShell	MixShell is a sophisticated, in-memory malware delivered through a multi-stage phishing campaign known as "ZipLine." It uses DNS tunneling for stealthy communication and is designed for remote command execution and data theft.	Social-engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	d39e177261ce9a354b4712f820ada3ee8cd84a277f173ecfbd1bf6b100ddb713

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-7775	✗	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-119	T1059: Command and Scripting Interpreter;
		T1499: Endpoint Denial of Service;
		T1190: Exploit Public-Facing Application
			https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗	Ivanti Connect Secure and Policy Secure	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter; T1133: External Remote Service	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46805	✗	Ivanti Connect Secure and Policy Secure	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400	✗	Palo Alto Networks PAN-OS	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77 CWE-20	T1190 : Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20273	✗	Cisco IOS XE Software	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	-
Cisco IOS XE Web UI Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20198	✗	Cisco IOS XE Software	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	-
Cisco IOS XE Web UI Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-420	T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0171	✗	Cisco IOS and IOS XE Software	Salt Typhoon
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios:15.2\(5\)e:*:*:*:*:*:*:*	-
Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-20	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54948	✗	Trend Micro Apex One Management Server Version 14039 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	-
Trend Micro Apex One OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting; T1203 : Exploitation for Client Execution	https://success.trendmicro.com/en-US/solution/KA-0020652

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54987	✗	Trend Micro Apex One Management Server Version 14039 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	-
Trend Micro Apex One Management Console Command Injection RCE Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting; T1203 : Exploitation for Client Execution	https://success.trendmicro.com/en-US/solution/KA-0020652

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Cookie Spider	-	All	Worldwide (Except Russia)
	MOTIVE		
	Information Theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	SHAMOS	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0010: Exfiltration; TA0006: Credential Access; TA0005: Defense Evasion; TA0003: Persistence; TA0009: Collection; T1041: Exfiltration Over C2 Channel; T1583.001: Domains; T1583: Acquire Infrastructure; T1189: Drive-by Compromise; T1204: User Execution; T1027.010: Command Obfuscation; T1027: Obfuscated Files or Information; T1105: Ingress Tool Transfer; T1059.002: AppleScript; T1059: Command and Scripting Interpreter; T1555: Credentials from Password Stores; T1555.001: Keychain; T1005: Data from Local System			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Salt Typhoon (aka GhostEmperor, OPERATOR PANDA, RedMike, UNC5807, FamousSparrow)	China	Telecommunications, Government, Transportation, Lodging, Military	United States, Australia, Canada, New Zealand, United Kingdom
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2024-21887 CVE-2023-46805 CVE-2024-3400 CVE-2023-20273 CVE-2023-20198 CVE-2018-0171	-	Ivanti Connect Secure and Policy Secure, Palo Alto Networks PAN-OS, Cisco IOS XE Software
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1090: Proxy; T1090.003: Multi-hop Proxy; T1071: Application Layer Protocol; T1595: Active Scanning; T1590: Gather Victim Network Information; T1590.004: Network Topology; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1584: Compromise Infrastructure; T1584.008: Network Devices; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1199: Trusted Relationship; T1569: System Services; T1609: Container Administration Command; T1059: Command and Scripting Interpreter; T1059.006: Python; T1059.008: Network Device CLI; T1136: Create Account; T1136.001: Local Account; T1543: Create or Modify System Process; T1543.005: Container Service; T1098: Account Manipulation; T1098.004: SSH Authorized Keys; T1068: Exploitation for Privilege Escalation; T1110: Brute Force; T1110.002: Password Cracking; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1562.004: Disable or Modify System Firewall; T1610: Deploy Container; T1070: Indicator Removal; T1070.009: Clear Persistence; T1599: Network Boundary Bridging; T1040: Network Sniffing; T1556: Modify Authentication Process; T1003: OS Credential Dumping; T1082: System Information Discovery; T1016: System Network Configuration Discovery;T1021: Remote Services; T1021.004: SSH; T1560: Archive Collected Data; T1602.001: SNMP (MIB Dump); T1602.002: Network Device Configuration Dump; T1005: Data from Local System; T1571: Non-Standard Port; T1572: Protocol Tunneling; T1095: Non-Application Layer Protocol; T1048: Exfiltration Over Alternative Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Storm-0501	-	Critical infrastructure, Government, Law enforcement, Energy, Aerospace, Defense, Healthcare, and Financial services, Agriculture, Media, and Consumer goods	Worldwide
	MOTIVE		
	Financial Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	-

TTPs
TA0040: Impact; TA0001: Initial Access; TA0002: Execution; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; T1567.002: Exfiltration to Cloud Storage; T1530: Data from Cloud Storage; T1486: Data Encrypted for Impact; T1485: Data Destruction; T1484: Domain Policy Modification; T1134: Access Token Manipulation; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1484.002: Domain Trust Modification; T1134.002: Create Process with Token; T1003.006: DCSync; T1482: Domain Trust Discovery; T1059: Command and Scripting Interpreter; T1133: External Remote Services; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059.009: Cloud API; T1098.003: Additional Cloud Roles; T1098: Account Manipulation; T1003: OS Credential Dumping; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1136.001: Local Account; T1059.001: PowerShell; T1136: Create Account; T1087: Account Discovery; T1087.002: Domain Account; T1021: Remote Services; T1567: Exfiltration Over Web Service; T1053.005: Scheduled Task; T1053: Scheduled Task/Job

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **Cookie Spider, Salt Typhoon, Storm-0501** and malware **SHAMOS, MixShell.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Salt Typhoon,** and malware **SHAMOS, MixShell,** in Breach and Attack Simulation(BAS).

Threat Advisories

New SHAMOS Stealer Exploits One-Line Commands on macOS

August 2025 Linux Patch Roundup

ZipLine Campaign Spins Web Around U.S. Supply Chain Manufacturers with MixShell

CVE-2025-7775: Actively Exploited Critical Flaw in Citrix NetScaler

Salt Typhoon Cyber Attacks Hit 200 Organizations in the United States

Storm-0501’s Shift to Cloud-Native Ransomware

Trend Micro Warns of Active Exploits in Apex One Console

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

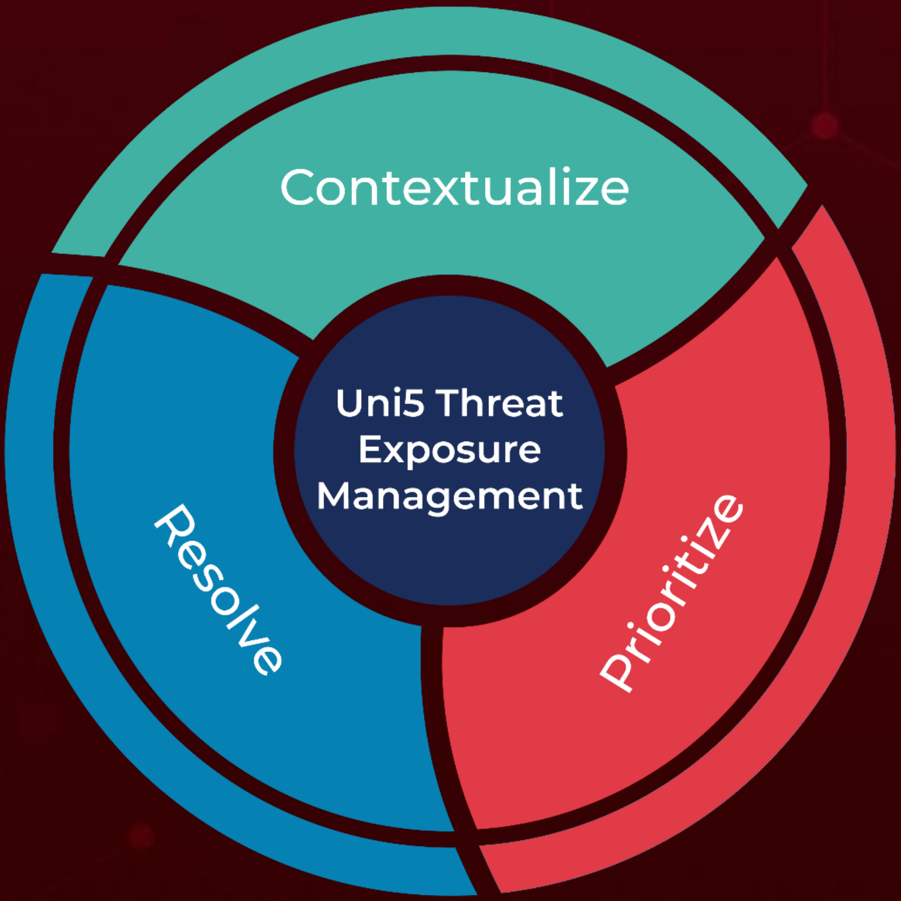
Attack Name	TYPE	VALUE
SHAMOS	SHA256	4549e2599de3011973fde61052a55e5cdb770348876abc82de14c2d99575790f, b01c13969075974f555c8c88023f9abf891f72865ce07efbcee6c2d906d410d5, a4e47fd76dc8ed8e147ea81765edc32ed1e11cff27d138266e3770c7cf953322, 95b97a5da68fcb73c98cd9311c56747545db5260122ddf6fae7b152d3d802877
	URLs	hxxps[:]//icloudservers[.]com/gm/update, hxxps[:]//macostutorial[.]com/iterm2/update
MixShell	SHA256	d39e177261ce9a354b4712f820ada3ee8cd84a277f173ecfbd1bf6b100ddb713

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

September 1, 2025 • 7:30 AM

More at www.hivepro.com