

Date of Publication
July 28, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

21 to 27 JULY 2025

Table Of Contents

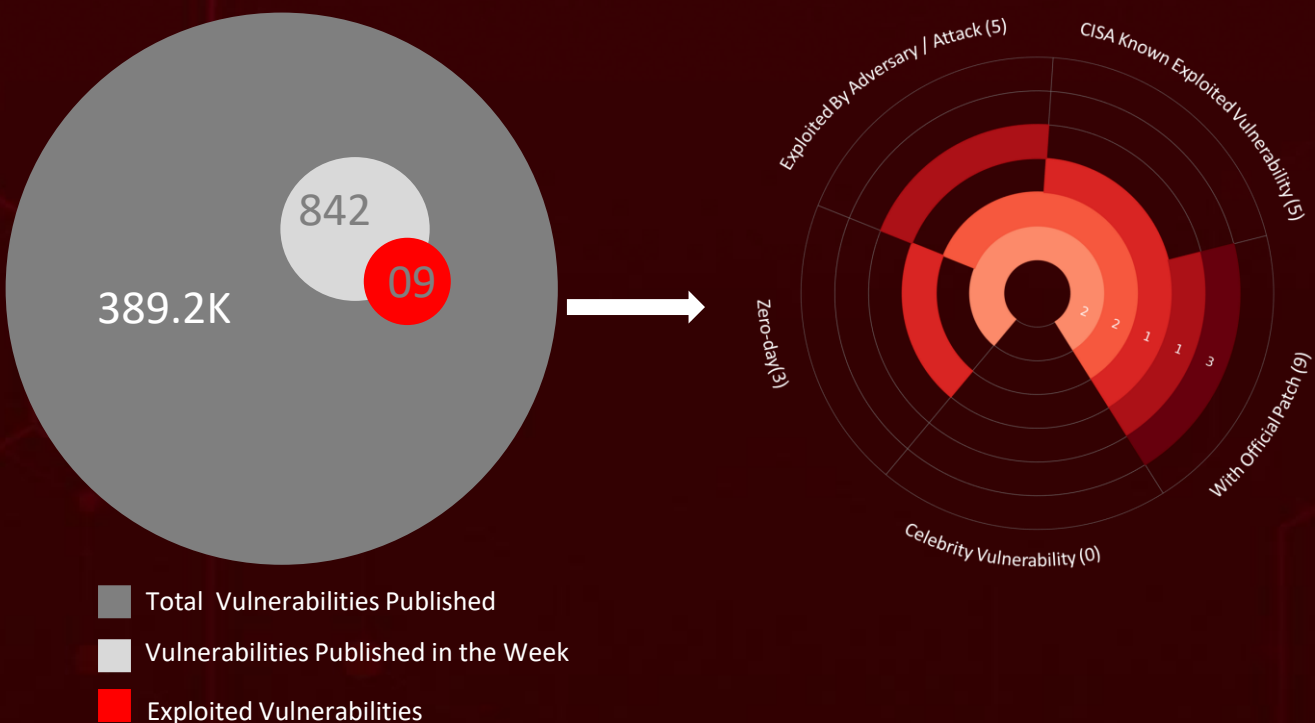
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	23
<u>Threat Advisories</u>	24
<u>Appendix</u>	25
<u>What Next?</u>	28

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **six** major attacks were detected, **nine** critical vulnerabilities were actively exploited, and **seven** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the most notable threats is **CVE-2025-54309**, a zero-day vulnerability in CrushFTP, a widely used enterprise file transfer solution. This flaw allows attackers to gain full administrative control via the web interface in deployments that don't use the DMZ proxy. Another critical zero-day, **CVE-2025-53770**, is being actively exploited in Microsoft SharePoint Servers, with China-backed groups **Linen Typhoon**, **Violet Typhoon**, and **Storm-2603** leveraging it to infiltrate vulnerable systems.

Financially motivated and espionage-driven threats are also on the rise. The **Greedy Sponge** cybercriminal group has been targeting Mexican organizations using tailored variants of the **AllaKore RAT** to steal financial data and commit fraud. Separately, **UNG0901** launched **Operation CargoTalon**, a cyber-espionage campaign against Russia's aerospace and defense sector. The attackers use malicious .LNK files to deliver a lightweight implant called **EAGLET**, enabling stealthy data theft and long-term access. Together, these incidents reflect a global escalation in cyber operations, reinforcing the urgent need for robust, adaptive cybersecurity strategies.



High Level Statistics

6

Attacks
Executed

- [PureRAT](#)
- [Ghost Crypt](#)
- [AllaKore RAT](#)
- [SystemBC](#)
- [EAGLET](#)
- [TINYHELL](#)

9

Vulnerabilities
Exploited

- [CVE-2025-54309](#)
- [CVE-2025-53770](#)
- [CVE-2025-53771](#)
- [CVE-2025-49706](#)
- [CVE-2025-49704](#)
- [CVE-2025-20281](#)
- [CVE-2025-20282](#)
- [CVE-2025-20337](#)
- [CVE-2025-21590](#)

7

Adversaries in
Action

- [Linen Typhoon](#)
- [Violet Typhoon](#)
- [Storm-2603](#)
- [APT41](#)
- [Greedy Sponge](#)
- [UNG0901](#)
- [UNC3886](#)



Insights

Flaws in Cisco ISE and ISE-PIC CVE-2025-20281, -20282, and -20337 could undermine enterprise security controls if left unpatched.

APT41 Expands Its Reach: China-linked group exploits misconfigurations to exfiltrate sensitive credentials.

CVE-2025-54309: A critical flaw in the popular enterprise file transfer solution CrushFTP opens the door to potential exploitation.

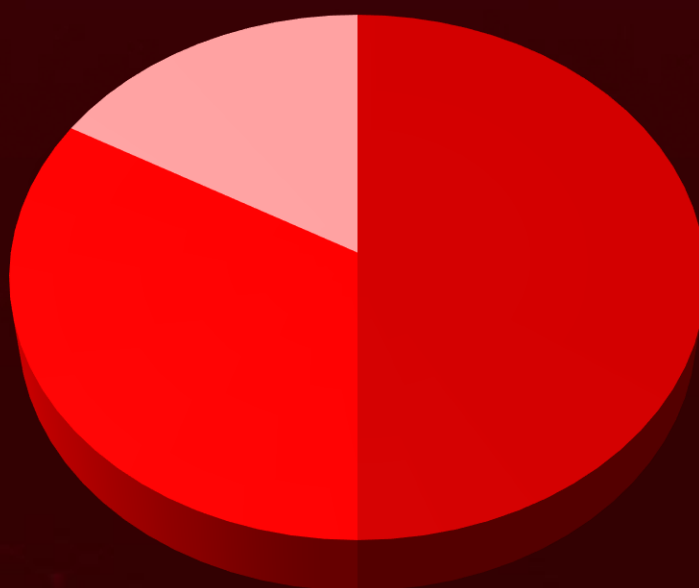
CVE-2025-53770 Actively Exploited in SharePoint Servers, China-linked threat actors are targeting unpatched on-prem environments in the wild.

Operation CargoTalon

UNG0901's targeted intrusions reveal growing cyber interest in defense technologies.

Greedy Sponge A financially motivated group leverages stealthy tools to harvest banking data.

Threat Distribution



■ RAT

■ Tool

■ Backdoor

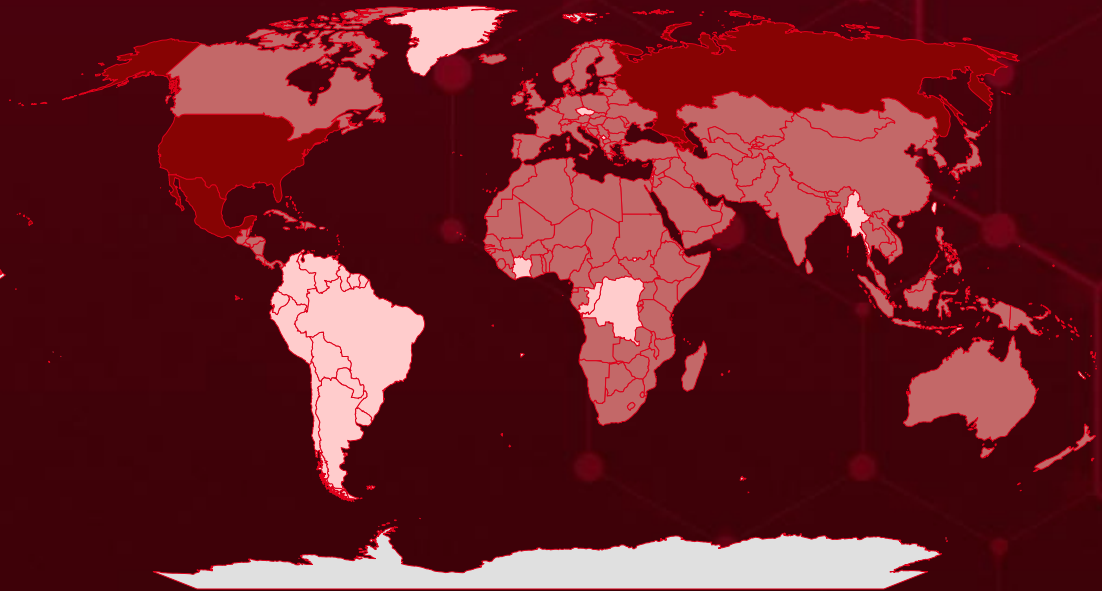


Targeted Countries

Most



Least



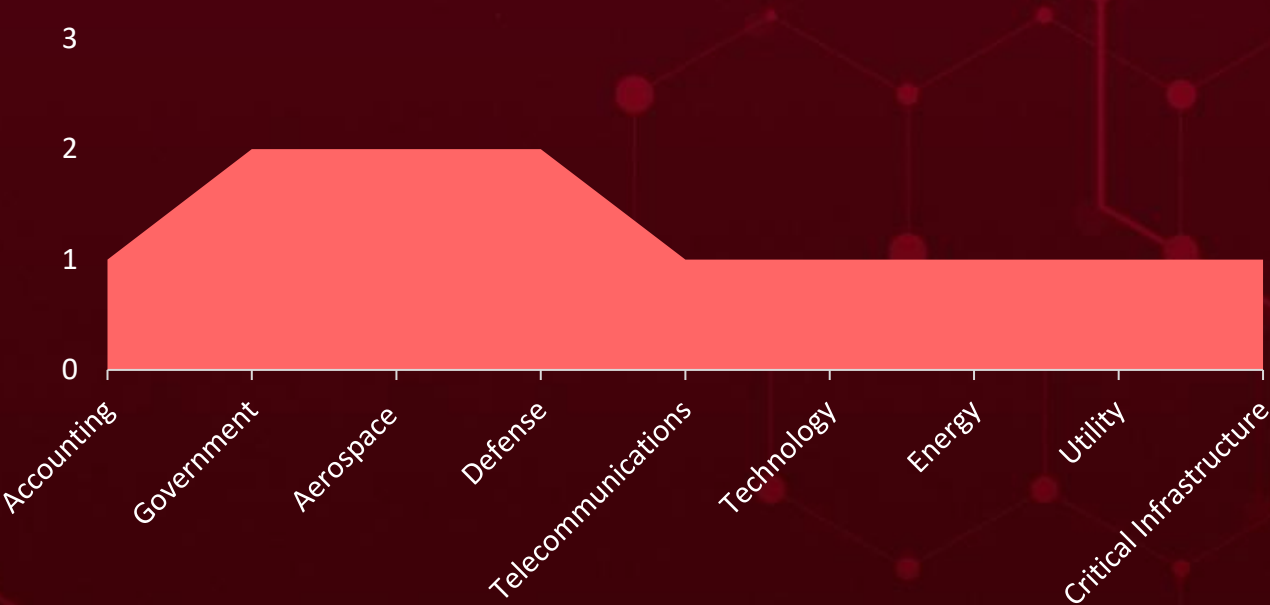
Powered by Bing

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

Countries	Countries	Countries	Countries
United States	Belize	China	Saudi Arabia
Russia	Albania	Palau	India
Cyprus	Benin	Comoros	Serbia
Armenia	Namibia	Poland	Indonesia
Mexico	Bhutan	Costa Rica	Sierra Leone
Azerbaijan	Papua New Guinea	Angola	Iran
Georgia	Bosnia and Herzegovina	Croatia	Slovakia
Somalia	Saint Lucia	San Marino	Iraq
Mongolia	Botswana	Cuba	Solomon Islands
Afghanistan	Singapore	Seychelles	Ireland
Austria	Brunei	Andorra	South Africa
Qatar	Spain	Slovenia	Israel
Algeria	Bulgaria	Denmark	South Sudan
Tunisia	Thailand	South Korea	Italy
Bahamas	Burkina Faso	Djibouti	Sri Lanka
Malta	Uganda	Sudan	Jamaica
Bahrain	Burundi	Dominica	Sweden
Oman	Yemen	Tajikistan	Japan
Bangladesh	Cabo Verde	Dominican Republic	Syria
Senegal	Luxembourg	Tonga	Jordan
Barbados	Cambodia	Egypt	Tanzania
Switzerland	Maldives	Turkmenistan	Kazakhstan
Belarus	Cameroon	El Salvador	Togo
Antigua and Barbuda	Mauritania	United Arab Emirates	Kenya
Belgium	Canada	Vanuatu	Trinidad and Tobago
Malawi	Moldova		Kiribati



Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1071

Application Layer Protocol

T1071.001

Web Protocols

T1059.001

PowerShell

T1140

Deobfuscate/Decode Files or Information

T1041

Exfiltration Over C2 Channel

T1005

Data from Local System

T1218

System Binary Proxy Execution

T1068

Exploitation for Privilege Escalation

T1543.003

Windows Service

T1566.001

Spearphishing Attachment

T1566

Phishing

T1588.006

Vulnerabilities

T1588

Obtain Capabilities

T1082

System Information Discovery

T1090

Proxy

T1190

Exploit Public-Facing Application

T1505

Server Software Component

T1036

Masquerading

T1033

System Owner/User Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PureRAT	PureRAT is a modern and highly capable Remote Access Trojan (RAT) that was first identified in January 2023. Engineered for stealth and flexibility, this malware gives attackers complete control over compromised systems. Once deployed, PureRAT can quietly monitor user activity, log keystrokes, steal sensitive data, and upload additional malicious payloads. It also has the ability to hijack webcams and microphones for surveillance, disable security tools, and install itself in a way that ensures persistence even after system reboots. Unlike older RATs, PureRAT is modular and lightweight, making it easier to customize and harder to detect.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	-
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Ghost Crypt	Ghost Crypt emerged on April 15, 2025, when it was first advertised on Hackforums by a newly created account under the name “ghostcrypt.” Marketed as a crypting and sideloading service, Ghost Crypt offers advanced obfuscation techniques designed to help threat actors bypass security defenses. It supports packing both executable (EXE) and dynamic link library (DLL) files, making it versatile for delivering a wide range of malicious payloads while evading detection.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Encryption	-
Tool			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	69a40bd2f667845ab95ad8438dae390f2e8b9680f4d30cb20e920c45cda565f9		

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 CVE
<u>AllaKore RAT</u>	AllaKore RAT is a lightweight, open-source remote access tool written in Delphi, first observed in the wild in 2015. Despite its simplicity, it serves as a powerful spying and data exfiltration utility. Once deployed on a victim's system, AllaKore can silently record keystrokes, capture screenshots, transfer files to and from the infected device, and even grant attacker's full remote control.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
TYPE			PATCH LINK
RAT			
ASSOCIATED ACTOR			-
Greedy Sponge			
IOC TYPE	VALUE		
SHA256	20fe630a63dd1741ec4ade9fe05b2e7e57208f776d5e20bbf0a012fea96ad0c0, f76b456cf2af1382325c704bf70b5168d28d30da0f3d0a5207901277e01db395, 4bf4bcf1cc45d9e50efbd184aad827e2c81f900a53961cf4fbea90fa31ca7549		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SystemBC</u>	SystemBC is a multi-platform malware proxy tool and Remote Access Trojan (RAT) written in C, with indications of Russian origins. It has become increasingly popular among cybercriminals due to its ability to maintain a persistent connection to compromised systems. This persistent access enables attackers to remotely deliver and execute a variety of malicious payloads, including additional executables, PowerShell scripts, Windows commands, and .bat or VBS scripts. Designed to act as a proxy and facilitate covert communications, SystemBC plays a key role in enabling follow-up attacks, data theft, or lateral movement within networks, making it an asset in the toolkits of many threat actors.	Phishing	-
		IMPACT	AFFECTED PRODUCT
		Deliver additional executables, Execute commands	-
TYPE			PATCH LINK
Tool			
ASSOCIATED ACTOR			-
Greedy Sponge			
IOC TYPE	VALUE		
Domain	pachisuave[.]com		

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 CVE
<u>EAGLET</u>	EAGLET is a custom backdoor designed to facilitate data exfiltration and remote command execution on compromised Windows systems. Once deployed, it collects detailed system information and connects to a hard-coded command-and-control (C2) server. Upon establishing this connection, EAGLET processes HTTP responses from the server to retrieve and execute attacker-issued commands. Its streamlined design enables covert communication with the C2 infrastructure, making it an effective tool for persistent access and data theft in targeted intrusions.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	Windows
			PATCH LINK
			-
TYPE			
RAT			
ASSOCIATED ACTOR			
UNG0901			
IOC TYPE	VALUE		
IPv4	185[.]225[.]17[.]104, 188[.]127[.]254[.]44		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TINYHELL</u>	TINYSHELL is a lightweight, fileless backdoor often used by Chinese state-sponsored threat actors in cyberespionage campaigns. Typically delivered via spear-phishing or exploited servers, it operates entirely in memory to evade detection and provides attackers with remote shell access, command execution, file transfer, and proxy capabilities for lateral movement. TINYSHELL leverages obfuscated PowerShell and HTTP/S-based C2 communication, making it stealthy and effective in long-term intrusions.	Exploiting Vulnerability	CVE-2025-21590
		IMPACT	AFFECTED PRODUCT
		System Compromise	Juniper Junos OS
			PATCH LINK
			https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US
TYPE			
Backdoor			
ASSOCIATED ACTOR			
UNC3886			
IOC TYPE	VALUE		
SHA256	98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14d244d8373888		
IPv4:Port	129[.]126[.]109[.]50[:]:22		

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-2025-54309		CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*	-
CrushFTP Unprotected Alternate Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-420	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1211: Exploitation for Defense Evasion	https://www.crushftp.com/download.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53770		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	-
Microsoft SharePoint Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-53771</u>		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*	-
Microsoft SharePoint Server Spoofing Vulnerability		cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707 CWE-22 CWE-20	T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53771




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49706</u>		Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*	-
Microsoft SharePoint Server Spoofing Vulnerability		cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-49704</u>		Microsoft SharePoint Enterprise Server: 2016 - 2019	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*	-
Microsoft SharePoint Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20281</u>		Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20282</u>		Cisco ISE and ISE-PIC Release 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*.:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*.:*:*:*:*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-20337</u>		Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*.:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*.:*:*:*:*	-
Cisco ISE API Unauthenticated Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21590</u>		Juniper Junos OS	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:juniper:junos:*:*:*:*:*	TINYSHELL
Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter	https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US




Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>Linen Typhoon (aka Emissary Panda, APT 27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Budworm, Group 35, ATK 15, Iron Tiger, Earth Smilodon, Red Phoenix, ZipToken, Iron Taurus, Circle Typhoon)</u></div>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Violet Typhoon (aka APT 31, Judgment Panda, Zirconium, RedBravo, Bronze Vinewood, TA412, Red Keres)</u>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Storm-2603</u>	China	All	United States, Netherlands, Ireland, United Kingdom, Canada
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-53770 CVE-2025-53771 CVE-2025-49706 CVE-2025-49704	-	Microsoft SharePoint Server

TTPs


TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1505.003: Web Shell; T1552.001: Credentials In Files; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1021.002: SMB/Windows Admin Shares; T1071.001: Web Protocols; T1033: System Owner/User Discovery; T1505: Server Software Component; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1047: Windows Management Instrumentation; T1505.004: IIS Components; T1053.005: Scheduled Task; T1484.001: Group Policy Modification; T1620: Reflective Code Loading; T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1003.001: LSASS Memory; T1570: Lateral Tool Transfer; T1119: Automated Collection; T1005: Data from Local System; T1090: Proxy; T1486: Data Encrypted for Impact


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)</u></div>	China	Government IT Services	Africa
	MOTIVE		
	Financial crime, Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	Windows
TTPs			
TA0008: Lateral Movement; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0001: Initial Access; TA0010: Exfiltration; TA0040: Impact; TA0007: Discovery; T1574.001: DLL; T1078: Valid Accounts; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1078.002: Domain Accounts; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1190: Exploit Public-Facing Application; T1567: Exfiltration Over Web Service; T1543.003: Windows Service; T1614.001: System Language Discovery; T1505.003: Web Shell; T1505: Server Software Component; T1505.004: IIS Components; T1543.003: Windows Service; T1543: Create or Modify System Process; T1055: Process Injection; T1140: Deobfuscate/Decode Files or Information; T1070.004: File Deletion; T1070: Indicator Removal; T1036: Masquerading; T1555: Credentials from Password Stores; T1003.002: Security Account Manager; T1003: OS Credential Dumping; T1552: Unsecured Credentials; T1555.003: Credentials from Web Browsers; T1046: Network Service Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1570: Lateral Tool Transfer; T1021.002: SMB/Windows Admin Shares; T1021: Remote Services; T1560.001: Archive via Utility; T1560: Archive Collected Data; T1119: Automated Collection; T1005: Data from Local System; T1071.001: Web Protocols; T1071.004: DNS; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1090.001: Internal Proxy; T1090: Proxy; T1572: Protocol Tunneling; T1048: Exfiltration Over Alternative Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Greedy Sponge</u>	-	All	Mexico
	MOTIVE		
	Financial crime		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	AllaKore RAT, SystemBC	-

TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1591: Gather Victim Org Information; T1591.001: Determine Physical Locations; T1027: Obfuscated Files or Information; T1027.015: Compression; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1204: User Execution; T1204.002: Malicious File; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1070: Indicator Removal; T1070.004: File Deletion; T1132: Data Encoding; T1132.001: Standard Encoding; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1140: Deobfuscate/Decode Files or Information; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1041: Exfiltration Over C2 Channel; T1555: Credentials from Password Stores; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1218: System Binary Proxy Execution; T1218.003: CMSTP; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNG0901	-	Aerospace and Defense	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	EAGLET	Windows
TTPs			
TA0007: Discovery; TA0002: Execution; TA0003: Persistence; TA0040: Impact; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; TA0001: Initial Access; TA0010: Exfiltration; T1041: Exfiltration Over C2 Channel; T1537: Transfer Data to Cloud Account; T1059: Command and Scripting Interpreter; T1566.001: Spearphishing Attachment; T1059.001: PowerShell; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1566: Phishing; T1574.002: DLL; T1036: Masquerading; T1082: System Information Discovery; T1482: Domain Trust Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1005: Data from Local System			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>UNC3886</u>	China	Government, Telecommunications, Technology, Aerospace, Defense, Energy, Utility, Critical Infrastructure	North America, Oceania, Europe, Africa, and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-21590	TINYSHELL	Juniper Junos OS
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0042: Resource Development; TA0005: Defense Evasion; TA0006: Credential Access; TA0003: Persistence; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1600: Weaken Encryption; T1041: Exfiltration Over C2 Channel; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities; T1059: Command and Scripting Interpreter; T1014: Rootkit; T1021.004: SSH; T1021: Remote Services; T1078: Valid Accounts; T1078.001: Default Accounts; T1068: Exploitation for Privilege Escalation; T1562: Impair Defenses; T1090: Proxy; T1202: Indirect Command Execution; T1140: Deobfuscate/Decode Files or Information; T1095: Non-Application Layer Protocol; T1588.004: Digital Certificates; T1584: Compromise Infrastructure; T1071.001: Web Protocols; T1071: Application Layer Protocol			

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 actors **Linen Typhoon, Violet Typhoon, Storm-2603, APT41, Greedy Sponge, UNG0901, UNC3886**, and malware **PureRAT, Ghost Crypt, AllaKore RAT, SystemBC, EAGLET, TINYSHELL**.

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

- Run 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 actors **Linen Typhoon, Violet Typhoon, Storm-2603, APT41, Greedy Sponge, UNG0901, UNC3886**, and malware **PureRAT, AllaKore RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[Critical Zero-Day in CrushFTP Exposes Admin Interface](#)

[Zero Day Watch CVE-2025-53770 Turns SharePoint into a Pivot Point](#)

[Ghost Crypt Delivers PureRAT in Accounting Firm Attack](#)

[Critical Cisco ISE Flaws Actively Exploited in the Wild](#)

[APT41 Targets African Government IT Services](#)

[Greedy Sponge's Stealthy RAT Attack in Mexico](#)

[Operation CargoTalon: Targeting Russian Aerospace & Defense Sector](#)

[UNC3886 Covert Operations Leveraging Rootkits and Backdoored Applications](#)

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
<u>Ghost Crypt</u>	SHA256	69a40bd2f667845ab95ad8438dae390f2e8b9680f4d30cb20e920c45cda565f9
<u>AllaKore RAT</u>	SHA256	20fe630a63dd1741ec4ade9fe05b2e7e57208f776d5e20bbf0a012fea96ad0c0, f76b456cf2af1382325c704bf70b5168d28d30da0f3d0a5207901277e01db395, 4bf4bcf1cc45d9e50efbd184aad827e2c81f900a53961cf4fbea90fa31ca7549, fed1c094280d1361e8a9aafdb4c1b3e63e0f2e5bb549d5d737d0a33f2b63b4b8, 5d16547900119112c12a755e099bed1fafe1890869df4db297a6a21ec40185b0, e9cd7c4db074c8e7c6b488a724be1cd05c8536dae28674ce3aa48ebb258e3c31, 32ef3a0da762bc88afb876537809350a885bbbc3ec59b1838e9e9ccc0a04b081, d8343068669d8fbb52b0af87bd3d4f3579d76192d021b37b6fd236b0973e4a5d, 53b85d1b7127c365a4ebae5f22ed479cd5d7e9efc716fb9df68ebdd18551834a, 84b046a4dbfcd9d4b2d62b4bc8faaf4c6395696f1e688f464bc9e0b760885263, 50e5cd438024b34ba638e170f6e4595b0361dedb0ea925d06d06f68988468ddf

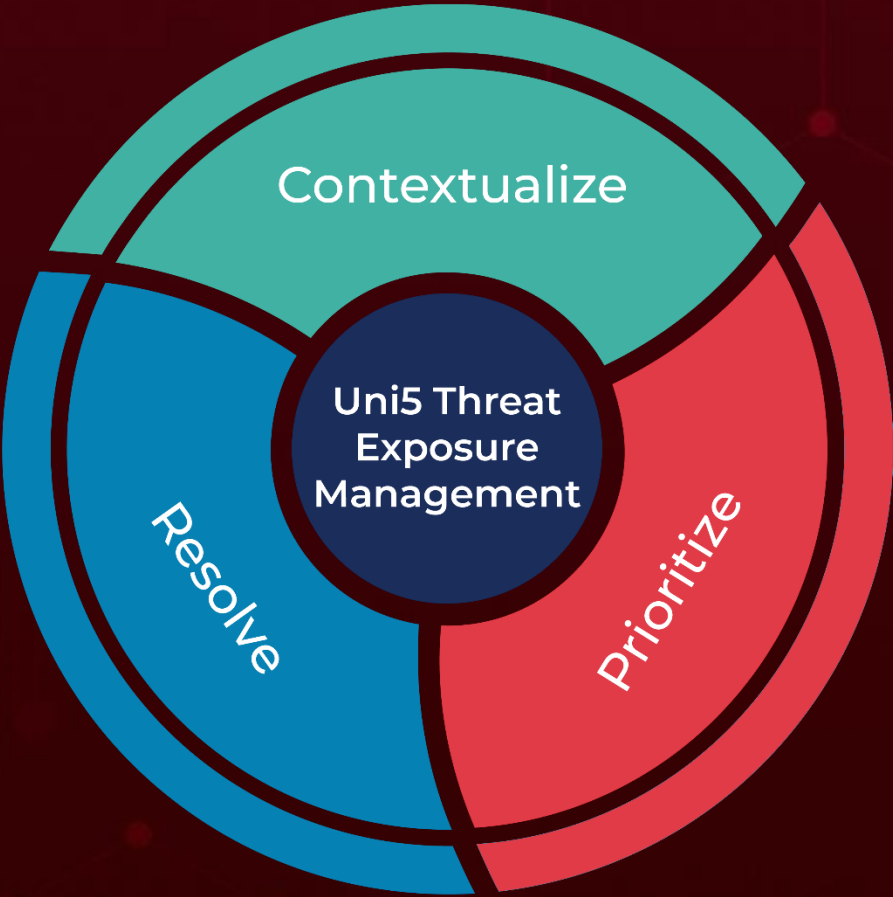
Attack Name	TYPE	VALUE
<u>AllaKore RAT</u>	Domain	manzisuape[.]com, siperasul[.]com, cupertujo[.]com, idaculipa[.]com, mepunico[.]com, barrosuon[.]com, tllemeuas[.]com
<u>SystemBC</u>	Domain	pachisuave[.]com
<u>EAGLET</u>	IPv4	185[.]225[.]17[.]104, 188[.]127[.]254[.]44
<u>TINYHELL</u>	MD5	2c89a18944d3a895bd6432415546635e, aac5d83d296df81c9259c9a533a8423a, 8023d01ffb7a38b582f0d598afb974ee, 5724d76f832ce8061f74b0e9f1dcad90, e7622d983d22e749b3658600df00296d, b9e4784fa0e6283ce6e2094426a02fce, bf80c96089d37b8571b5de7cab14dd9f, 3243e04afe18cc5e1230d49011e19899
	SHA1	50520639cf77df0c15cc95076fac901e3d04b708, 1a6d07da7e77a5706dd8af899ebe4daa74bbbe91, 06a1f879da398c00522649171526dc968f769093, f8697b400059d4d5082eee2d269735aa8ea2df9a, cf7af504ef0796d91207e41815187a793d430d85, 01735bb47a933ae9ec470e6be737d8f646a8ec66, cec327e51b79cf11b3eeffebf1be8ac0d66e9529, 2e9215a203e908483d04dfc0328651d79d35b54f
	SHA256	98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14 d244d8373888, 5bef7608d66112315eefff354dae42f49178b7498f994a728ae6 203a8a59f5a2, c0ec15e08b4fb3730c5695fb7b4a6b85f7fe341282ad469e4e14 1c40ead310c3, 5995aaff5a047565c0d7fe3c80fa354c40e7e8c3e7d4df292316c 8472d4ac67a, 905b18d5df58dd6c16930e318d9574a2ad793ec993ad2f68bca 813574e3d854b, e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd411 82deea978400ed, 3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd 1065723f11f7e, 7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc 3ae56cfd13b4

Attack Name	TYPE	VALUE
<u>TINYSHELL</u>	IPv4:Port	129[.]126[.]109[.]50[:]22, 116[.]88[.]34[.]184[:]22, 223[.]25[.]78[.]136[:]22, 45[.]77[.]39[.]28[:]22, 101[.]100[.]182[.]122[:]22, 118[.]189[.]188[.]122[:]22, 158[.]140[.]135[.]244[:]22, 8[.]222[.]225[.]8[:]22

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
July 28, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com