

Date of Publication  
August 4, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities, and Actors**

28 JULY to 3 AUGUST 2025

# Table Of Contents

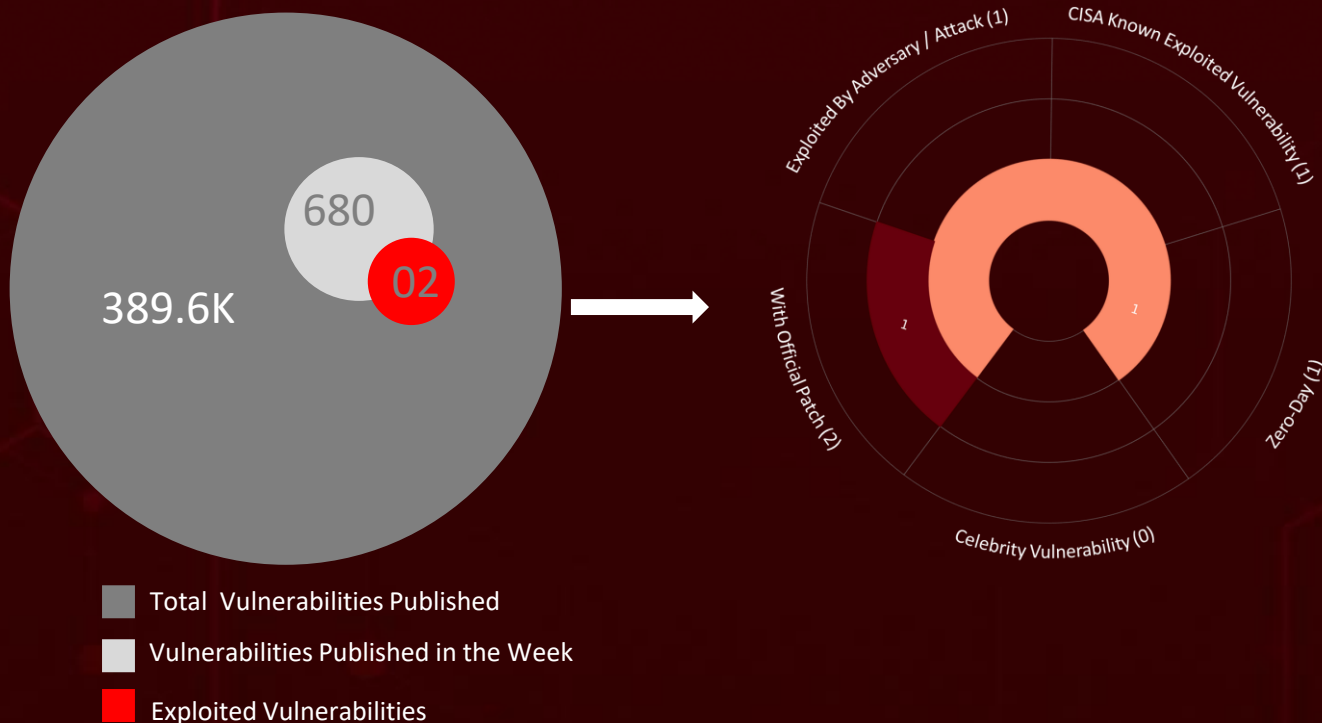
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	12
<u>Recommendations</u>	14
<u>Threat Advisories</u>	15
<u>Appendix</u>	16
<u>What Next?</u>	18

# 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, **two** critical vulnerabilities were actively exploited, and **two** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

One of the critical vulnerabilities observed was **CVE-2025-5394** in the widely used Alone WordPress theme. This flaw allows attackers to upload malicious files without authentication, no login credentials or admin rights required. In another case, the **Auto-Color** backdoor was deployed by exploiting **CVE-2025-31324**, a critical flaw in SAP NetWeaver. Meanwhile, the financially motivated group **Scattered Spider** launched a campaign in mid-2025 targeting VMware vSphere environments, using social engineering to infiltrate Active Directory and then exploiting vCenter and ESXi for credential theft and ransomware deployment.

On the espionage front, Chinese-linked threat actors behind **Operation GhostChat** and **Operation PhantomPrayers** intensified surveillance efforts against the Tibetan community. At the same time, the Russian state-sponsored group **Secret Blizzard** has been targeting diplomats in Moscow through a deceptive tactic: luring victims into downloading a fake antivirus installer, which silently delivers the stealthy **ApolloShadow** malware. Together, these incidents reflect a growing and global escalation in cyber operations, emphasizing the critical need for proactive, resilient cybersecurity strategies.



# High Level Statistics

6

Attacks  
Executed

- [NailaoLocker](#)
- [Auto-color](#)
- [Bert Ransomware](#)
- [Ghost RAT](#)
- [PhantomNet](#)
- [ApolloShadow](#)

2

Vulnerabilities  
Exploited

- [CVE-2025-31324](#)
- [CVE-2025-5394](#)

2

Adversaries in  
Action

- [Scattered Spider](#)
- [Secret Blizzard](#)



# Insights

## BERT Ransomware

A fast-evolving threat uses Session for negotiation and hits global enterprises hard.

## CVE-2025-5394: Wordpress Alone

Theme Flaw, allows attackers to upload malware without logging in, affecting thousands of WordPress sites.

**Auto-Color:** A critical vulnerability opens the door to stealthy backdoor installation and long-term compromise.

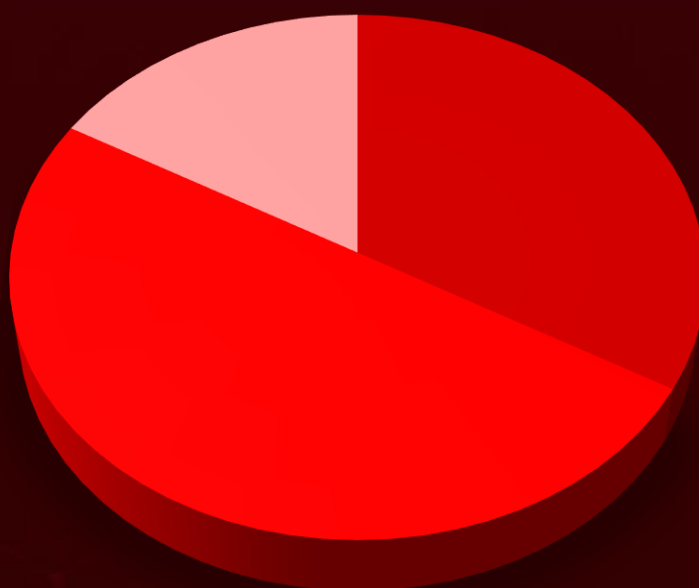
**Scattered Spider** leverages persuasive social engineering to gain Active Directory access, exploit VMware infrastructure, and steal credentials.

**Operation GhostChat and Operation PhantomPrayers** Tailored malware disguised behind fake apps puts Tibetan users in the crosshairs.

## Secret Blizzard

leads a sophisticated cyber-espionage campaign silently breaches diplomatic networks in Russia's capital.

## Threat Distribution



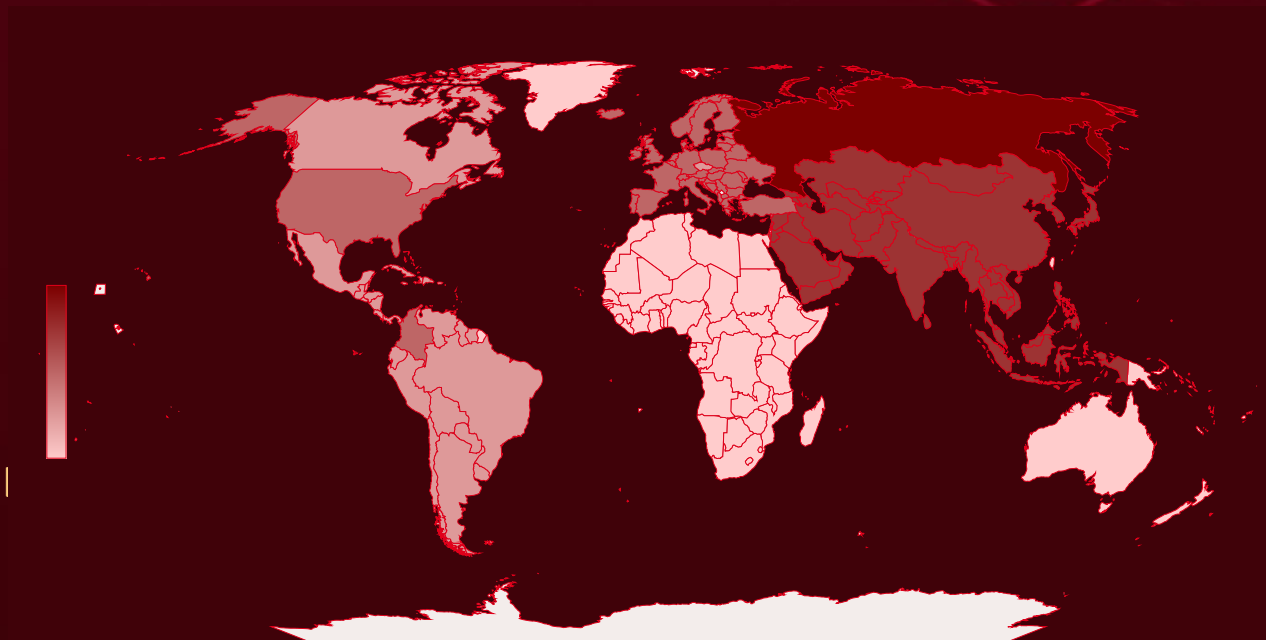
■ Ransomware

■ Backdoor

■ RAT



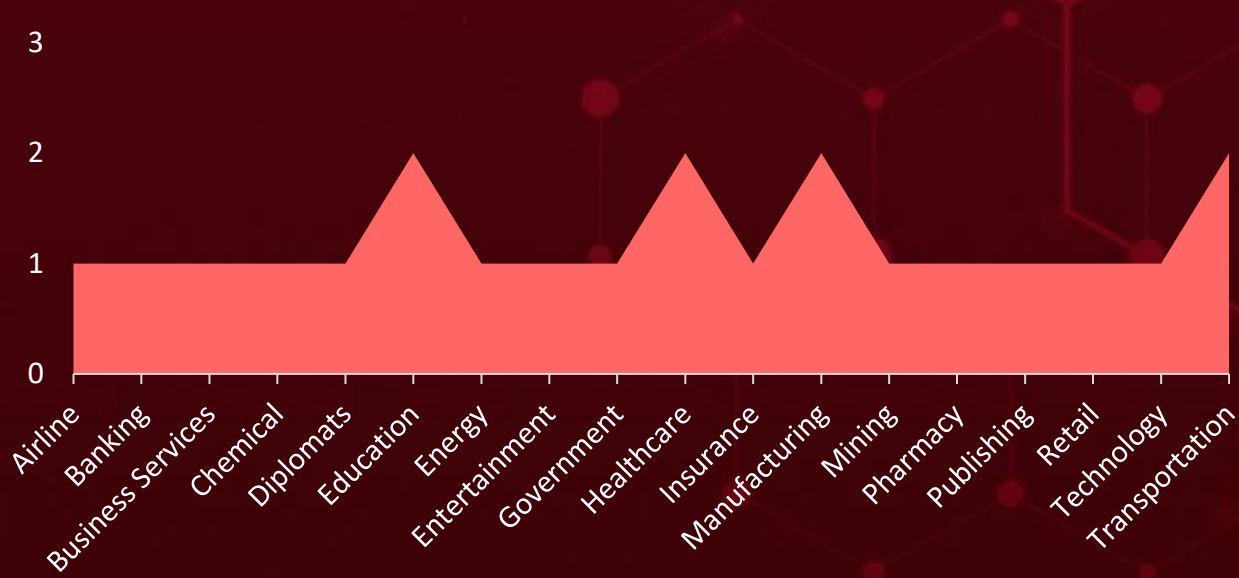
# Targeted Countries



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

Countries	Countries	Countries	Countries
Russia	Iran	Malta	France
Philippines	North Korea	Finland	Ireland
Malaysia	Iraq	Moldova	Liechtenstein
Thailand	Pakistan	Andorra	Romania
Azerbaijan	Israel	Monaco	United States
Nepal	Armenia	Slovakia	Belarus
Bahrain	Qatar	Holy See	Luxembourg
South Korea	Japan	Belgium	San Marino
Bangladesh	Singapore	Montenegro	Italy
Uzbekistan	Jordan	Denmark	Lithuania
Bhutan	Sri Lanka	Hungary	Uruguay
Mongolia	Kazakhstan	Turkey	Suriname
Brunei	Tajikistan	Iceland	Peru
Oman	Kuwait	United Kingdom	Bahamas
Cambodia	Timor-Leste	Netherlands	Guyana
Saudi Arabia	Kyrgyzstan	Germany	Jamaica
China	United Arab Emirates	Bosnia and Herzegovina	Panama
Syria	Laos	Colombia	Canada
Cyprus	Vietnam	North Macedonia	Saint Lucia
Turkmenistan	Lebanon	Slovenia	Chile
Georgia	Afghanistan	Norway	Guatemala
Yemen	Sweden	Spain	Antigua and Barbuda
India	Serbia	Albania	Honduras
Maldives	Ukraine	State of Palestine	Costa Rica
Indonesia	Greece	Bulgaria	El Salvador
Myanmar	Croatia		Barbados

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1027

Obfuscated  
Files or  
Information

### T1059

Command and  
Scripting  
Interpreter

### T1204

User  
Execution

### T1071

Application  
Layer Protocol

### T1041

Exfiltration  
Over C2  
Channel

### T1082

System  
Information  
Discovery

### T1083

File and  
Directory  
Discovery

### T1036

Masquerading

### T1070

Indicator  
Removal

### T1140

Deobfuscate/  
Decode Files  
or Information

### T1070.004

File Deletion

### T1548

Abuse Elevation  
Control  
Mechanism

### T1486

Data  
Encrypted for  
Impact

### T1036.005

Match  
Legitimate  
Resource Name  
or Location

### T1574

Hijack  
Execution  
Flow

### T1005

Data from  
Local System

### T1087

Account  
Discovery

### T1055

Process  
Injection

### T1547

Boot or Logon  
Autostart  
Execution

### T1056

Input Capture



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>NailaoLocker</u>	NailaoLocker is a ransomware distributed by the Green Nailao threat cluster, primarily targeting European healthcare organizations via ShadowPad and PlugX backdoors. It uses AES-256-CTR encryption, appending a ".locked" extension to encrypted files, and demands ransom via a Proton email address.	Exploiting Vulnerability	CVE-2024-24919
		IMPACT	AFFECTED PRODUCT
		Encrypt Data	Check Point Security Gateway
			PATCH LINK
TYPE			
Ransomware			
ASSOCIATED ACTOR			
-			<a href="https://support.checkpoint.com/results/sk/sk182336">https://support.checkpoint.com/results/sk/sk182336</a>
IOC TYPE	VALUE		
SHA256	46f3029fcc7e2a12253c0cc65e5c58b5f1296df1e364878b178027ab26562d68		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Auto-color</u>	A Linux malware strain, Auto-color, is named after the filename it adopts upon installation. Auto-color provides attackers with complete remote control over compromised systems. The malware integrates seamlessly into the system, resisting deletion. If the user lacks root privileges, it halts installation to avoid detection. However, when executed with elevated privileges, it installs a malicious library that mimics a legitimate system library to remain undetected.	Exploiting Vulnerability	CVE-2025-31324
		IMPACT	AFFECTED PRODUCT
		Remote Control, Persistent Presence	SAP NetWeaver
			PATCH LINK
TYPE			
Backdoor			
ASSOCIATED ACTOR			
-			<a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html</a>
IOC TYPE	VALUE		
SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43		

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>Bert Ransomware</u>	BERT ransomware (aka Water Pombero), active since March 2025, has rapidly evolved into a multi-platform threat targeting systems across critical sectors. Leveraging REvil’s code and demanding Bitcoin via the Session messenger, the campaign’s growing operational footprint and double-extortion tactics signal a persistent and escalating threat landscape for global enterprises.	Phishing	
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft and Data exfiltration	Windows, Linux
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE	
<u>Ghost RAT</u>	Gh0st RAT is a notorious remote access trojan designed for Windows systems, widely used in cyber espionage campaigns targeting high-value networks. It provides attackers with complete control over infected machines, allowing them to monitor screens in real time, log keystrokes both online and offline, and stream live audio and video from the victim’s webcam and microphone. The malware can download and execute remote binaries, forcibly shut down or reboot the system, disable user input by locking the keyboard and mouse, and grant shell access for full command execution. Gh0st RAT also allows attackers to monitor running processes and manipulate the System Service Descriptor Table (SSDT) to evade detection.	Social Engineering	-	
		IMPACT	AFFECTED PRODUCT	
TYPE		System Compromise	-	
			ASSOCIATED ACTOR	PATCH LINK
				-
RAT				
IOC TYPE	VALUE			
SHA256	1e5c37df2ace720e79e396bbb4816d7f7e226d8bd3ffc3cf8846c4cf49ab1740			




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
<a href="#">PhantomNet</a>	PhantomNet, also known as SManager, is a stealthy backdoor malware linked to China-nexus APT groups. Typically deployed in multi-stage attacks, PhantomNet is known for its role in maintaining long-term access to compromised systems. It is often delivered through supply-chain compromises or trojanized applications. Once active, it facilitates command execution, data exfiltration, and ongoing surveillance, making it a key tool in the APT arsenal.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
TYPE			PATCH LINK
Backdoor			
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	c9dac9ced16e43648e19a239a0be9a9836b80ca592b9b36b70d0b2bdd85b5157		


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#">ApolloShadow</a>	ApolloShadow is a modular backdoor designed to target Windows systems, typically delivered through phishing emails, fake software updates, or trojanized application downloads. Once it infects a device, it establishes persistence through techniques like registry modifications and DLL side-loading. The malware conducts system reconnaissance, steals user credentials, and may deploy additional payloads. It communicates with a command-and-control (C2) server over encrypted HTTPS channels to exfiltrate stolen data.	Phishing	-
		IMPACT	AFFECTED PRODUCT
		System Compromise	-
TYPE			PATCH LINK
Backdoor			
ASSOCIATED ACTOR			-
Secret Blizzard			
IOC TYPE	VALUE		
SHA256	13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20		


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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-31324</u>		SAP NetWeaver	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*	Auto-color
SAP NetWeaver Unrestricted File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
		CWE-434	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1505: Server Software Component, T1505.003: Web Shell

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-5394</u>		WordPress Alone Theme Version 7.8.3 and below	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:alone_theme:alone_theme:*:*:*:*:*	-
WordPress Alone Theme Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1059 Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	<a href="https://themeforest.net/item/alone-charity-multipurpose-nonprofit-wordpress-theme/15019939?srsltid=AfmBOooSAqUyZH2ZA9U0DOLSX4pH_drgM0BOTtNABJqo1l-WYwYInBjV">https://themeforest.net/item/alone-charity-multipurpose-nonprofit-wordpress-theme/15019939?srsltid=AfmBOooSAqUyZH2ZA9U0DOLSX4pH_drgM0BOTtNABJqo1l-WYwYInBjV</a>

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Scattered Spider (aka UNC3944, Starfraud, Oktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest, Oktapus, DEV-0971, Storm-0971)</u>	-	Retail, Airline, Insurance	United States
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	-	VMware vSphere, Windows
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1566.004: Spearphishing Voice; T1598: Phishing for Information; T1566: Phishing; T1059.001: PowerShell; T1490: Inhibit System Recovery; T1547: Boot or Logon Autostart Execution; T1078.002: Domain Accounts; T1078: Valid Accounts; T1548.001: Setuid and Setgid; T1204: User Execution; T1136: Create Account; T1548: Abuse Elevation Control Mechanism; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1003.003: NTDS; T1003: OS Credential Dumping; T1555: Credentials from Password Stores; T1018: Remote System Discovery; T1087.002: Domain Account; T1087: Account Discovery; T1555.003: Credentials from Web Browsers; T1021: Remote Services; T1005: Data from Local System; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <p><u>Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Pensive Ursa, Blue Python, G0010, Hippo Team, Pfinet, Snake, UAC-0003, UAC-0024, UAC-0144, Uroburos)</u></p>	Russia	Diplomats	Moscow
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	ApolloShadow	-
TTPs			
TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1557: Adversary-in-the-Middle; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1068: Exploitation for Privilege Escalation; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1112: Modify Registry; T1070: Indicator Removal; T1070.004: File Deletion; T1136: Create Account; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1553: Subvert Trust Controls; T1553.004: Install Root Certificate; T1087: Account Discovery; T1071: Application Layer Protocol; T1082: System Information Discovery			

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **Scattered Spider, Secret Blizzard**, and malware **NailaoLocker Ransomware, Auto-color, Bert Ransomware, Ghost RAT, PhantomNet, ApolloShadow**.

## 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 **two exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Scattered Spider, Secret Blizzard**, and malware **NailaoLocker Ransomware, Auto-color, Bert Ransomware, ApolloShadow** in Breach and Attack Simulation(BAS).

# Threat Advisories

[NailaoLocker Ransomware: Basic Design, Deadly Reach](#)

[Auto-Color: The Stealthy Linux Malware Lurking in the Shadows](#)

[BERT Ransomware Quietly Gains Global Ground](#)

[Operation GhostChat and PhantomPrayers Breach Tibetan Trust](#)

[Scattered Spider's Hypervisor Attack on VMware vSphere](#)

[Alone Theme Vulnerability Puts WordPress Sites at Risk](#)

[Secret Blizzard Strikes Moscow with ApolloShadow](#)

# 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)

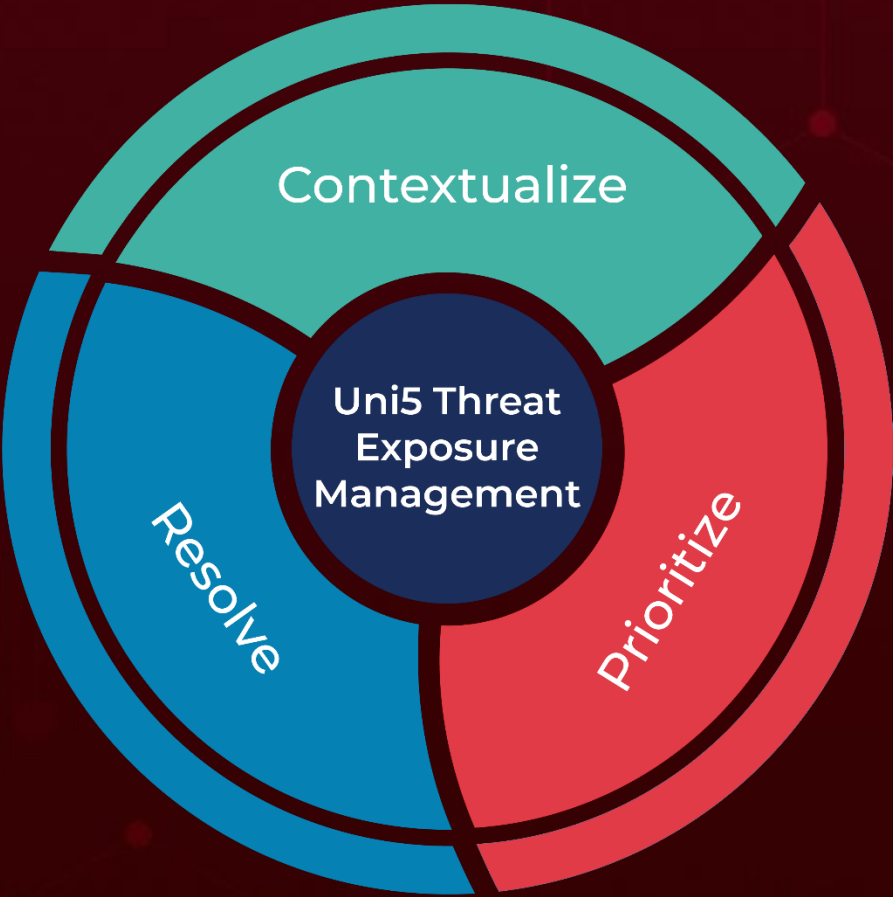
Attack Name	TYPE	VALUE
<u>NailaoLocker</u>	SHA256	46f3029fcc7e2a12253c0cc65e5c58b5f1296df1e364878b178027ab26562d68
<u>Bert Ransomware (aka Water Pombero)</u>	SHA256	c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db
<u>Auto-color</u>	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43
<u>Ghost RAT</u>	MD5	1244b7d19c37baab18348fc2bdb30383
	SHA1	365888661b41cbe827c630fd5eea05c5ddc2480d
	SHA256	1e5c37df2ace720e79e396bbb4816d7f7e226d8bd3ffc3cf8846c4cf49ab1740
	IPv4:Port	104[.]234[.]15[.]90[:]19999

Attack Name	TYPE	VALUE
<u>PhantomNet</u> <u>(SManager)</u>	IPv4:Port	45[.]154[.]12[.]93[:.]2233
	MD5	a74c5c49b6f1c27231160387371889d3
	SHA1	fb32d8461ddb6ca2f03200d85c09f82fb6c5bde3
	SHA256	c9dac9ced16e43648e19a239a0be9a9836b80ca592b9b36b70d0b2bdd85b5157
<u>ApolloShadow</u>	SHA256	13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20

# 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  
**August 4, 2025 • 5:20 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)