

Date of Publication  
February 24, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

17 to 23 February 2025

# Table Of Contents

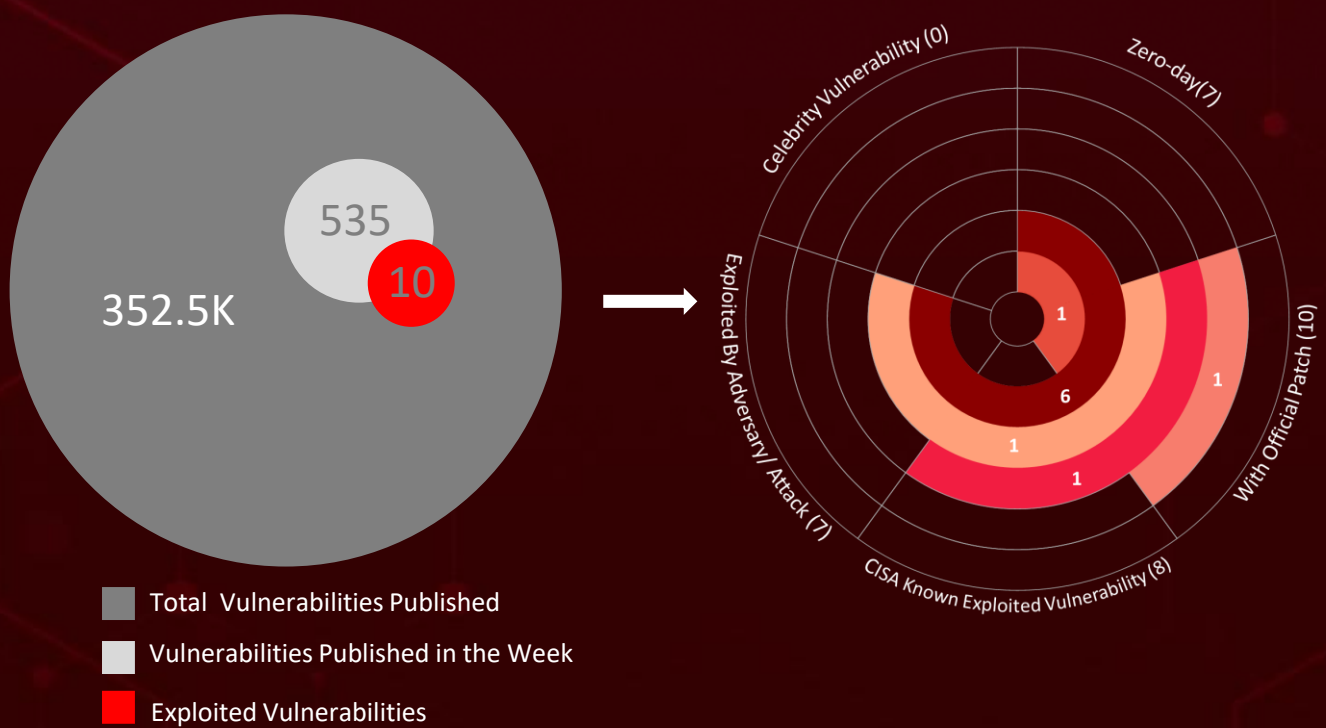
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	20
<u>Recommendations</u>	24
<u>Threat Advisories</u>	25
<u>Appendix</u>	26
<u>What Next?</u>	29

# Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **eleven** attacks, reported **ten** vulnerabilities, and identified **four** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, the new **NailaoLocker ransomware** exploits a Check Point vulnerability, leveraging ShadowPad and PlugX, tools linked to Chinese state-sponsored hackers. The **RevivalStone campaign** by China-based **Winnti Group** targeted Japanese companies in March 2024, using advanced malware and stealth tactics to infiltrate networks.

Furthermore, this week, **Salt Typhoon** has been targeting U.S. telecoms by exploiting Cisco devices, using stolen credentials, **CVE-2018-0171**, and LOTL techniques to evade detection, with persistent access lasting years. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

11

Attacks  
Executed

- [Lumma Stealer](#)
- [RA World](#)
- [PlugX](#)
- [Vgod](#)
- [XMRig](#)
- [Snake Keylogger](#)
- [Winnti RAT](#)
- [Winnti Loader](#)
- [Winnti Rootkit](#)
- [NailaoLocker](#)
- [Shadowpad](#)

10

Vulnerabilities  
Exploited

- [CVE-2025-0108](#)
- [CVE-2025-1094](#)
- [CVE-2024-12356](#)
- [CVE-2024-12686](#)
- [CVE-2024-0012](#)
- [CVE-2025-26465](#)
- [CVE-2018-0171](#)
- [CVE-2023-20198](#)
- [CVE-2023-20273](#)
- [CVE-2024-24919](#)

4

Adversaries in  
Action

- [Silk Typhoon](#)
- [Emperor](#)
- [Dragonfly](#)
- [Winnti Group](#)
- [Salt Typhoon](#)



# Insights

**CVE-2025-1094** is a high-severity SQL injection in psql, enabling RCE when chained with **CVE-2024-12356**, actively exploited by Silk Typhoon.

A new **Go-based backdoor** malware uses Telegram as its C2 channel, enabling remote control and suggesting a possible Russian origin.

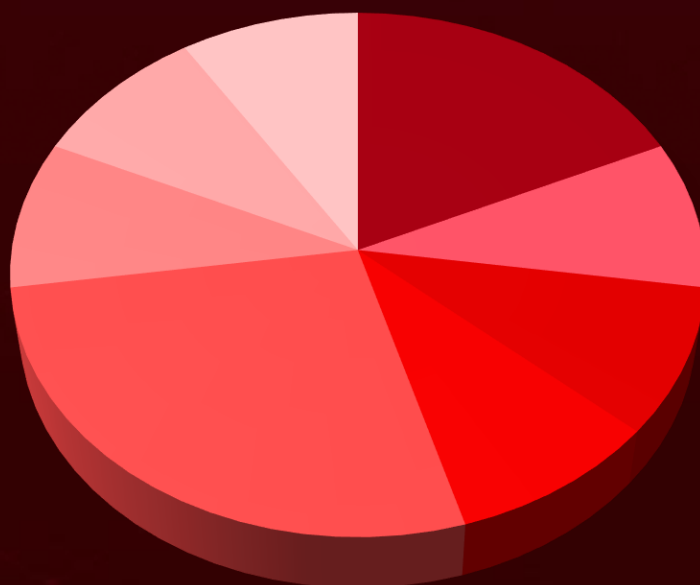
The new **Vgod ransomware** threatens Windows users with double extortion, encrypting files and stealing data to force ransom payments.

**Lumma Stealer campaign** exploits compromised educational institutions to spread malicious LNK files, stealing credentials and crypto while using Steam profiles for C2.

The **Chinese state-sponsored group Salt Typhoon** targets U.S. telecoms using JumbledPath and LOTL techniques to stealthily monitor traffic and capture sensitive data.

**CVE-2025-0108 PAN-OS** Authentication Bypass Flaw Under Active Exploitation.

## Threat Distribution



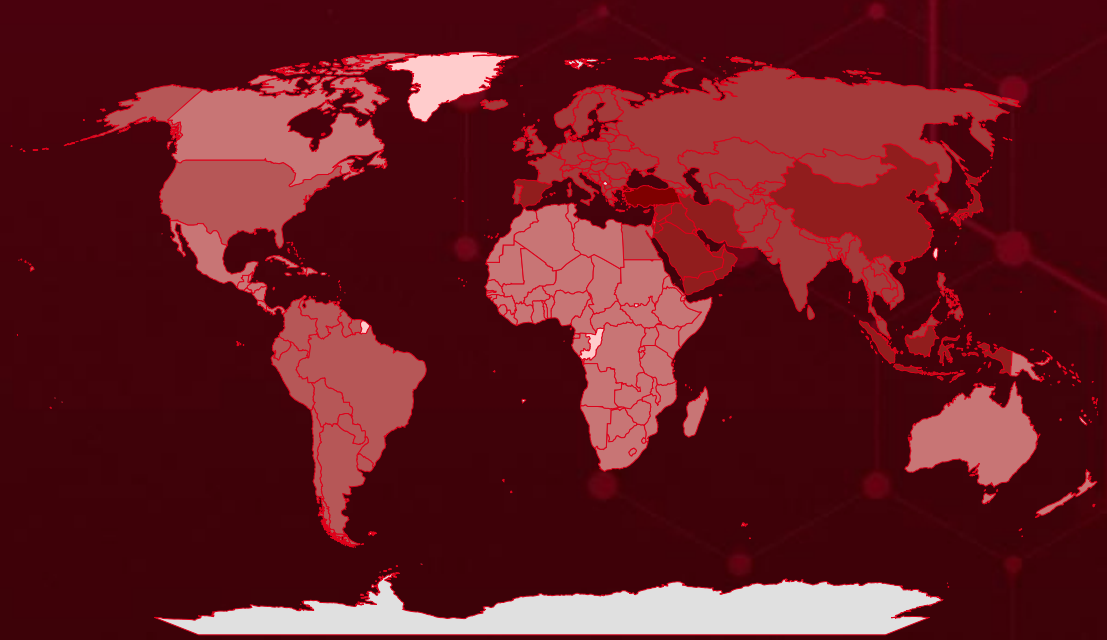
■ Backdoor   ■ Cryptominer   ■ Keylogger   ■ Loader  
■ Ransomware   ■ RAT   ■ Rootkit   ■ Stealer



# Targeted Countries

Most

Least

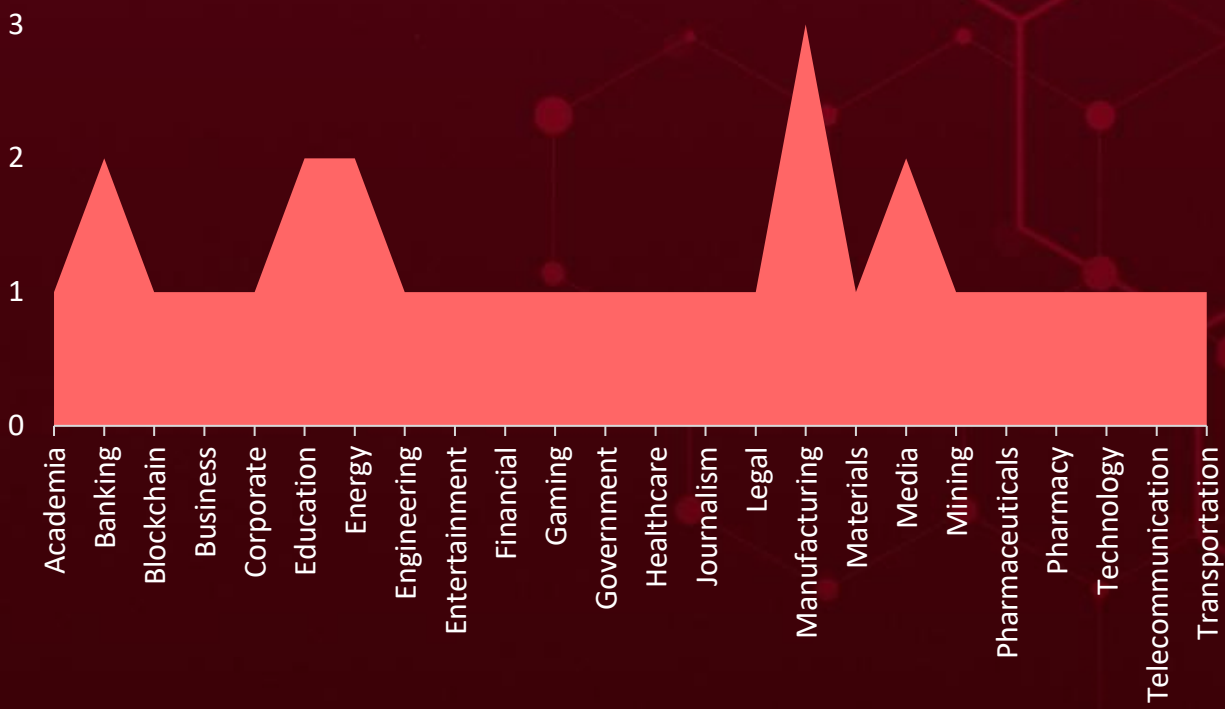


Powered by Bing

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

Countries	Countries	Countries	Countries
Turkey	United Kingdom	Hungary	Switzerland
Jordan	Bulgaria	Moldova	Lithuania
Qatar	North Korea	Iceland	Tajikistan
Lebanon	Cambodia	Mongolia	Luxembourg
China	Bangladesh	India	Timor-Leste
Bahrain	Croatia	Myanmar	Malaysia
Spain	South Korea	Ireland	Ukraine
Cyprus	Andorra	Netherlands	Bhutan
Kuwait	Thailand	Armenia	Uzbekistan
Indonesia	Czech Republic	North Macedonia	Malta
Oman	Monaco	Italy	Maldives
Iran	Denmark	Albania	State of Palestine
Saudi Arabia	Nepal	Austria	Liechtenstein
Iraq	Estonia	Philippines	Suriname
Syria	Norway	Kazakhstan	Colombia
Israel	Finland	Portugal	United States
United Arab Emirates	Poland	Azerbaijan	Suriname
Japan	France	Romania	Ecuador
Yemen	Russia	Kyrgyzstan	Venezuela
Sweden	Georgia	San Marino	Egypt
Pakistan	Slovakia	Laos	Argentina
Montenegro	Germany	Singapore	Brazil
Bosnia and Herzegovina	Sri Lanka	Latvia	Bolivia
Serbia	Greece	Slovenia	Paraguay
Brunei	Belgium	Vietnam	Uruguay
	Holy See	Belarus	Peru
	Turkmenistan	Afghanistan	Chile
			Guyana

# Targeted Industries



# TOP MITRE ATT&CK TTPs

**T1190**

Exploit Public-Facing Application

**T1059**

Command and Scripting Interpreter

**T1566**

Phishing

**T1588**

Obtain Capabilities

**T1588.006**

Vulnerabilities

**T1204**

User Execution

**T1566.001**

Spearphishing Attachment

**T1105**

Ingress Tool Transfer

**T1204.002**

Malicious File

**T1041**

Exfiltration Over C2 Channel

**T1140**

Deobfuscate/Decode Files or Information

**T1053.005**

Scheduled Task

**T1204.001**

Malicious Link

**T1068**

Exploitation for Privilege Escalation

**T1133**

External Remote Services

**T1071.001**

Web Protocols

**T1027**

Obfuscated Files or Information

**T1547**

Boot or Logon Autostart Execution

**T1036**

Masquerading

**T1588.005**

Exploits



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u><a href="#">Lumma Stealer</a></u>	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two- factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Windows
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	e15c6ecb32402f981c06f3d8c48f7e3a5a36d0810aa8c2fb8da0be053b95a8e2		
URL	hxxps[:]//80[.]76[.]51[.]231/Kompass-4[.]1[.]2[.]exe		

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>RA World ransomware</u>	RA World ransomware active since late 2023, has targeted over 20 organizations globally, primarily in manufacturing and healthcare sectors. They employ a multi-extortion strategy, exfiltrating sensitive data before encryption to pressure victims into paying ransoms. Notably, recent attacks have utilized tools associated with Chinese cyber espionage groups, suggesting possible overlaps between espionage and financially motivated activities.	Exploiting vulnerabilities	CVE-2024-0012
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption and Data Exfiltration	Palo Alto Networks PAN-OS software
Ransomware			PATCH LINK
ASSOCIATED ACTOR			<a href="https://security.paloaltonetworks.com/CVE-2024-0012">https://security.paloaltonetworks.com/CVE-2024-0012</a>
Emperor Dragonfly			
IOC TYPE	VALUE		
SHA256	2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813, 38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PlugX</u>	PlugX, a backdoor linked to China-based espionage groups like Mustang Panda, enables remote access, data exfiltration, and command execution. Recent attacks show its use alongside RA World ransomware, indicating a shift toward financially motivated cybercrimes.	Exploiting vulnerabilities	CVE-2024-0012, <u>CVE-2024-24919</u>
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data collection and Espionage	Palo Alto Networks PAN-OS, Check Point Security Gateway
ASSOCIATED ACTOR			PATCH LINK
Emperor Dragonfly			<u><a href="https://security.paloaltonetworks.com/CVE-2024-0012">https://security.paloaltonetworks.com/CVE-2024-0012</a></u> , <u><a href="https://support.checkpoint.com/results/sk/sk182336">https://support.checkpoint.com/results/sk/sk182336</a></u>
IOC TYPE	VALUE		
SHA256	8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be, b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177, 583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83, e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280, 60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797,		

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="#"><u>Vgod Ransomware</u></a>	Vgod is a newly identified ransomware variant that targets Windows systems, encrypting files and appending the ".Vgod" extension. This malware employs a double extortion tactic encrypting files while stealing sensitive data leaving victims with the grim choice of paying a ransom or risking a data leak.	Exploiting vulnerabilities	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption and Data Exfiltration	Windows
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	241c3b02a8e7d5a2b9c99574c28200df2a0f8c8bd7ba4d262e6aa8ed1211ba1f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">XMRig</a>	XMRig is an open-source cryptocurrency mining software primarily used for mining Monero (XMR). While it has legitimate uses, cybercriminals often deploy it in cryptojacking attacks, secretly using victims' computing resources to mine cryptocurrency.	Trojanized games	-
TYPE		IMPACT	AFFECTED PRODUCTS
Cryptominer		Resource drain, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e60ef7de4d1e27944469ce534b113b6d49ddd266febba5fc8d02e77a3b6d5b08		

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="#">Snake Keylogger (aka 404 Keylogger)</a>	Snake Keylogger is a stealthy malware that captures keystrokes, credentials, and other sensitive data from infected systems. Recent variants have evolved to evade detection, making it a persistent cybersecurity threat. It's actively targeting Windows users across China, Turkey, Indonesia, Taiwan, and Spain. This persistent malware has already triggered over 280 million blocked infection attempts, underscoring its widespread impact.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Windows
Keylogger			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	7e9b9833268dae6e33c83b582ec7fb353f0dc6514f869e3228f0effa161da00f		
MD5	f8410bcd14256d6d355d7076a78c074f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">Winnti RAT (aka DEPLOYLOG)</a>	Winnti RAT is a remote access Trojan used by the Winnti Group to maintain persistence and execute commands on compromised systems. It enables data exfiltration, credential theft, and lateral movement within networks. The malware is often deployed via ERP vulnerabilities or supply chain attacks, posing risks to intellectual property.	Winnti Loader	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data Theft and Data Exfiltration	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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="#">Winnti Loader (aka PRIVATELOG)</a>	Winnti Loader is a stealthy malware loader designed to execute second-stage payloads while evading detection. It uses obfuscation techniques such as encrypted logs and DLL sideloading to deploy additional malware, including backdoors and keyloggers. The loader is frequently used in targeted attacks against critical industries.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware Deployment	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	169d35bdb36c2bfcb3bbf64392de1b05d56553172a13cae43a43acbe2aa18587, b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090, 4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779, 1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">Winnti Rootkit</a>	Winnti Rootkit is an advanced persistence tool that allows attackers to hide malicious activities and maintain long-term access to infected systems. It operates at the kernel level, intercepting system calls and bypassing security mechanisms. This rootkit is primarily used in espionage campaigns targeting high-value corporate and government networks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Rootkit		Stealthy access and Persistence	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596, c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad, 569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8		




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>NailaoLocker Ransomware</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 Vulnerabilities	CVE-2024-24919
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption	Check Point Security Gateway
Ransomware			PATCH LINK
ASSOCIATED ACTOR			<a href="https://support.checkpoint.com/results/sk/sk182336">https://support.checkpoint.com/results/sk/sk182336</a>
-			
IOC TYPE	VALUE		
SHA256	7a0503da293da51a95aab0b1aa0970c8f82f04cb5149abe98fef934ba991064e, 2b069dcde43b874441f66d8888dcf6c24b451d648c8c265dfffb81c7dffafd667, 27b313243daf145c9105f5372e01f1cea74c62697195c1a21c660be5f7ee788c, a2e937d0b9d5afa5b638cd511807e0fcb44ec81b354e2cf0c406f19e5564e54e		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>ShadowPad</u>	ShadowPad is a modular backdoor malware linked to Chinese state-sponsored threat groups, used for espionage and cybercrime. It provides remote access, keylogging, data exfiltration, and the ability to deploy additional payloads like ransomware. Initially discovered in supply chain attacks, it remains a persistent threat to critical industries worldwide.	Exploiting Vulnerabilities	CVE-2024-24919
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote access and Data exfiltration	Check Point Security Gateway
Backdoor			PATCH LINK
ASSOCIATED ACTOR			<a href="https://support.checkpoint.com/results/sk/sk182336">https://support.checkpoint.com/results/sk/sk182336</a>
-			
IOC TYPE	VALUE		
SHA256	c5f8a256d0969e253633160b9728b6c2bc044f536e92af178a05a598aaa09c1f, 0a749474b5f4a8537e50ea5b60d8c94f5c688fe414cd400c3397adca4315a509, a2bb321d41b2300e80f9400950fa2125470d5b3927933ab4d6397f0cbf81532a, 697e6454d9be19f0bd60aeffa0238498a91d1ea5a23112f7c8f981afd2fedb23		

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
<u>CVE-2025-0108</u>		PAN-OS 10.1 versions earlier than 10.1.14-h9 PAN-OS 10.2 versions earlier than 10.2.13-h3 PAN-OS 11.1 versions earlier than 11.1.6-h1 PAN-OS 11.2 versions earlier than 11.2.4-h4 PAN-OS 11.0 (EOL)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<a href="https://security.paloaltonetworks.com/CVE-2025-0108">https://security.paloaltonetworks.com/CVE-2025-0108</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2025-1094</a>		PostgreSQL Versions Before 17.3, 16.7, 15.11, 14.16, and 13.19	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:postgresql:postgresql:*:*:*:*:*	-
PostgreSQL psq SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-149	T1059: Command and Scripting Interpreter	<a href="https://www.postgresql.org/support/security/CVE-2025-1094/">https://www.postgresql.org/support/security/CVE-2025-1094/</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-12356</a>		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	<a href="https://www.beyondtrust.com/trust-center/security-advisories/bt24-10">https://www.beyondtrust.com/trust-center/security-advisories/bt24-10</a>









CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-12686</u>		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	<a href="https://www.beyondtrust.com/trust-center/security-advisories/bt24-11">https://www.beyondtrust.com/trust-center/security-advisories/bt24-11</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-0012</u>		Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2	Emperor Dragonfly
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*	RA World ransomware, PlugX
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1556: Modify Authentication Process	<a href="https://security.paloaltonetworks.com/CVE-2024-0012">https://security.paloaltonetworks.com/CVE-2024-0012</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-26465</u>		OpenSSH versions 6.8p1 to 9.9p1, Red Hat, SUSE, Debian, Fedora, ALT Linux, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openssh:openssh:*.~*~*~*~*~*~*	-
OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-390	T1203: Exploitation for Client Execution T1656: Impersonation	<a href="https://security-tracker.debian.org/tracker/CVE-2025-26465">https://security-tracker.debian.org/tracker/CVE-2025-26465</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-0171</u>		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\~*~*~*~*~*~*	-
Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20 CWE-787	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-20198</u>		Cisco IOS XE- All versions	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-269	T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-20273</u>		Cisco IOS XE- All versions	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-20 CWE-787	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-24919</u>		Check Point Security Gateway	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:checkpoint:quantum_gateway:*:*:*:*:*.*	NailaoLocker Ransomware, Shadowpad, PlugX
Check Point Security Gateway Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1133: External Remote Services, T1212: Exploitation for Credential Access	<a href="https://support.checkpoint.com/results/sk/sk182336">https://support.checkpoint.com/results/sk/sk182336</a>




# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><a href="#">Silk Typhoon (aka Hafnium, Red Dev 13, ATK233, G0125)</a></div>	China	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACK S/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-12356 CVE-2024-12686	-	-
TTPs			
TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1588.005: Exploits, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1133: External Remote Services			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
  <u>Emperor Dragonfly</u> <u>(aka Bronze Starlight,</u> <u>DEV-0401, Cinnamon</u> <u>Tempest,</u> <u>SLIME34, SLIME34)</u>	China	Government banks, think tanks, embassies, legal entities	Europe, Asia
	<b>MOTIVE</b>  Espionage and Financial Gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-0012	RA World ransomware (aka RA Group ransomware), PlugX	Palo Alto Networks PAN-OS software
<b>TTPs</b>			
TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, TA0006: Credential Access, TA0009: Collection, T1083: File and Directory Discovery, T1490: Inhibit System: Recovery, T1552: Unsecured Credentials, T1560: Archive Collected Data, T1573: Encrypted Channel, T1496: Resource Hijacking, T1203: Exploitation for Client Execution, T1055.001: Dynamic-link Library Injection, T1055: Process Injection, T1105: Ingress Tool Transfer, T1555: Credentials from Password Stores, T1027: Obfuscated Files or Information, T1036: Masquerading, T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Winnti Group (aka APT 41, Blackfly, Wicked Panda)</u></p>	Iran	Manufacturing, Materials, Energy	Japan
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	Winnti RAT (aka DEPLOYLOG), Winnti Loader (also known as PRIVATELOG), Winnti Rootkit	Windows
<b>TTPs</b>			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1505: Server Software: Component, T1505.003: Web Shell, T1574: Hijack Execution Flow, T1574.001: DLL Search Order Hijacking, T1547: Boot or Logon Autostart Execution, T1547.006: Kernel Modules and Extensions, T1543: Create or Modify System Process, T1543.003: Windows Service, T1078: Valid Accounts, T1078.002: Domain Accounts, T1014: Rootkit: T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1070: Indicator Removal, T1070.004: File Deletion, T1016: System Network Configuration Discovery, T1018: Remote System Discovery, T1201: Password Policy Discovery, T1069: Permission Groups Discovery, T1135: Network Share Discovery, T1007: System Service Discovery, T1049: System Network Connections Discovery, T1033: System Owner/User Discovery, T1082: System Information Discovery, T1120: Peripheral Device Discovery, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1588.004: Digital Certificates			



NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Salt Typhoon (aka GhostEmperor, UNC2286, FamousSparrow, Earth Estries, RedMike)</u></p>	China	Telecommunication	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2018-0171 CVE-2023-20198 CVE-2023-20273	-	-
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0010: Exfiltration, TA0011: Command and Control, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1555: Credentials from Password Stores, T1555.003: Credentials from Web Browsers, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1600: Weaken Encryption, T1027: Obfuscated Files or Information, T1556: Modify Authentication Process, T1016: System Network Configuration Discovery, T1222: File and Directory Permissions Modification, T1190: Exploit Public-Facing Application, T1021: Remote Services, T1021.004: SSH, T1068: Exploitation for Privilege Escalation, T1584: Compromise Infrastructure, T1105: Ingress Tool Transfer			

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eleven exploited vulnerabilities** and block the indicators related to the threat actors **Silk Typhoon, Emperor Dragonfly, Winnti Group, Salt Typhoon**, and malware **Lumma Stealer, RA World, PlugX, Vgod, XMRig, Snake Keylogger, Winnti RAT, Winnti Loader, Winnti Rootkit, NailaoLocker, Shadowpad**.

## 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 **eleven exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Emperor Dragonfly, Winnti Group, Salt Typhoon**, and malware **Lumma Stealer, PlugX, Vgod, XMRig, Snake Keylogger, Winnti Loader, Winnti Rootkit, NailaoLocker, Shadowpad** in Breach and Attack Simulation(BAS).

# Threat Advisories

[CVE-2025-0108: PAN-OS Authentication Bypass Flaw Under Active Exploitation](#)

[PostgreSQL Flaw CVE-2025-1094 Joins BeyondTrust Zero-Day in Stealthy Attacks](#)

[Go-Based Backdoor Exploits Telegram for Covert Command Execution](#)

[Malware-as-a-Service in Action: Lumma Stealer's Expanding Attack Methods](#)

[Chinese Hackers Turn to RA World Ransomware for Profit](#)

[The High-Stakes Game of Vgod Ransomware](#)

[StaryDobry Campaign: Trojanized Games Fuel a Global Cybercrime Wave](#)

[Is Your Server Safe? New OpenSSH Vulnerabilities Exposed](#)

[Snake Keylogger Strikes Again: A Stealthy Threat Targeting Millions](#)

[RevivalStone A New Wave of Winnti Group's Cyber Attacks Hits Japan](#)

[Salt Typhoon's Covert Campaign: Targeting U.S. Telecom Networks](#)

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

# 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>Lumma Stealer</u>	SHA256	e15c6ecb32402f981c06f3d8c48f7e3a5a36d0810aa8c2fb8da0be053b95a8e2
	URL	hxtps[:]//80[.]76[.]51[.]231/Kompass-4[.]1[.]2[.]exe,
<u>RA World (aka RA Group ransomware)</u>	SHA256	2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813, 38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25
<u>PlugX</u>	Domain	police[.]tracksyscloud[.]com, caco[.]blueskyanalytics[.]net
	IPv4	154[.]223[.]18[.]123, 23[.]227[.]203[.]181
	SHA256	8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be, b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177, 583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83, e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280, 60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797, eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afb234a33f13, 16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe, 5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914, 70cd979cc17a89856c2a6acccb32964c01c208cb232cbd9e782d2baab00c36e4

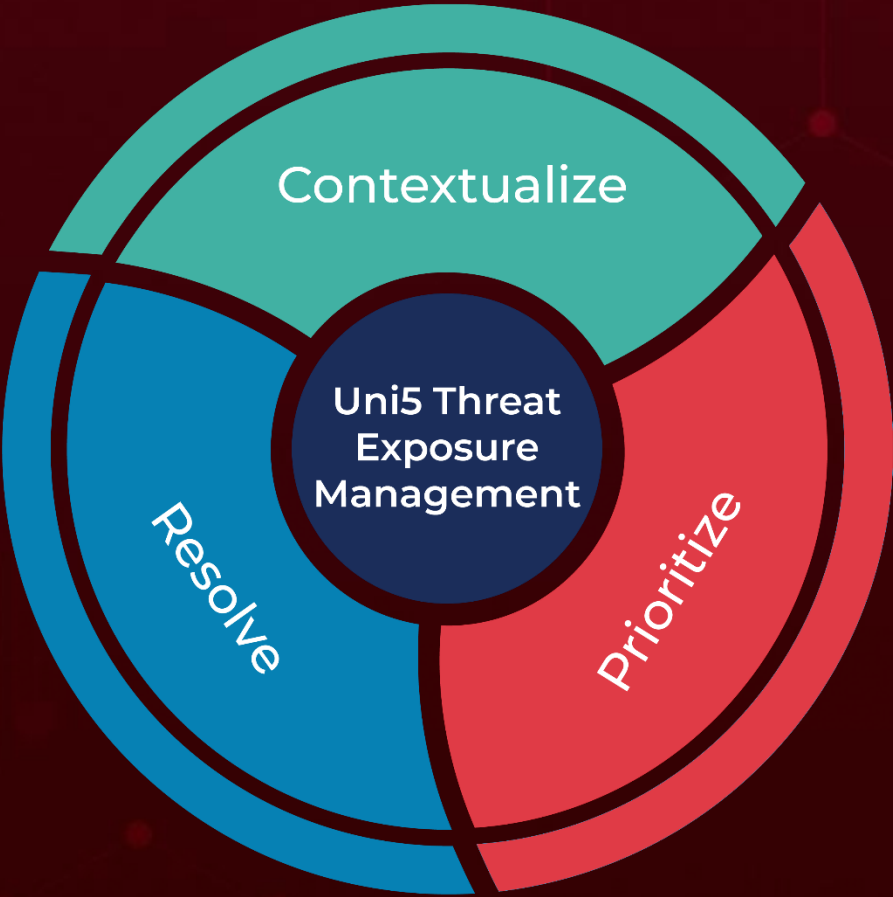
Attack Name	TYPE	VALUE
<u>Vgod</u>	SHA256	241c3b02a8e7d5a2b9c99574c28200df2a0f8c8bd7ba4d262e6aa8ed1211ba1f
<u>XMRig</u>	SHA256	e60ef7de4d1e27944469ce534b113b6d49ddd266febbba5fc8d02e77a3b6d5b08
<u>Snake Keylogger</u>	MD5	f8410bcd14256d6d355d7076a78c074f, f8410bcd14256d6d355d7076a78c074f
	SHA256	7e9b9833268dae6e33c83b582ec7fb353f0dc6514f869e3228f0effa161da00f
<u>Winnti Loader</u> (also known as <u>PRIVATELOG</u> )	SHA256	169d35bdb36c2bfc3bbf64392de1b05d56553172a13cae43a43acbe2aa18587, b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090, 4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779, 1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c
<u>Winnti Rootkit</u>	SHA256	e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596, c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad, 569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8
<u>NailaoLocker</u>	SHA256	7a0503da293da51a95aab0b1aa0970c8f82f04cb5149abe98fef934ba991064e, 2b069dcde43b874441f66d8888dcf6c24b451d648c8c265dfffb81c7dfafad667, 27b313243daf145c9105f5372e01f1cea74c62697195c1a21c660be5f7ee788c, a2e937d0b9d5afa5b638cd511807e0fcb44ec81b354e2cf0c406f19e5564e54e
<u>Shadowpad</u>	URL	hxxps[:]//dscry[.]chtq[.]net
	IPv4	193[.]56[.]255[.]214, 158[.]247[.]199[.]185, 104[.]238[.]135[.]232, 139[.]84[.]137[.]63, 141[.]164[.]35[.]65, 176[.]222[.]55[.]131, 193[.]56[.]255[.]214, 37[.]120[.]239[.]33, 45[.]76[.]209[.]205, 45[.]77[.]153[.]108, 45[.]77[.]170[.]188, 47[.]242[.]0[.]122, 52[.]194[.]253[.]134,

Attack Name	TYPE	VALUE
<u>Shadowpad</u>	IPv4	64[.]176[.]226[.]182, 64[.]176[.]59[.]232, 64[.]176[.]65[.]49, 8[.]210[.]30[.]189, 8[.]218[.]244[.]117
	SHA256	c5f8a256d0969e253633160b9728b6c2bc044f536e92af178a05a598 aaa09c1f, 0a749474b5f4a8537e50ea5b60d8c94f5c688fe414cd400c3397adca4 315a509, a2bb321d41b2300e80f9400950fa2125470d5b3927933ab4d6397f0c bf81532a, 697e6454d9be19f0bd60aeffa0238498a91d1ea5a23112f7c8f981afd 2fedb23

# 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  
**February 24, 2025 • 9:45 PM**

© 2025 All Rights are Reserved by Hive Pro



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