

Date of Publication
August 25, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors
18 to 24 AUGUST 2025

Table Of Contents

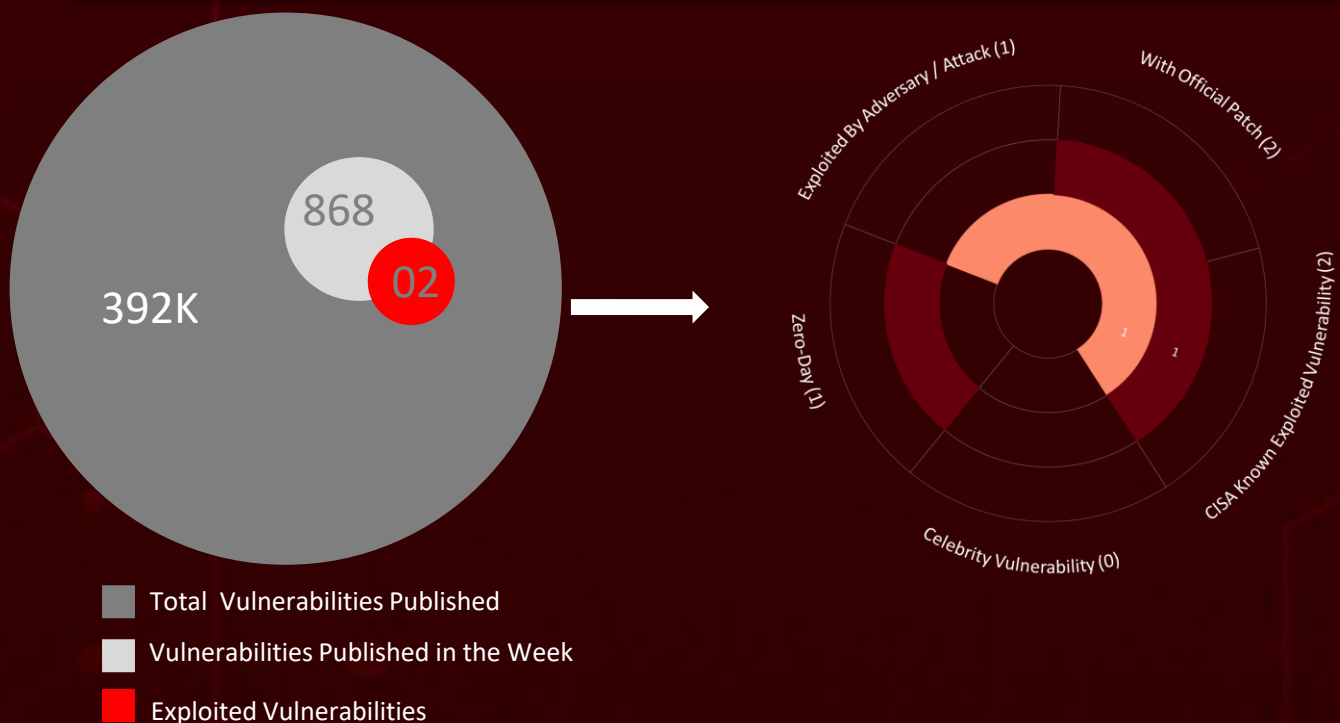
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	20

Summary

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

Among the most concerning findings was **CVE-2025-43300**, a zero-day flaw in Apple's Image I/O framework that enables remote code execution through a maliciously crafted image file, requiring little to no user interaction. Another active exploit tracked was **CVE-2018-0171**, a long-standing vulnerability in Cisco IOS Smart Install, abused by **Static Tundra**, a Russian state-backed espionage group, to extract device configurations and sensitive credentials, an example of how older flaws remain valuable tools in state-driven operations.

Adding to the complexity, the **Crypto24** ransomware family has rapidly matured since late 2024, expanding into a global threat against critical industries across Asia, Europe, and the U.S. Its operators blend legitimate IT tools with custom-built malware to maximize disruption and evade detection. At the same time, the **GodRAT** campaign demonstrates how legacy malware families like Gh0st RAT continue to resurface in new forms. GodRAT blends stealth, modular functionality, and data theft into an attack chain tailored for industries like finance. Together, these developments illustrate a mounting wave of cyber aggression, underscoring the urgent need for resilience, proactive defense, and swift patch management in the face of evolving digital threats.



High Level Statistics

7

Attacks
Executed

2

Vulnerabilities
Exploited

1

Adversaries in
Action

- [PS1Bot](#)
 - [Noodlophile](#)
 - [GodRAT](#)
 - [AsyncRAT](#)
 - [Crypto24](#)
 - [SYNful Knock](#)
 - [QuirkyLoader](#)
- [CVE-2018-0171](#)
 - [CVE-2025-43300](#)
- [Static Tundra](#)



Insights

PS1Bot strikes with a multi-stage PowerShell and C# framework, armed with a stealer module built to plunder passwords and crypto secrets.

GodRAT, built on the Gh0st RAT codebase, stands out for its stealthy twist, using steganography to hide shellcode in plain sight.

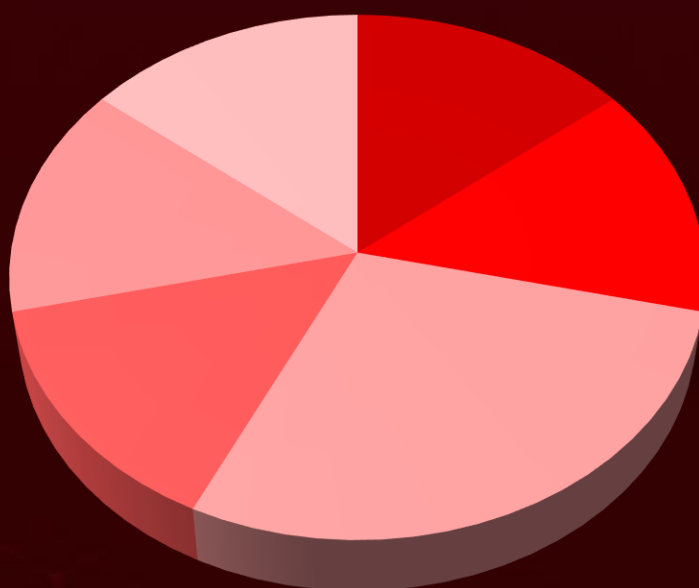
CVE-2025-43300: A critical Apple Image I/O zero-day that turns a simple image file into a silent doorway for remote code execution.

Static Tundra, a Russian state-backed espionage group, is notorious for hijacking unpatched Cisco devices with advanced implants and custom-built tools.

Crypto24 ransomware is a carefully crafted, multi-stage operation that mixes admin tools with custom malware to silently infiltrate networks, spread laterally, and evade detection.

QuirkyLoader spreads through phishing archives, using DLL side-loading and process hollowing to stealthily inject encrypted payloads into trusted Windows processes.

Threat Distribution



■ Framework ■ Stealer ■ RAT ■ Ransomware ■ Backdoor ■ Loader

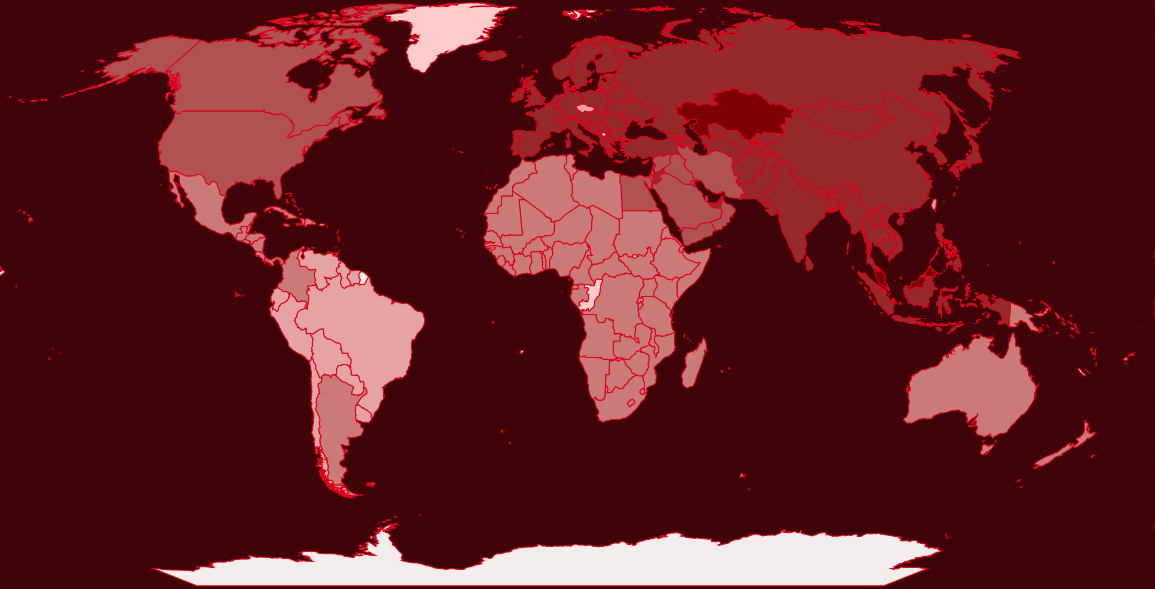


Targeted Countries

Most



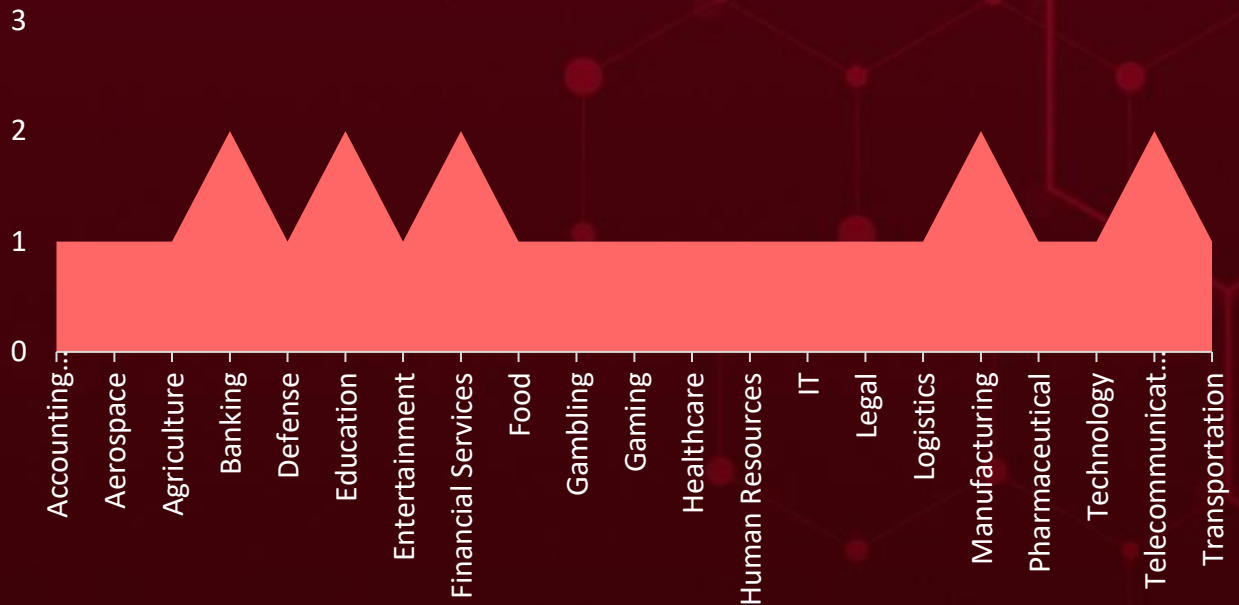
Least



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

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

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1574.001

DLL

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1574

Hijack Execution Flow

T1071.001

Web Protocols

T1082

System Information Discovery

T1547

Boot or Logon Autostart Execution

T1566

Phishing

T1555

Credentials from Password Stores

T1056.001

Keylogging

T1204

User Execution

T1036

Masquerading

T1547.001

Registry Run Keys / Startup Folder

T1083

File and Directory Discovery

T1555.003

Credentials from Web Browsers

T1105

Ingress Tool Transfer

T1056

Input Capture

T1059.003

Windows Command Shell

T1588

Obtain Capabilities

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PS1Bot	PS1Bot is a multi-stage malware framework built in PowerShell and C# that operates with a modular design, allowing attackers to load different components as needed. These modules enable a wide range of malicious activities, from stealing sensitive information and logging keystrokes to conducting reconnaissance and maintaining long-term access on compromised machines. What makes PS1Bot particularly dangerous is its focus on stealth, it avoids leaving obvious traces on infected systems and relies heavily on in-memory execution, ensuring that follow-on payloads can run without ever being written to disk.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, Persistence	-
Framework			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	809f4ffef71ab43d692d4fececf1dfefffb0854ae1f15486960b1c198c47c69f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Noodlophile	Noodlophile Stealer is a powerful data-harvesting malware designed to aggressively target browser-based information and sensitive system details. Once active, it siphons credentials, cookies, credit card data, system metadata, and even security configurations from multiple browsers, giving attackers deep access to a victim's digital footprint. To strengthen its stealth, the stealer sometimes deploys a .NET executable that disables monitoring mechanisms and security defenses.	Spear phishing emails	-
		IMPACT	AFFECTED PRODUCT
TYPE		Steal Data	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	8773071c5a06eafa8b6a4dc102422583c0fe18890667b9fff53f5d5e78991d81		

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>GodRAT</u>	<p>GodRAT is a newly uncovered Remote Access Trojan (RAT) built on the Gh0st RAT codebase. To avoid detection, its operators cleverly used steganography to hide malicious shellcode inside image files, which then retrieved the GodRAT payload from a Command-and-Control (C2) server. Once deployed, GodRAT can be extended with plugins, such as a FileManager module that lets attackers browse, modify, and control files on the victim’s system. Sharing striking similarities with AwesomePuppet, a Gh0st RAT-based backdoor, GodRAT appears to be its evolutionary successor, carrying forward the same core design while adopting new tactics to stay effective in today’s threat landscape.</p>	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	0E2889F6475AEA625D18B200A2CACDAC745ECB22044F6366F21AFC2E24046025, C52FB4EDDF64779B7BEDA43D26618251EEFE84BBB7F1C8EBB725E5E2DFDCFE4A		
IPv4	103[.]237[.]92[.]191		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>AsyncRAT</u>	<p>AsyncRAT is a publicly available remote access trojan (RAT) on GitHub. A modified version ensures persistence by creating a scheduled task that triggers at startup. Upon activation, a complex sequence initiates AsyncRAT within Windows Sandbox, which must be manually enabled and requires a reboot.</p>	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Remote Control, Information Theft	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	ED1DFD2E913E1C53D9F9AB5B418F84E0F401ABFDF8E3349E1FCFC98663DCB23F		

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>Crypto24</u>	Crypto24 ransomware, first observed in late 2024, has quickly risen as a significant global cyber threat. The operators behind it plan their campaigns with precision, often launching attacks during off-peak hours to slip past defenses and cause maximum disruption. Their arsenal combines legitimate tools with custom malware, enabling them to infiltrate networks, move laterally, and evade detection. Tactics include using PSEXEC for internal propagation, AnyDesk for persistent remote access, keyloggers to steal credentials, and multiple backdoors to maintain control.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft, Encrypt Data, System Compromise	Windows
Ransomware			PATCH LINK
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	10c3317566f52eaeb45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SYNful Knock</u>	SYNful Knock is a stealthy modular backdoor implant that attackers insert into a modified Cisco IOS image and deploy onto compromised network devices. Once installed, it grants persistent access that survives reboots, allowing adversaries to maintain long-term control while remaining difficult to detect.	Exploiting Vulnerability	CVE-2018-0171
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	Cisco IOS and IOS XE Software
Backdoor			PATCH LINK
ASSOCIATED ACTOR			
Static Tundra			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

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>QuirkyLoader</u>	QuirkyLoader is a stealthy malware loader distributed primarily through phishing emails containing malicious archive files. When executed, it leverages techniques like DLL side-loading and process hollowing to covertly inject encrypted payloads into legitimate Windows processes, enabling the delivery of information stealers and remote access trojans (RATs). QuirkyLoader particularly distinctive is its DLL module, developed in C#.NET with Ahead-of-Time (AOT) compilation. This approach first converts C# code into Microsoft Intermediate Language (MSIL) before compiling it into native machine code, giving the loader both efficiency and an added layer of complexity that hinders detection and analysis.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Loads other Payloads	-
Loader			PATCH LINK
ASSOCIATED ACTOR			
-	-		
IOC TYPE	VALUE		
SHA256	011257eb766f2539828bdd45f8aa4ce3c4048ac2699d988329783290a7b4a0d3, 0ea3a55141405ee0e2dfbf333de01fe93c12cf34555550e4f7bb3fdec2a7673b, a64a99b8451038f2bbcd322fd729edf5e6ae0eb70a244e342b2f8eff12219d03		

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-2018-0171</u>		Cisco IOS and IOS XE Software	Static Tundra
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:cisco:ios:15.2\ (5\) e:*.~*.~*.~*.~*~*	SYNful Knock
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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-43300</u>		macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://support.apple.com/en-us/124925 , https://support.apple.com/en-us/124926 , https://support.apple.com/en-us/124927 , https://support.apple.com/en-us/124928 , https://support.apple.com/en-us/124929

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Static Tundra</u>	Russia	Telecommunications, Higher Education, Manufacturing	North America, Asia, Africa, Europe
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2018-0171	SYNful Knock	Cisco IOS and 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; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1601: Modify System Image; T1596: Search Open Technical Databases; T1596.005: Scan Databases; T1543: Create or Modify System Process; T1210: Exploitation of Remote Services; T1587: Develop Capabilities; T1587.004: Exploits; T1018: Remote System Discovery; T1046: Network Service Discovery; T1040: Network Sniffing; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1542.005: TFTP Boot; T1068: Exploitation for Privilege Escalation; T1543.003: Windows Service; T1036: Masquerading; T1105: Ingress Tool Transfer; T1601.002: Downgrade System Image; T1552.001: Credentials In Files; T1016: System Network Configuration Discovery; T1602.002: Network Device Configuration Dump; T1059: Command and Scripting Interpreter; T1571: Non-Standard Port; T1048: Exfiltration Over Alternative Protocol			

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 actor **Static Tundra**, and malware **PS1Bot, Noodlophile Stealer, GodRAT, AsyncRAT, Crypto24 Ransomware, SYNful Knock, QuirkyLoader**.

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 actor **Static Tundra**, and malware **PS1Bot, GodRAT, Crypto24 Ransomware, QuirkyLoader** in Breach and Attack Simulation(BAS).

Threat Advisories

[PS1Bot: The Modular Malware Lurking Behind Malvertising](#)

[Noodlophile Stealer Advances with Obfuscation, Social Media Deception](#)

[GodRAT Reloaded: Legacy Code, Modern Tactics](#)

[Crypto24 Ransomware Disrupts Businesses Using Custom EDR Bypass](#)

[Static Tundra Fuels Espionage Campaigns Through an Old Cisco Bug](#)

[CVE-2025-43300: Zero-Day in Apple Image I/O Exploited in Targeted Attacks](#)

[QuirkyLoader: A Silent Enabler of Modern Malware Families](#)

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>PS1Bot</u>	SHA256	809f4ffef71ab43d692d4fececf1dfefffb0854ae1f15486960b1c198c47c69f
<u>Noodlophile</u>	SHA256	8773071c5a06eafa8b6a4dc102422583c0fe18890667b9fff53f5d5e78991d81, 4b7d98e3bf3b6c1c20e735e21b8f98c15f2ed032ce1a54a09de b303d22bebac5, 6082396e63f134eed71fb16e30e975cc43810c0b091cd038796 6df934d88fcd0, ac358f3465c63f41eea6539a42fd4ee8b32ca63cbb52ec3de7df 303314543f30, 0009e715036493ca4bada2c99287654f57e66173c10c6aae424 d1cce16f0dd51, 11c873cee11fd1d183351c9cdf233cf9b29e28f5e71267c2cb1f3 73a564c6a73
<u>GodRAT</u>	MD5	d09fd377d8566b9d7a5880649a0192b4, e723258b75fee6fbd8095f0a2ae7e53c, 318f5bf9894ac424fd4faf4ba857155e, 512778f0de31fcce281d87f00affa4a8, 6cad01ca86e8cd5339ff1e8fff4c8558, 58f54b88f2009864db7e7a5d1610d27d, 64dfcdd8f511f4c71d19f5a58139f2c0, 8008375eec7550d6d8e0eaf24389cf81, 04bf56c6491c5a455efea7dbf94145f1, 5f7087039cb42090003cc9dbb493215e

Attack Name	TYPE	VALUE
<u>GodRAT</u>	SHA256	0E2889F6475AEA625D18B200A2CACDAC745ECB22044F6366F21AFC2E24046025, C52FB4EDDF64779B7BEDA43D26618251EEFE84BBB7F1C8EBB725E5E2DFDCFE4A, 2E33A3C604C4212547BDBB31BD842B365EF28EB7B9A84564FB8EF3C0268F6268, 51B7478388593F90516D04053B95DD0861D93D6195341B36272D2474D196BA86, CED343EE088F8FDDAF74D3B85C0D9176A3DB852E580467CA6C60EC86BD5E2132, 67C713A44186315D7CBFEC4745B7DD199D86711F48C5F0778A71871AC3B02624, B673444DAF876EEFF6AA81BFCD86F68FA7E5C4C48EFFF183D94EDFBB57D93EF5
	IPV4	103[.]237[.]92[.]191, 118[.]99[.]3[.]33, 118[.]107[.]46[.]174, 154[.]91[.]183[.]174
<u>AsyncRAT</u>	MD5	605f25606bb925d61ccc47f0150db674, 961188d6903866496c954f03ecff2a72, 4ecd2cf02bdf19cdbcb5507e85a32c657, 17e71cd415272a6469386f95366d3b64
	SHA256	ED1DFD2E913E1C53D9F9AB5B418F84E0F401ABFDF8E3349E1FCFC98663DCB23F, C5F5D5A9BA824E235ABD02E9D09052CA8A17B8C18253C7B25727A17DF675E66B, 8A1A19741DC3626CFF78E1C54DE827058060A42F3ACADDF6D5C3DEBE7071185B
	Domain	wuwu6[.]cfd
	IPv4	156[.]241[.]134[.]49, 47[.]238[.]124[.]68
<u>Crypto24 Ransomware</u>	SHA256	10c3317566f52eae45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b, 0e36b1837e5a2cbd14fac2c3b709a5470b7b488bd15898d30840ec60448e83e0, 3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac, 686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac, 24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73

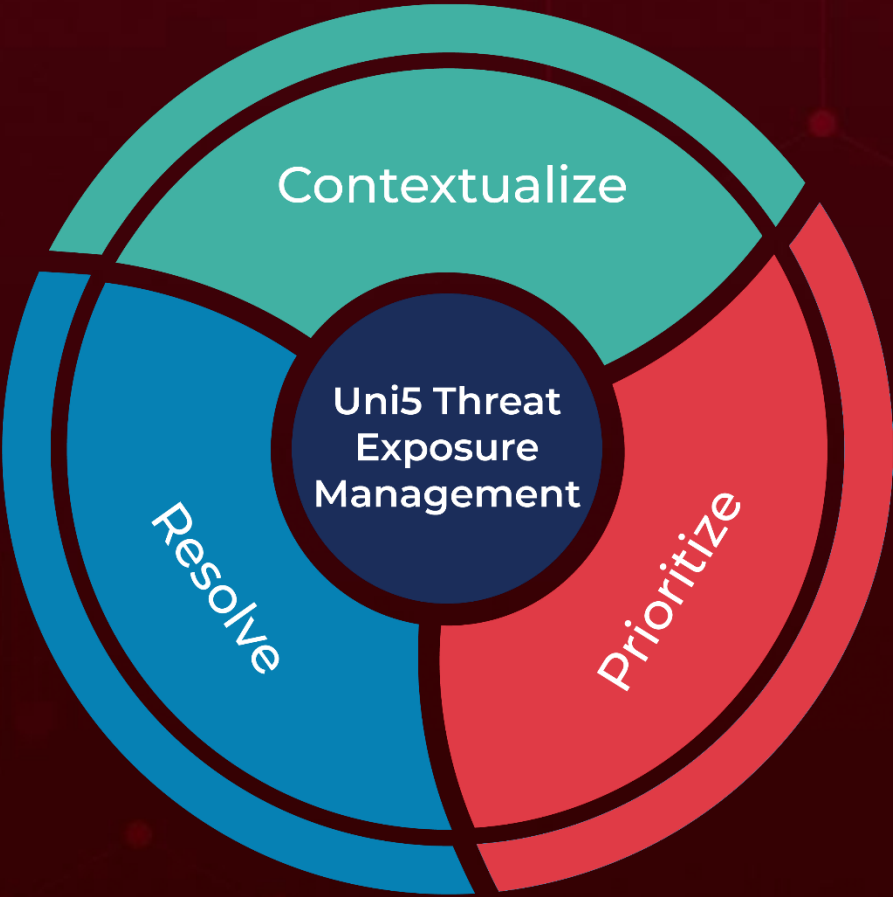
Attack Name	TYPE	VALUE
<u>QuirkyLoader</u>	SHA256	011257eb766f2539828bdd45f8aa4ce3c4048ac2699d988329783290a7b4a0d3, 0ea3a55141405ee0e2dfbf333de01fe93c12cf34555550e4f7bb3fdec2a7673b, a64a99b8451038f2bbcd322fd729edf5e6ae0eb70a244e342b2f8eff12219d03, 9726e5c7f9800b36b671b064e89784fb10465210198fbbb75816224e85bd1306, a1994ba84e255eb02a6140cab9fc4dd9a6371a84b1dd631bd649525ac247c111, d954b235bde6ad02451cab6ee1138790eea569cf8fd0b95de9dc505957c533cd, 5d5b3e3b78aa25664fb2bfdbf061fc1190310f5046d969adab3e7565978b96ff, 6f53c1780b92f3d5affcf095ae0ad803974de6687a4938a2e1c9133bf1081eb6, ea65cf2d5634a81f37d3241a77f9cd319e45c1b13ffbaf5f8a637b34141292eb, 1b8c6d3268a5706fb41ddfff99c8579ef029333057b911bb4905e24aacc05460, d0a3a1ee914bcbfcf709d367417f8c85bd0a22d8ede0829a66e5be34e5e53bb9, b22d878395ac2f2d927b78b16c9f5e9b98e006d6357c98dbe04b3fd78633ddde, a83aa955608e9463f272adca205c9e1a7cbe9d1ced1e10c9d517b4d1177366f6, 3391b0f865f4c13dcd9f08c6d3e3be844e89fa3afbcd95b5d1a1c5abcacf41f4, b2fdf10bd28c781ca354475be6db40b8834f33d395f7b5850be43ccace722c13, bf3093f7453e4d0290511ea6a036cd3a66f456cd4a85b7ec8fbf ea6b9c548504, 97aee6ca1bc79064d21e1eb7b86e497adb7ece6376f355e47b2ac60f366e843d, b42bc8b2aeec39f25babdcbbdaab806c339e4397debfd2ff1b69dca5081eb44, 5aaf02e4348dc6e962ec54d5d31095f055bd7fb1e58317682003552fd6fe25dc, 8e0770383c03ce69210798799d543b10de088bac147dce4703f13f79620b68b1, 049ef50ec0fac1b99857a6d2beb8134be67ae67ae134f9a3c53699cdaa7c89ac, cba8bb455d577314959602eb15edcaa34d0b164e2ef9d89b08733ed64381c6e0
	IPv4	103[.]75[.]77[.]90,161[.]248[.]178[.]212

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
August 25, 2025 • 6:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com