

Date of Publication
June 16, 2025



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

9 to 15 JUNE 2025

Table Of Contents

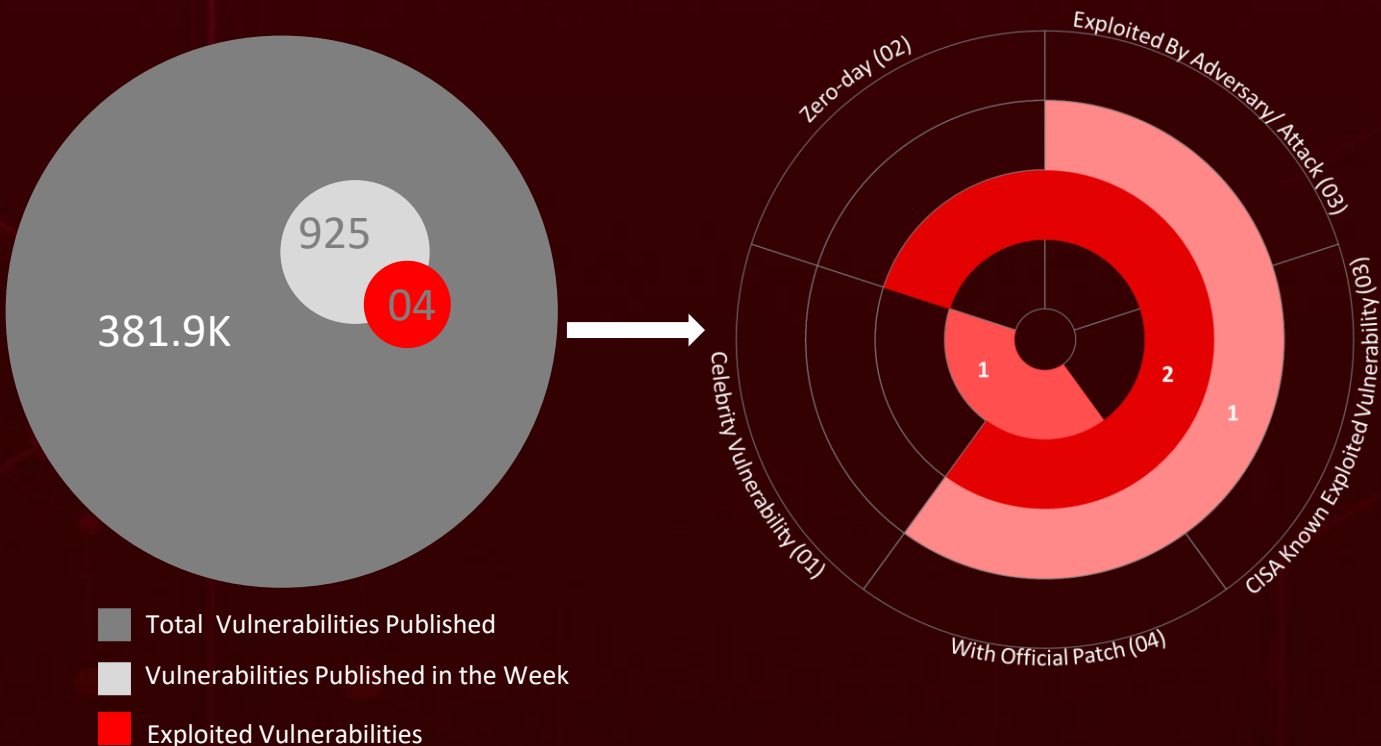
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	15
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	25

Summary

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

Among the notable incidents, **Blitz** is a Windows-based malware distributed via fake **Standoff 2 game cheats** on Telegram. Separately, **Stealth Falcon**, a long-running cyber-espionage group, exploited a zero-day vulnerability in Windows (**CVE-2025-33053**) to breach a Turkish defense contractor.

North Korea-linked **APT37** launched **Operation ToyBox Story**, a spear-phishing campaign using fileless malware and sophisticated social engineering to compromise strategic targets within South Korea. Meanwhile, cybercriminals have been hijacking expired or deleted **Discord invite links**, redirecting users to fake servers where disguised "verification" prompts install malware. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



High Level Statistics

14

Attacks
Executed

4

Vulnerabilities
Exploited

3

Adversaries in
Action

- [Blitz](#)
- [XMRig](#)
- [Atomic Stealer](#)
- [VELETRIX](#)
- [VShell](#)
- [Myth Stealer](#)
- [Horus Agent](#)
- [Horus Loader](#)
- [RoKRAT](#)
- [AsyncRAT](#)
- [Skuld Stealer](#)
- [Mirai](#)
- [Resbot](#)
- [Fog ransomware](#)

- [CVE-2025-33053](#)
- [CVE-2025-32711](#)
- [CVE-2022-41128](#)
- [CVE-2025-24016](#)

- [sw1zzx](#)
- [Stealth Falcon](#)
- [APT37](#)



Insights

Mirai Reloaded:

CVE-2025-24016

Under Active
Exploitation

Fog Ransomware Strikes

Asian Bank: Two Weeks of Silent
Intrusion Before Devastation

Gamers Beware:

Myth Stealer
Malware Disguised
as Game Cheats

Blitz Malware Exploits
Hugging Face to Launch
Cryptomining, Keylogging Attacks

Operation DRAGONCLONE

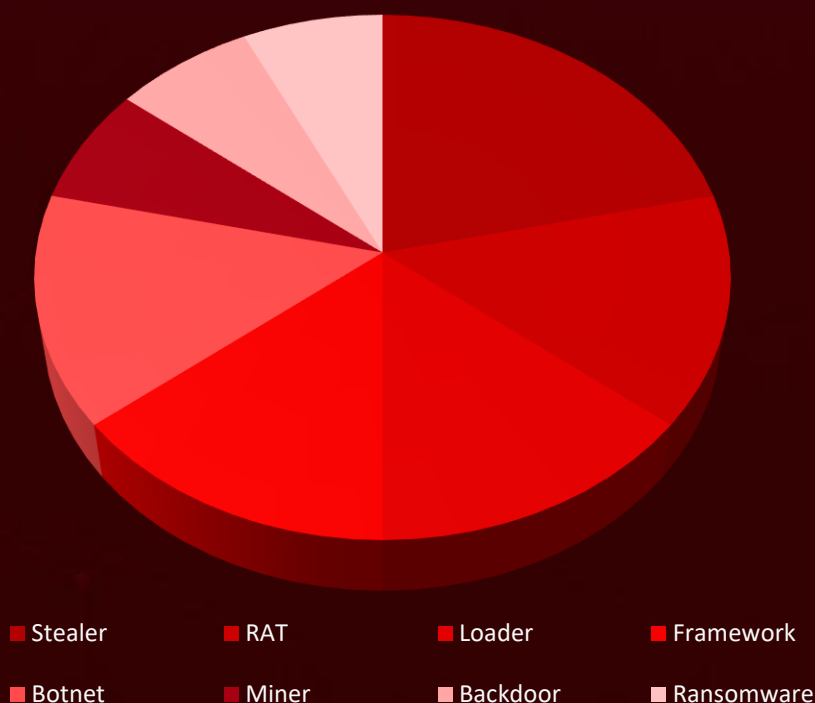
Exploits Trusted Platforms for Silent
Intrusion

Zero-Click and Zero-Day

Vulnerabilities
Headline

Microsoft's June
2025 Patches

Threat Distribution



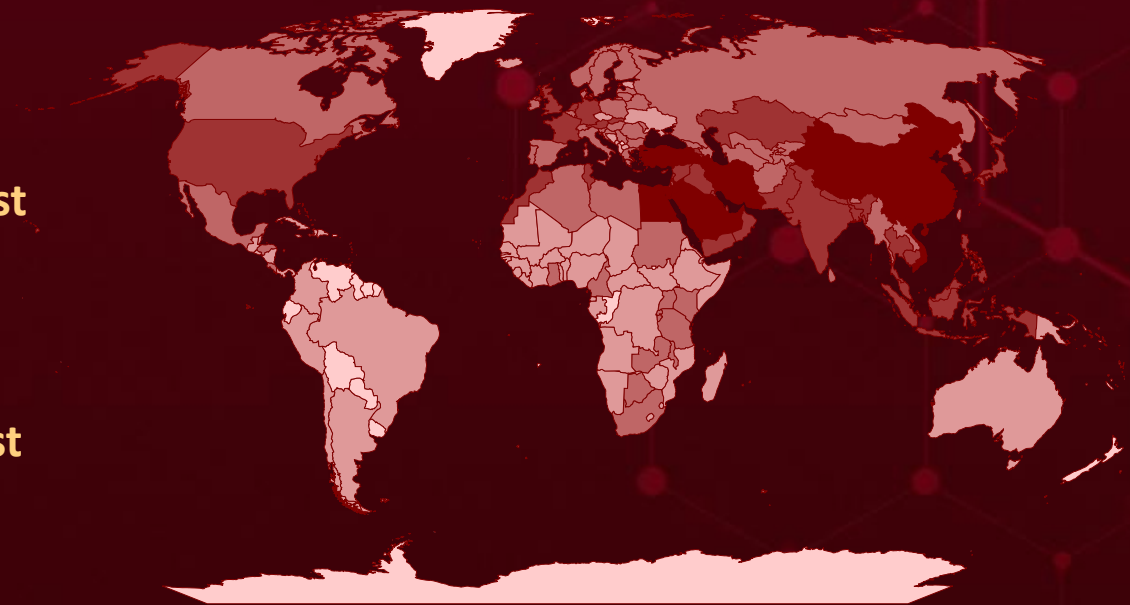


Targeted Countries

Most



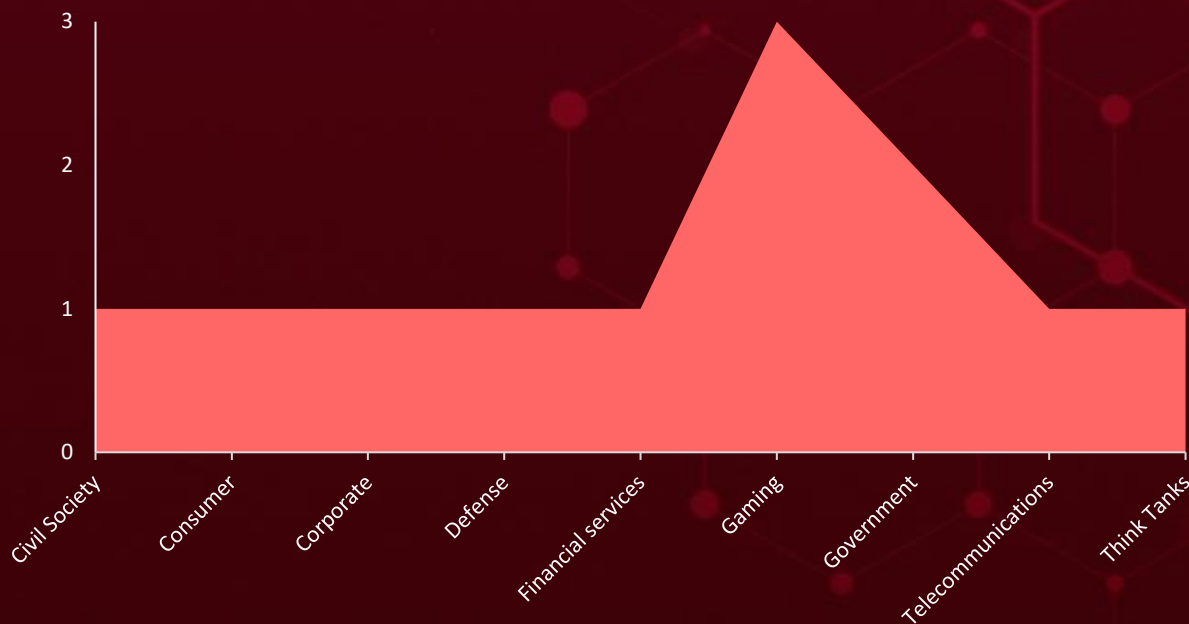
Least



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

Countries	Countries	Countries	Countries
United Arab Emirates	Philippines	Libya	Norway
Egypt	Tunisia	Brunei	Taiwan
Saudi Arabia	Austria	Denmark	Botswana
Iran	Armenia	Burundi	Tanzania
Turkey	Slovakia	Zambia	Ghana
China	United States	Sweden	Timor-Leste
Vietnam	Syria	Malawi	Greece
Jordan	Cyprus	Tajikistan	Italy
Israel	France	Belgium	Honduras
Nepal	Malaysia	Cameroon	Uganda
Singapore	Kazakhstan	Maldives	Poland
Palestine	United Kingdom	Canada	Azerbaijan
Germany	Kuwait	Mexico	Portugal
Thailand	Lebanon	Kenya	Uzbekistan
India	Yemen	Moldova	Hong Kong
Oman	Hungary	Rwanda	Romania
Indonesia	Ireland	Mongolia	Lithuania
Qatar	Sri Lanka	Serbia	Macao
Bahrain	Croatia	Finland	Laos
South Korea	Costa Rica	Bulgaria	Mauritius
Iraq	Kyrgyzstan	Myanmar	Chile
Morocco	Slovenia	South Africa	Jamaica
Bangladesh	Latvia	Bhutan	Ethiopia
Netherlands	Algeria	Spain	Zimbabwe
Japan	Belarus	Georgia	Monaco
Pakistan	Turkmenistan	Sudan	Liechtenstein
Cambodia	Afghanistan	North Korea	Colombia
	Russia	Switzerland	Czech Republic

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1082

System Information Discovery

T1027

Obfuscated Files or Information

T1566

Phishing

T1204

User Execution

T1140

Deobfuscate/Decode Files or Information

T1056

Input Capture

T1056.001

Keylogging

T1113

Screen Capture

T1574

Hijack Execution Flow

T1115

Clipboard Data

T1574.001

DLL Search Order Hijacking

T1497

Virtualization/Sandbox Evasion

T1588

Obtain Capabilities

T1204.002

Malicious File

T1218

System Binary Proxy Execution

T1106

Native API

T1566.001

Spearphishing Attachment

T1059.001

PowerShell



Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Blitz</u> TYPE RAT ASSOCIATED ACTOR sw1zzx	Blitz is a Windows-based malware first detected in 2024, distributed via fake Standoff 2 game cheats on Telegram. It employs a two-stage infection process with a downloader and a versatile bot capable of keylogging, DoS attacks, and cryptomining.	Fake Standoff 2 game cheats on Telegram	-
		IMPACT	AFFECTED PLATFORM
		Denial-of-Service (DoS) attacks, Financial Losses	Windows
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	ae2f4c49f73f6d88b193a46cd22551bb31183ae6ee79d84be010d6acf9f2ee57, 0e80fe5636336b70b1775e94aaa219e6aa27fcf700f90f8a5dd73a22c898d646		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XMRig</u>	XMRig is an open-source cryptocurrency miner often exploited by cybercriminals in cryptojacking attacks, covertly harnessing victims' computing resources to mine Monero (XMR).	Fake Standoff 2 game cheats on Telegram	-
		IMPACT	AFFECTED PLATFORM
		Operational Disruption, Financial Losses	Windows
			PATCH LINK
			-
TYPE			
Miner			
ASSOCIATED ACTOR			
sw1zzx			
IOC TYPE	VALUE		
SHA256	47ce55095e1f1f97307782dc4903934f66beec3476a45d85e33e48d63e1f2e15		

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>Atomic Stealer</u>	Atomic Stealer, or AMOS, is a prevalent macOS-targeting malware designed to harvest and exfiltrate sensitive data, including account credentials, browser information, and cryptocurrency wallet details.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Financial Losses	Windows and macOS
			PATCH LINK
TYPE			
Stealer			
ASSOCIATED ACTOR			
-			-
IOC TYPE	VALUE		
SHA256	3fb1bafe9e659a68b9177ef7b5d2e5240e6be86fb82f33f89c281bb058857c7a, a6a2ffe881e4e771f9c09283c483bcb41b5b84448b2df64afb84709d3fa09a9e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>VELETRIX</u>	VELETRIX is a custom implant that functions as a loader, establishing initial access on compromised systems. It uses basic anti-analysis techniques, notably leveraging the Sleep and Beep Windows APIs to evade detection and disrupt automated analysis.	Spear-phishing email	-
		IMPACT	AFFECTED PRODUCT
		Payload Delivery, Persistence Risk	-
			PATCH LINK
TYPE			
Loader			
ASSOCIATED ACTOR			
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>VShell</u>	VShell is a well-known cross-platform OST framework developed in Golang. Originally released as open-source and later removed by its creator, it has been widely weaponized by China-aligned threat groups. The VShell implant establishes a persistent command-and-control (C2) channel, providing attackers with continuous remote access to compromised systems.	Spear-phishing email	-
		IMPACT	AFFECTED PRODUCTS
		Persistent Remote Access, Information Theft	-
TYPE			PATCH LINK
OST framework			
ASSOCIATED ACTOR			-
-			-
IOC TYPE	VALUE		
SHA256	ba4f9b324809876f906f3cb9b90f8af2f97487167beead549a8cddfd9a7c2fdc, bb6ab67ddbb74e7afb82bb063744a91f3fecf5fd0f453a179c0776727f6870c7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Myth Stealer</u>	Myth Stealer is a Rust-based malware that continually evolves, adding features like clipboard hijacking to steal cryptocurrency. It exfiltrates passwords, browser cookies, saved credit cards, and screenshots to its operators. The malware is actively sold via subscription plans on Telegram.	Fraudulent gaming websites	-
		IMPACT	AFFECTED PRODUCT
		Information Theft, Financial Loss	-
TYPE			PATCH LINK
InfoStealer			
ASSOCIATED ACTOR			-
-			-
IOC TYPE	VALUE		
SHA256	65a84024daf30c12fd2e76db661bf6e85f3da30bb3aaa7e774152855d718b0c4, e5d09da6648add4776de8091b0182b935405791bf41476465b0e7dcb066fc0dc		

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>Horus Agent</u>	Horus Agent is a custom C++ based espionage tool. It employs advanced protections, including custom string encryption, control flow flattening, and API hashing to evade analysis. The implant can fingerprint systems, inject shellcode into legitimate processes, and remain dormant until receiving further instructions.	Phishing	CVE-2025-33053
		IMPACT	AFFECTED PRODUCTS
		Persistent Remote Control	Web Distributed Authoring and Versioning (WebDAV)
			PATCH LINK
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053
Stealth Falcon			
IOC TYPE	VALUE		
SHA256	ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Horus Loader</u>	Horus Loader is a custom, multi-stage C++ loader that leverages Code Virtualizer to transform code into custom virtual machine (VM) instructions, complicating reverse engineering. It serves as a lightweight alternative to the Themida protector. The loader is digitally signed, though with an outdated, timestamp-free signature, likely to evade certain security detections.	Phishing	CVE-2025-33053
		IMPACT	AFFECTED PRODUCT
Initial Payload Delivery		Web Distributed Authoring and Versioning (WebDAV)	
		PATCH LINK	
		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053	
TYPE			
Loader			
ASSOCIATED ACTOR			
Stealth Falcon			
IOC TYPE	VALUE		
SHA256	da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa		

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>RoKRAT</u>	RokRAT is a sophisticated remote access trojan that collects sensitive system data, captures live screenshots, monitors processes, and maintains encrypted command-and-control communications via cloud APIs on services like Dropbox, pCloud, and Yandex.	Spear-phishing	CVE-2022-41128
		IMPACT	AFFECTED PRODUCT
TYPE		Microsoft Windows	
Backdoor			
ASSOCIATED ACTOR		PATCH LINK	
APT37			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128
IOC TYPE	VALUE		
SHA256	92ab3a9040f5e620bc4b76295239c5240130d968c6cbeaa7dc555d2cf19bfae1, d182834a984c9f5b44ea0aca5786223a78138ff23d33362ab699c76bf6987261, 9b8218774c3abc0a449cfc490f12e81155af00ec90c2e1d630a61c29f70a98cb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>AsyncRAT</u>	AsyncRAT is a publicly available remote access trojan (RAT) hosted on GitHub. A modified variant achieves persistence by creating a scheduled task set to run at startup. On execution, it triggers a multi-step process to launch AsyncRAT within Windows Sandbox, which requires manual activation and a system reboot.	Spear-phishing Link	-
		IMPACT	AFFECTED PRODUCT
Remote Control, Information Theft		Windows	
		PATCH LINK	
		-	
TYPE			
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeeaa44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a		

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
Skuld Stealer TYPE Stealer ASSOCIATED ACTOR -	Skuld Stealer specializes in data exfiltration, targeting browser credentials, gaming sessions, Discord tokens, and cryptocurrency wallet seed phrases. It also compromises Electron-based wallets like Exodus and Atomic by injecting malicious .asar files.	Spear-phishing Link	-
		IMPACT	AFFECTED PRODUCT
		Wallet Compromise, Facilitates Further Intrusions	Windows
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	8135f126764592be3df17200f49140bfb546ec1b2c34a153aa509465406cb46c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mirai TYPE Botnet ASSOCIATED ACTOR -	Mirai is a notorious malware targeting Internet of Things (IoT) devices by exploiting weak or default credentials. Compromised devices are enlisted into a botnet used for large-scale Distributed Denial of Service (DDoS) attacks. Its open-source release has spawned numerous variants.	Exploiting Vulnerability	CVE-2025-24016
		IMPACT	AFFECTED PRODUCT
		Device Hijacking, Network Overload	Wazuh Server
			PATCH LINK
			https://github.com/wazuh/wazuh/releases/tag/v4.9.1
IOC TYPE	VALUE		
SHA256	dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9,7b659210c509058bd5649881f18b21b645acb42f56384cbd6dcb8d16e5aa0549,64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4eb692b08f52b0f		




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>Resbot</u>	ResBot, also known as Resensual, is a Mirai-based botnet variant. It leveraged multiple domains featuring Italian nomenclature to distribute and expand its network of infected devices.	Exploiting Vulnerability	CVE-2025-24016
		IMPACT	AFFECTED PRODUCTS
TYPE		Wazuh Server	
Botnet			
ASSOCIATED ACTOR		Device Hijacking, Network Overload	PATCH LINK
-			https://github.com/wazuh/wazuh/releases/tag/v4.9.1
IOC TYPE	VALUE		
SHA256	9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Fog ransomware</u>	Fog ransomware, first identified in April 2024, is a double-extortion threat that infiltrates networks. It spreads laterally using legitimate tools like RDP and PowerShell, exfiltrates sensitive data, and encrypts files with AES and RSA algorithms, appending extensions such as .fog, .FLOCKED, or .ffog. The malware disables security tools, deletes backups, and targets both Windows and Linux systems.	-	-
		IMPACT	AFFECTED PRODUCT
		Information Theft, Data encryption, Financial loss	Windows
			PATCH LINK
			-
TYPE			
Ransomware			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa		




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-2025-33053</u>		Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	Stealth Falcon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	Horus Agent, Horus Loader
Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability		cpe:2.3:o:microsoft:windows _server:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1071.002: File Transfer Protocols	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-32711</u>	EchoLeak	Microsoft 365 Copilot	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:365_copilot:*:*:*:*:*:*	-
M365 Copilot Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1005: Data from Local System	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-41128</u>		Windows: 7 - 11 22H2 10.0.22621.521, Windows Server: 2008 - 2022 20H2	APT37
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	RoKRAT
Microsoft Windows Scripting Languages Remote Code Execution Vulnerability		cpe:2.3:o:microsoft:windows _server:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24016</u>		Wazuh Server version 4.4.0 to 4.9.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wazuh:wazuh:*:*:* :*:*:*:*	Mirai, Resbot
Wazuh Server Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059.006: Python, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://github.com/wazuh/wazuh/releases/tag/v4.9.1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>sw1zzx</u>	Russian-speaking	Gaming	Europe, Asia, North Africa and North America
	MOTIVE		
	Information Theft, Espionage, Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Blitz, XMRig	Windows
TTPs			
TA0003: Persistence; TA0040: Impact; TA0005: Defense Evasion; TA0002: Execution; TA0007: Discovery; TA0011: Command and Control; TA0009: Collection; T1496: Resource Hijacking; T1204: User Execution; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1497.001: System Checks; T1574.001: DLL; T1574: Hijack Execution Flow; T1036: Masquerading; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1082: System Information Discovery; T1056.001: Keylogging; T1056: Input Capture; T1113: Screen Capture; T1499: Endpoint Denial of Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
<div></div> <div><u>Stealth Falcon (aka FruityArmor, Project Raven, G0038)</u></div>	UAE	Defense and Government Organizations	Middle East, Africa
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2025-33053	Horus Agent, Horus Loader	Web Distributed Authoring and Versioning (WebDAV)
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1003: OS Credential Dumping; T1105: Ingress Tool Transfer; T1056: Input Capture; T1056.001: Keylogging; T1095: Non-Application Layer Protocol; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1016: System Network Configuration Discovery; T1106: Native API			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
<div></div> <div><u>APT37 (aka RICOCHET CHOLLIMA, Reaper, TEMP.Reaper, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt)</u></div>	North Korea	Governments, Think Tanks, Activists (Civil Society)	South Korea
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2022-41128	RoKRAT	Microsoft Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1082: System Information Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1113: Screen Capture; T1115: Clipboard Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1070.004: File Deletion; T1132: Data Encoding; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **sw1zzx, Stealth Falcon, APT37**, and malware **Blitz, XMRig, Atomic Stealer, VELETRIX, VShell, Myth Stealer, Horus Agent, Horus Loader, RoKRAT, AsyncRAT, Skuld Stealer, Mirai, Resbot, Fog ransomware**.

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 **four exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **sw1zzx, Stealth Falcon, APT37**, and malware **Blitz, Atomic Stealer, VShell, Myth Stealer, Horus Loader, AsyncRAT, Resbot Botnet, Mirai Botnet, RokRAT Backdoor** in Breach and Attack Simulation(BAS).

Threat Advisories

[Blitz Malware Exposed: The Dark Side of Free Game Cheats](#)

[Clickfix Scam Targets macOS with AMOS Malware](#)

[Operation DRAGONCLONE Strikes the Telecom Sector](#)

[Myth Stealer Strikes Through Game Lures](#)

[Zero-Day Stealth: Inside Stealth Falcon's Abuse of CVE-2025-33053](#)

[Microsoft's June 2025 Patch Tuesday Fixes Active Zero-Day Exploits](#)

[APT37 Operation ToyBox Story Exposes Cybersecurity Blind Spots](#)

[Invite Only: How Discord Links Became a Cybercrime Gateway](#)

[Wazuh Server Vulnerability Hijacked by Mirai Variants](#)

[Fog Ransomware: From Financial Extortion to Covert Espionage](#)

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>Blitz</u>	SHA256	0e80fe5636336b70b1775e94aaa219e6aa27fcf700f90f8a5dd73a22c898d646, cacc1f36b3817e8b48fabbb4b4bd9d2f1949585c2f5170e3d2d04211861ef2ac, aa5cd0219e8a0bd2e7d6c073f611102d718387750198bff564c20ca7ebada309, f3b7bbe1079974fd505abaadbcbf4dc0517620592eacbbe5f314a76775dd760c2, cdf192e92d14b9d7e1201c23621c4e0b8ee0673c192bdd734afd97519afef271, 6441e7000713f96c7ae114ce62378556d01fa29d435a5be0f11a5e80be9a26ed, b1b1ce259fcf5127c3477e278c3696dc7d15db63b673fdcf75e1deb89a0f6fd1, 5ef29d6d4f72e62e0d5a1d0b85eed70b729cd530c8cb2745c66a25f5b5c7299e, 5fc132b054099a1a65f377a3a22b003a6507107f3095371b44dbf5e098b02295, b18e21e50f1c346c83c4cba933b6466ada22febaafa25c03ac01122a12164375, a34a4a7c71de2d4ec4baf56fd143d27eedebbb785a2ba3e0740b92e62efd81ea, bedeafd3680cad581a619fb58aa4f57ed991c4a8dd94df46ef9cbd08a8dd6052, ae2f4c49f73f6d88b193a46cd22551bb31183ae6ee79d84be010d6acf9f2ee57, 88e2d0d59a9751e4ce5223951f5a75b1731b1ee82d18705aba83ba4bd7e8e5c1

Attack Name	TYPE	VALUE
<u>XMRig</u>	SHA256	47ce55095e1f1f97307782dc4903934f66beec3476a45d85e33e48d63e1f2e15
<u>Atomic Stealer</u>	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 3fb1bafe9e659a68b9177ef7b5d2e5240e6be86fb82f33f89c281bb058857c7a, a6a2ffe881e4e771f9c09283c483bcb41b5b84448b2df64afb84709d3fa09a9e
	MD5	eaedee8fc9fe336bcde021bf243e332a, 6fd092d86235d7ae35c557523f493674
<u>VShell</u>	SHA256	ba4f9b324809876f906f3cb9b90f8af2f97487167beead549a8cddfd9a7c2fdc, bb6ab67ddbb74e7afb82bb063744a91f3fecf5fd0f453a179c0776727f6870c7, 2206cc6bd9d15cf898f175ab845b3deb4b8627102b74e1accefe7a3ff0017112, a0f4ee6ea58a8896d2914176d2bfdbdb9e16b700f52d2df1f77fe6ce663c1426a
<u>Myth Stealer</u>	SHA256	65a84024daf30c12fd2e76db661bf6e85f3da30bb3aaa7e774152855d718b0c4, e5d09da6648add4776de8091b0182b935405791bf41476465b0e7dcb066fc0dc, acd66cb5f1447b803245c495400ad0886352920e35defcca6c45519fb7d33693, 6c54e6648a6a33583d7707a9f7c5e83dd08ed481df6354c52e8f81e729d74a82
<u>Horus Agent</u>	SHA256	ddce79afe9f67b78e83f6e530c3e03265533eb3f4530e7c89fdc357f7093a80b
<u>Horus Loader</u>	SHA256	da3bb6e38b3f4d83e69d31783f00c10ce062abd008e81e983a9bd4317a9482aa
<u>RoKRAT</u>	SHA256	92ab3a9040f5e620bc4b76295239c5240130d968c6cbeaa7dc555d2cf19bfae1, d182834a984c9f5b44ea0aca5786223a78138ff23d33362ab699c76bf6987261, 9b8218774c3abc0a449cfc490f12e81155af00ec90c2e1d630a61c29f70a98cb
<u>AsyncRAT</u>	SHA256	53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a
	Domain	microads[.]top

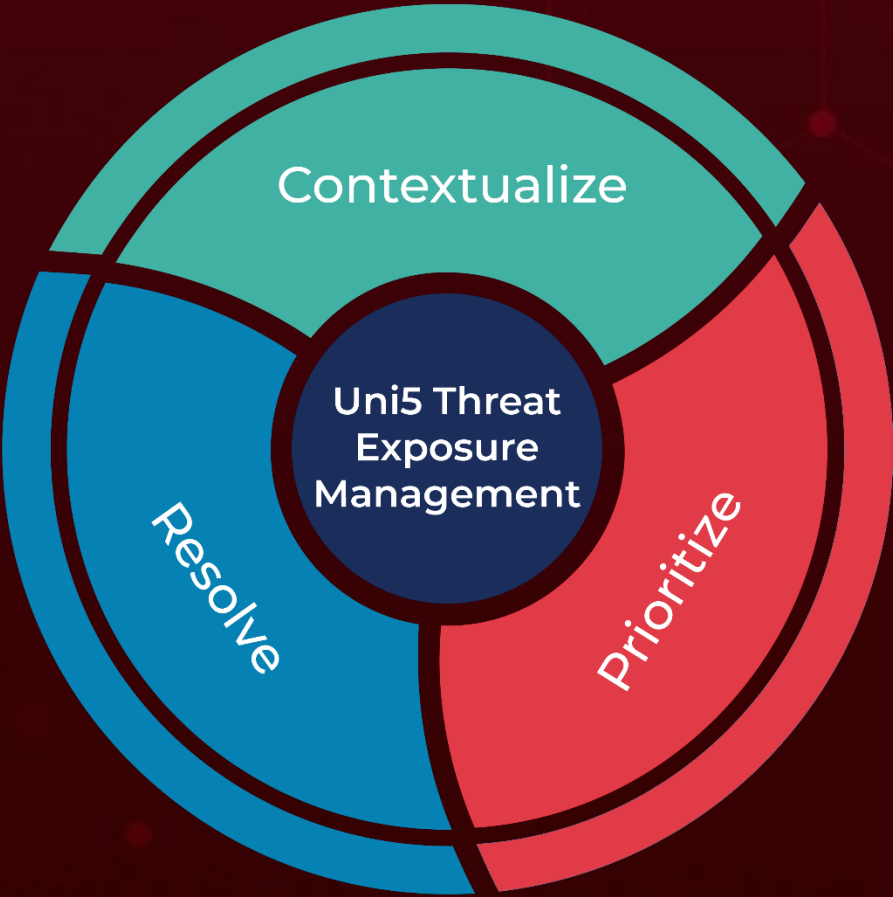
Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	URLs	hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/AClient[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/AClient[.]exe, hxxps[:]//pastebin[.]com/raw/ftknPNF7, hxxps[:]//pastebin[.]com/raw/NYpQCL7y, hxxps[:]//pastebin[.]com/raw/QdseGsQL
	IPv4	101[.]99[.]76[.]120, 87[.]120[.]127[.]37, 185[.]234[.]247[.]8
<u>Skuld Stealer</u>	SHA256	8135f126764592be3df17200f49140bfb546ec1b2c34a153aa509465406cb46c
	URLs	hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/skul[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/skul[.]exe
<u>Mirai</u>	Botnet	dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9, 7b659210c509058bd5649881f18b21b645acb42f56384cbd6dc b8d16e5aa0549, 64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4e b692b08f52b0f, 4c1e54067911aeb5aa8d1b747f35fdcdfdf4837cad60331e58a7 bbb849ca9eed, 811cd6eb9e2b7438ad9d7c382db13c1c04b7d52049526109 3af51797f5d4cc, 90df78db1fb5aea6e21c3daca79cc690900ef8a779de61d5b3c0 db030f4b4353, 8a58fa790fc3054c5a13f1e4e1fcb0e1167dbfb5e889b7c543d3c dd9495e9ad6, c9df0a2f377ffab37ede8f2b12a776a7ae40fa8a6b4724d5c1898 e8e865cfea1, 6614545eec64c207a6cc981fccae8077eac33a79f286fc9a9258 2f78e2ae243a
<u>Resbot</u>	SHA256	9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b
<u>Fog ransomware</u>	SHA256	181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa

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
June 16, 2025 • 9:30 PM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com