

Date of Publication  
July 21, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

14 to 20 JULY 2025

# Table Of Contents

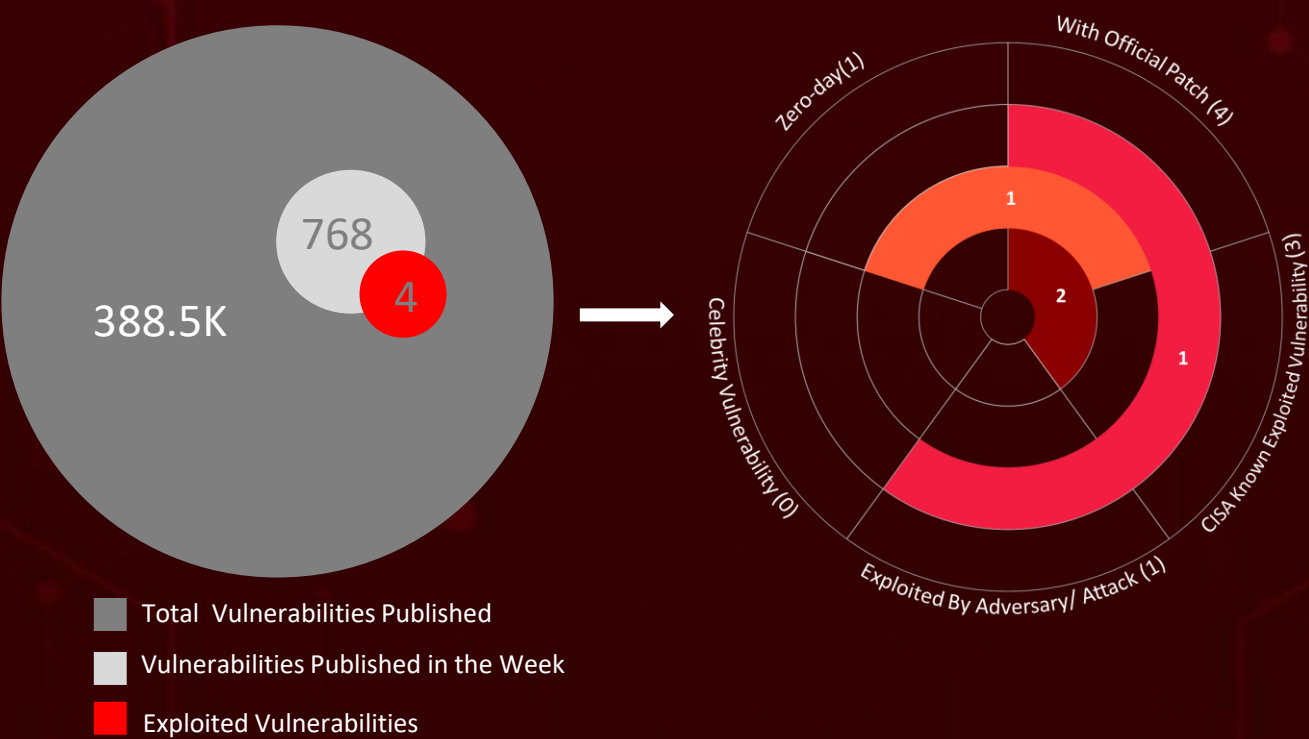
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	18
<u>Threat Advisories</u>	19
<u>Appendix</u>	20
<u>What Next?</u>	22

# Summary

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

Recent, a critical flaw ([CVE-2025-47812](#)) in Wing FTP Server allows attackers to execute code via a null byte login exploit, with active attacks and a public PoC emerging just a day after disclosure. [CVE-2025-25257](#) is a critical unauthenticated SQL injection flaw in Fortinet FortiWeb that allows attackers to execute SQL commands and achieve RCE; a public PoC is available, making immediate patching essential.

Additionally, [NordDragonScan](#) is a new .NET-based info-stealer spreading via malicious HTA scripts and deceptive links, designed to covertly harvest sensitive data in targeted cyber-espionage attacks. [Interlock ransomware](#) now uses a PHP-based RAT via fake CAPTCHA lures and Cloudflare Tunnel, enabling stealthy system access and advanced intrusion tactics. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

8

Attacks  
Executed

4

Vulnerabilities  
Exploited

0

Adversaries in  
Action

- [NordDragonScan](#)
- [Interlock ransomware](#)
- [Interlock PHP RAT](#)
- [Octalyn Stealer](#)
- [GLOBAL Ransomware](#)
- [GhostContainer](#)
- [Voldemort](#)
- [HealthKick](#)
- [CVE-2025-47812](#)
- [CVE-2025-25257](#)
- [CVE-2025-6558](#)
- [CVE-2020-0688](#)



# Insights

**Octalyn** Forensic Toolkit poses as a research tool but is a stealthy credential stealer, openly shared on GitHub, enabling easy data theft via Telegram.

**NordDragonScan** is a .NET info-stealer using malicious HTA scripts and deceptive links to steal data.

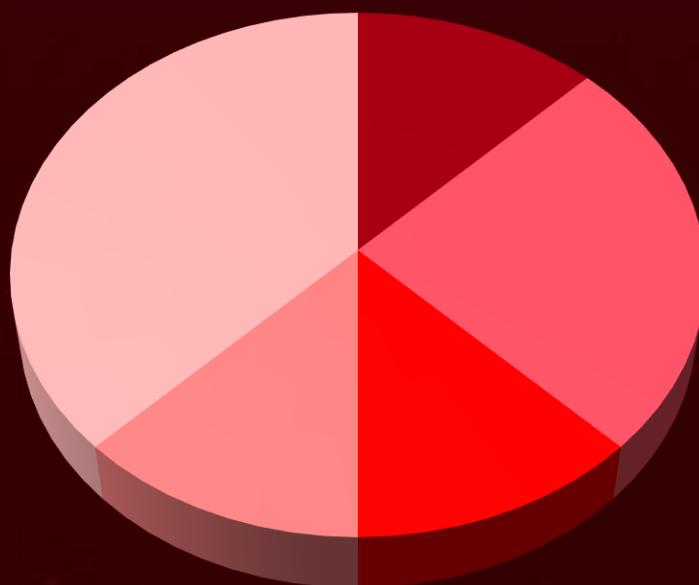
**Critical Zero-Day** vulnerability in Google Chrome (CVE-2025-6558) under active exploitation, immediate patch required to prevent full system compromise.

**GLOBAL GROUP**, a RaaS operation since June 2025, offers high payouts, AI-driven negotiation tools, and flexible ransomware kits, gaining popularity on Russian cybercrime forums.

**CVE-2025-25257** is a critical unauthenticated SQL injection in Fortinet FortiWeb allowing RCE via malicious API requests, immediate patching is urged.

**CVE-2025-3648** "Count(er) Strike" exposes sensitive ServiceNow data via access control flaws, allowing attackers to infer hidden info through search count leaks.

## Threat Distribution



■ Infostealer ■ Ransomware ■ RAT ■ Stealer ■ Backdoor

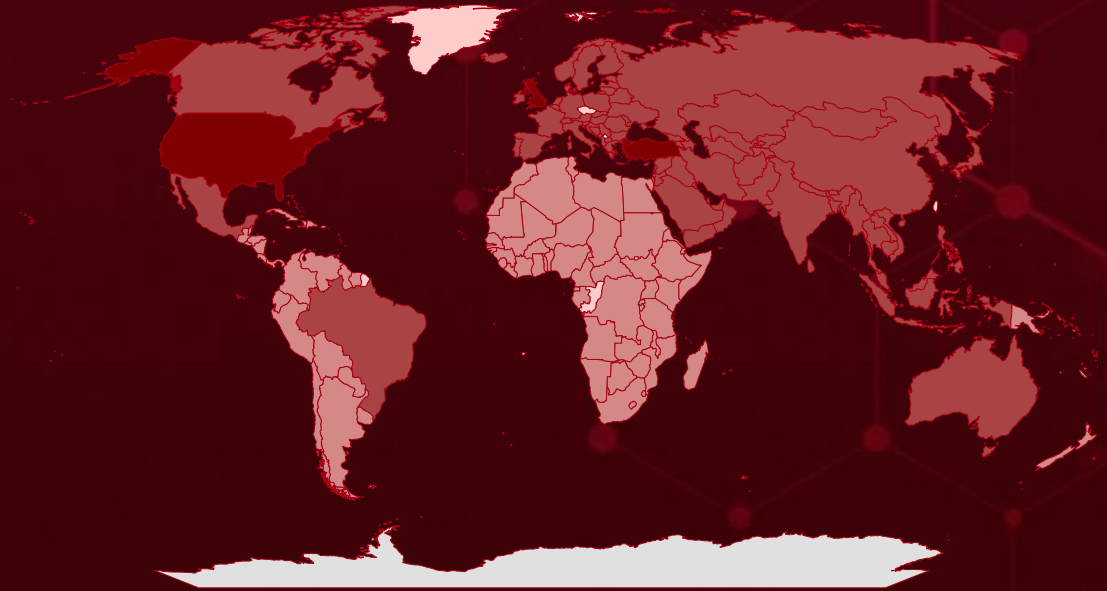


# Targeted Countries

Most



Least



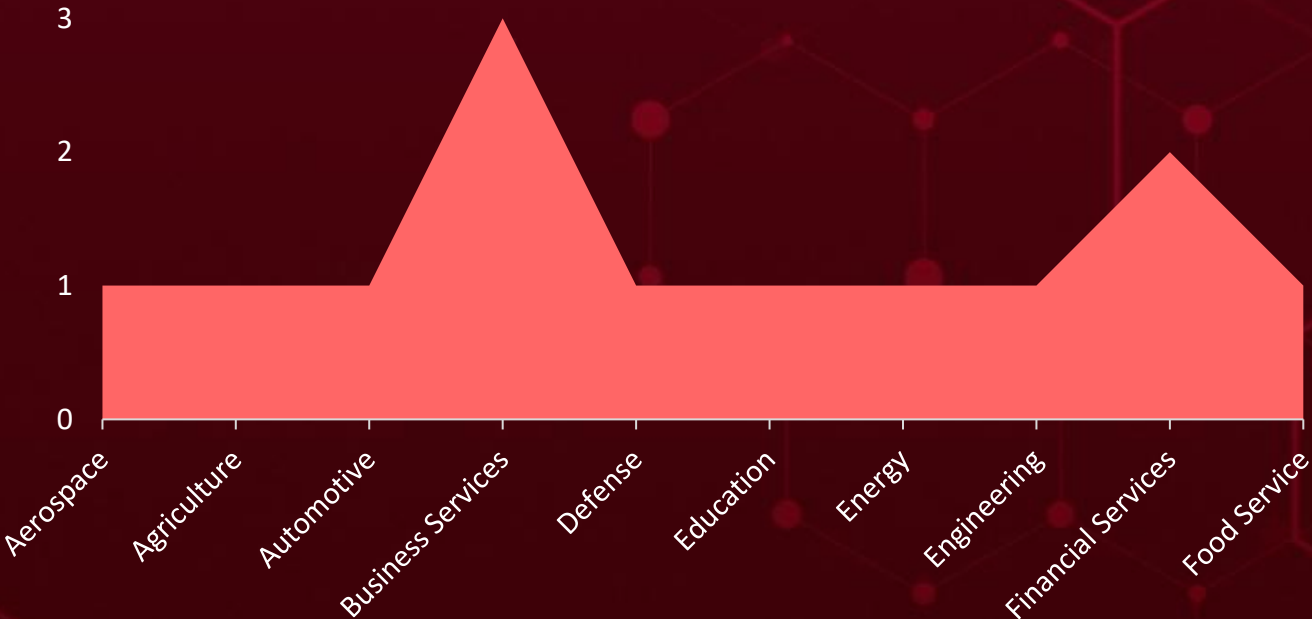
Powered by Bing

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

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



# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1190

Exploit Public-Facing Application

### T1204

User Execution

### T1566

Phishing

### T1068

Exploitation for Privilege Escalation

### T1090

Proxy

### T1078

Valid Accounts

### T1036

Masquerading

### T1588.002

Tool

### T1027

Obfuscated Files or Information

### T1204.001

Malicious Link

### T1588

Obtain Capabilities

### T1566.001

Spearphishing Attachment

### T1203

Exploitation for Client Execution

### T1572

Protocol Tunneling

### T1133

External Remote Services

### T1588.006

Vulnerabilities

### T1105

Ingress Tool Transfer

### T1041

Exfiltration Over C2 Channel

### T1588.005

Exploits



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">NordDragonScan</a>	NordDragonScan, a newly identified information-stealing malware, is actively targeting systems through malicious HTA scripts delivered via deceptive shortened links. This .NET based threat is engineered to quietly harvest sensitive data.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data theft and Data exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	f8403e30dd495561dc0674a3b1aediaea5d6839808428069d98e30e19bd6dc045, fbffe681c61f9bba4c7abcb6e8fe09ef4d28166a10bfeb73281f874d84f69b3d, 39c68962a6b0963b56085a0f1a2af25c7974a167b650cf99eb1acd433ecb772b, 9d1f587b1bd2cce1a14a1423a77eb746d126e1982a0a794f6b870a2d7178bd2c, 7b2b757e09fa36f817568787f9eae8ca732dd372853bf13ea50649dbb62f0c5b		

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>INTERLOCK</u>	INTERLOCK is an emerging ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. While the Windows variant is most common, INTERLOCK stands out for its rare focus on FreeBSD. The group employs refined double-extortion tactics and runs a leak site called “Worldwide Secrets Blog” to publish stolen data and pressure victims into negotiations.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaaae3a486aabdb8c0266e9426f		

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>INTERLOCK</u> <u>PHP</u>	The Interlock PHP RAT is a lightweight, fileless remote access trojan used by the Interlock ransomware group for initial access and system reconnaissance. It is delivered via social engineering (FileFix phishing) and establishes covert communication through Cloudflare Tunnel and fallback IPs. The RAT enables attackers to execute commands, deploy payloads, and maintain persistent access before ransomware deployment.	FileFix phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
RAT		Stealthy Persistence, Pre-Ransomware Intrusion	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3, 8afd6c0636c5d70ac0622396268786190a428635e9cf28ab23add939377727b0		
IPv4	64[.]95[.]12[.]71, 184[.]95[.]51[.]165		

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="#">Octalyn Stealer</a>	The Octalyn Forensic Toolkit, though disguised as an educational tool, is actually a stealthy credential stealer that preys on unsuspecting users. Shared openly on GitHub, it lures in low-skilled actors with a simple builder that creates custom data-stealing payloads using just a Telegram bot token and chat ID. Once deployed, the malware silently steals sensitive information like browser cookies, saved passwords, Discord tokens, crypto wallets, VPN configs, and more organizing everything neatly into folders before zipping it up and sending it back to the attacker via Telegram.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Stealer		Data theft and System Compromise.	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	8bd9925f7b7663ca2fcb305870248bd5de0c684342c364c24ef24bffbcdcd8b		

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>GLOBAL Ransomware</u>	GLOBAL GROUP, a Ransomware-as-a-Service (RaaS) operation active since June 2025, is gaining traction on Russian-speaking cybercrime forums by offering high affiliate payouts and flexible tooling. The group relies on Initial Access Brokers for network entry. It offers affiliates AI-powered negotiation systems, mobile-accessible dashboards, and customizable ransomware builders, making the platform more attractive to a wider range of cybercriminal partners.	Via Initial Access Brokers	-
TYPE		IMPACT	AFFECTED PRODUCT
Ransomware		Data Theft and Data Encryption	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73		
TOR Address	vg6xwkmfyirv3l6qtqus7jykucvgx6imegb73hqny2avxccnmqt5m2id[.]onion, gdbkvfe6g3whrzkdlibytksygk45zwgmnnzh5i2xmoyo3mrpipysjagqyd[.]onion		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>GhostContainer</u>	GhostContainer, is a stealthy and highly sophisticated malware and has been discovered targeting Microsoft Exchange servers in government and high-tech environments across Asia. This backdoor blends seamlessly into normal operations, making it incredibly hard to detect, while allowing attackers to maintain long-term access, all without ever reaching out to an external command-and-control server.	Exploiting vulnerabilities	CVE-2020-0688
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor			
ASSOCIATED ACTOR			
-		Unauthorized access and Data theft	Microsoft Exchange Server
	PATCH LINK		
			<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688</a>
IOC TYPE	VALUE		
SHA256	87a3aefb5cdf714882eb02051916371fbf04af2eb7a5ddeae4b6b441b2168e36		

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>Voldemort</u>	Voldemort malware is a stealthy, modular backdoor used in targeted cyberattacks for persistent access and surveillance. It supports command execution, credential theft, and lateral movement across compromised networks. The malware often employs encrypted communication channels to evade detection and maintain long-term access.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Persistent Access, Credential Theft, Lateral Movement	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb, ec5fef700d1ed06285af1f2d01fa3db5ea924de3c2da2f0e6b7a534f69d8409c, cd009ea4c682b61963210cee16ed663eee20c91dd56483d456e03726e09c89a7		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>HealthKick</u>	HealthKick is a custom backdoor used by China-aligned threat actors, specifically observed targeting the Taiwanese semiconductor industry. It is typically delivered via spear-phishing campaigns, often through DLL sideloading vulnerabilities. Once active, HealthKick can execute commands, capture results, and exfiltrate data to a command-and-control server using a "FakeTLS" protocol.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Credential Theft, 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.






# Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-47812</u>		Wing FTP Server before 7.4.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wftpserver:wing_ftp_server:*:*:*:*:*:*	-
Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-158	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1136: Create Account	<a href="https://www.wftpserver.com/download.htm">https://www.wftpserver.com/download.htm</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-25257</u>		Fortinet FortiWeb versions: 7.6.0 - 7.6.3 7.4.0 - 7.4.7 7.2.0 - 7.2.10 7.0.0 - 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*	-
Fortinet FortiWeb SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	<a href="https://fortiguard.fortinet.com/psirt/FG-IR-25-151">https://fortiguard.fortinet.com/psirt/FG-IR-25-151</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-6558</u>		Google Chrome prior to 138.0.7204.157	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chrome Insufficient Validation of Untrusted Input in ANGLE and GPU Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1497: Virtualization/Sandbox Evasion, T1189: Drive-by Compromise	<a href="https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html">https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-0688</u>		Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY		
Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	GhostContainer
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1203: Exploitation for Client Execution, T1059: Command and Scripting	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688</a>



# Adversaries in Action

No active threat actors have been tracked in the past week.

# 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 malware **NordDragonScan, Interlock ransomware, Interlock PHP RAT, Octalyn Stealer, GLOBAL Ransomware, GhostContainer, Voldemort, HealthKick.**

## 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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to malware **NordDragonScan, Octalyn Stealer, GLOBAL Ransomware, Voldemort Backdoor**, in Breach and Attack Simulation(BAS).

# Threat Advisories

[Wing FTP Flaw Enables System Takeover](#)

[Critical Unauthenticated SQL Injection Flaw in Fortinet FortiWeb](#)

[NordDragonScan Turns Simple Lures into Silent Data Heists](#)

[Count\(er\) Strike: CVE-2025-3648 Exposes ServiceNow Data](#)

[CVE-2025-6558: Chrome Flaw Lets Hackers Break the Sandbox](#)

[Interlock Ransomware Deploys New PHP RAT via FileFix Phishing](#)

[Octalyn: The Stealer Hidden in Plain Sight](#)

[GLOBAL GROUP RaaS Gains Momentum with AI-Powered Negotiation Tools](#)

[GhostContainer Malware Targets Asian Government Networks](#)

[Taiwan's Semiconductor Firms Under Siege by Chinese Cyber Operations](#)

# 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)

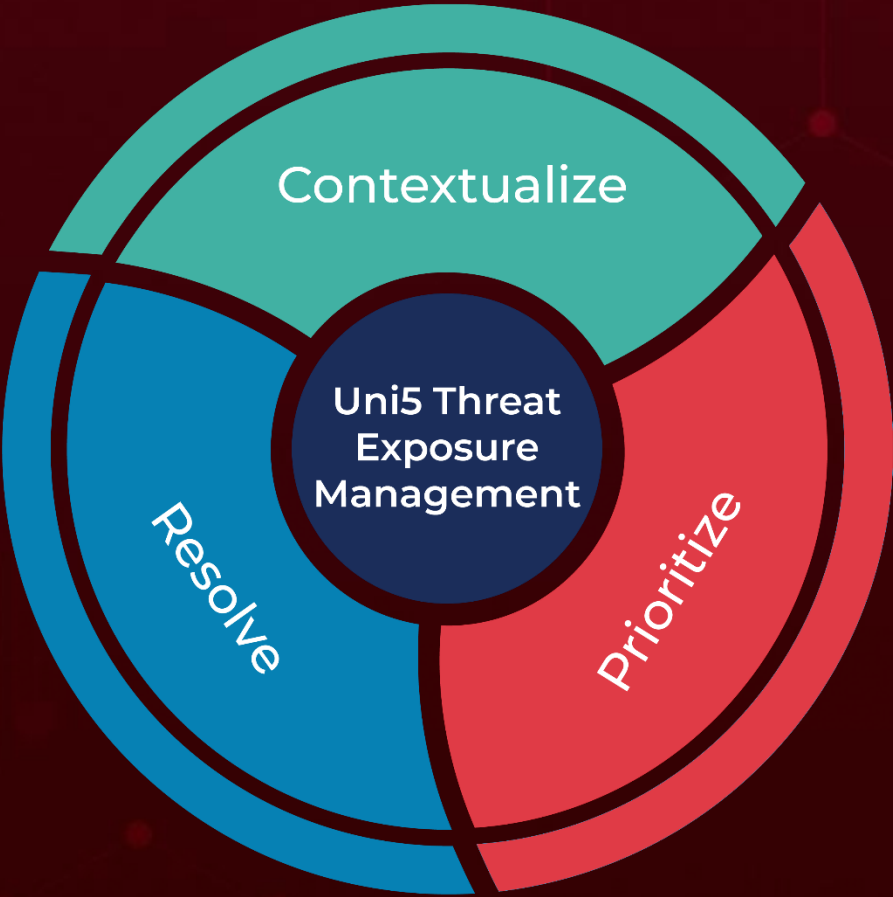
Attack Name	TYPE	VALUE
<u>NordDragonScan</u>	SHA256	f8403e30dd495561dc0674a3b1aedaea5d6839808428069d98e30e19bd6dc045, fbffe681c61f9bba4c7abcb6e8fe09ef4d28166a10bfeb73281f874d84f69b3d, 39c68962a6b0963b56085a0f1a2af25c7974a167b650cf99eb1acd433ecb772b, 9d1f587b1bd2cce1a14a1423a77eb746d126e1982a0a794f6b870a2d7178bd2c, 7b2b757e09fa36f817568787f9eae8ca732dd372853bf13ea50649dbb62f0c5b, f4f6beea11f21a053d27d719dab711a482ba0e2e42d160cefdbdad7a958b93d0
<u>Interlock ransomware</u>	SHA256	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f
<u>Interlock PHP RAT</u>	SHA256	28a9982cf2b4fc53a1545b6ed0d0c1788ca9369a847750f5652ffa0ca7f7b7d3, 8afd6c0636c5d70ac0622396268786190a428635e9cf28ab23add939377727b0

Attack Name	TYPE	VALUE
<u>Interlock PHP RAT</u>	IPv4	64[.]95[.]12[.]71, 184[.]95[.]51[.]165
	Domain	existed-bunch-balance-councils[.]trycloudflare[.]com, ferrari-rolling-facilities-lounge[.]trycloudflare[.]com, galleries-physicians-ppsp-wv[.]trycloudflare[.]com, evidence-deleted-procedure-bringing[.]trycloudflare[.]com, nowhere-locked-manor-hs[.]trycloudflare[.]com, ranked-accordingly-ab-hired[.]trycloudflare[.]com
<u>Octalyn Stealer</u>	SHA256	8bd9925f7b7663ca2fcb305870248bd5de0c684342c364c24ef24bffbcbcdcd8b
<u>GLOBAL Ransomware</u>	SHA256	a8c28bd6f0f1fe6a9b880400853fc86e46d87b69565ef15d8ab757979cd2cc73
	TOR Address	vg6xwkmfyirv3l6qtqus7jykcuvngx6imegb73hqny2avxccnmqt5m2id[.]onion, gdbkvfe6g3whrzkdbytksygk45zwgmnh5i2xmgyo3mrpipysjagqyd[.]onion
<u>GhostContainer</u>	MD5	01d98380dfb9211251c75c87ddb3c79c
	SHA1	2bb0a91c93034f671696da64a2cf6191a60a79c5
	SHA256	87a3aefb5cdf714882eb02051916371fbf04af2eb7a5ddeae4b6b441b2168e36
	Filename	App_Web_Container_1.dll
<u>Voldemort</u>	SHA256	1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb, ec5fef700d1ed06285af1f2d01fa3db5ea924de3c2da2f0e6b7a534f69d8409c, cd009ea4c682b61963210cee16ed663eee20c91dd56483d456e03726e09c89a7

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON  
**July 21, 2025 • 7:30 AM**

© 2025 All Rights are Reserved by Hive Pro



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