Date of Publication
May 5, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

28 APRIL to 04 MAY 2025

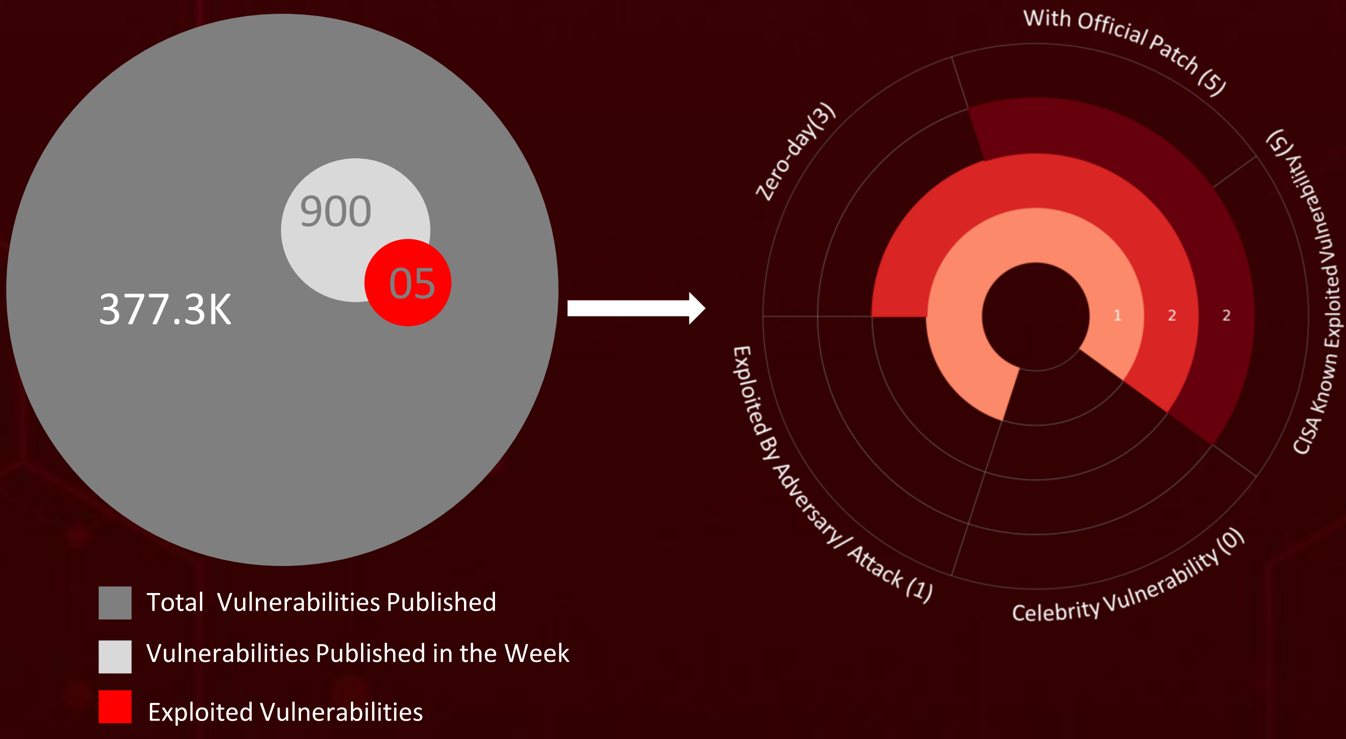
Table Of Contents

Summary

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

One such threat is the active exploitation of a high-severity vulnerability **(CVE-2025-3928)** in Commvault’s Web Server. Authenticated attackers can plant web shells and execute code on Windows and Linux systems, potentially leading to full system compromise. Similarly, active exploits are targeting SonicWall's SMA 100 Series flaws **(CVE-2023-44221 and CVE-2024-38475),** enabling command injection and session hijacking.

Adding to the growing list of cyber threats, **Hannibal Stealer** is a rebranded, advanced malware targeting browsers, cryptocurrency wallets, and communication apps. Evolving from Sharp and TX Stealer, it bypasses modern security measures, blurring the line between financial cybercrime and hacktivist motives, signaling a mounting threat. These developments underscore the increasing sophistication of cyber adversaries and reinforce the urgent need for agile, proactive cybersecurity defenses to navigate an increasingly hostile digital landscape.



High Level Statistics

2
Attacks Executed

5
Vulnerabilities Exploited

0
Adversaries in Action

- DslogdRAT
- Hannibal Stealer

- CVE-2025-0282
- CVE-2025-31324
- CVE-2025-3928
- CVE-2024-38475
- CVE-2023-44221

Insights

CVE-2025-3928 in Commvault's Web Server allows authenticated attackers to plant web shells.

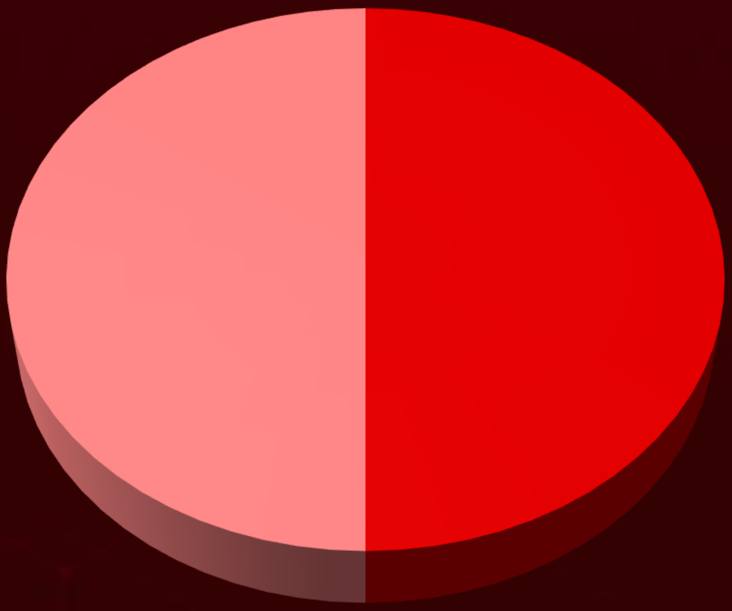
SonicWall Alert: Active exploits target SMA 100 Series flaws **(CVE-2023-44221, CVE-2024-38475)**, enabling command injection and session hijacking.

Japanese firms hit by **CVE-2025-0282**, deploying DslogdRAT via a hidden Perl shell.

Critical **SAP NetWeaver flaw (CVE-2025-31324)** is being exploited to drop web shells and run malicious code. Attackers can upload harmful files without logging in.

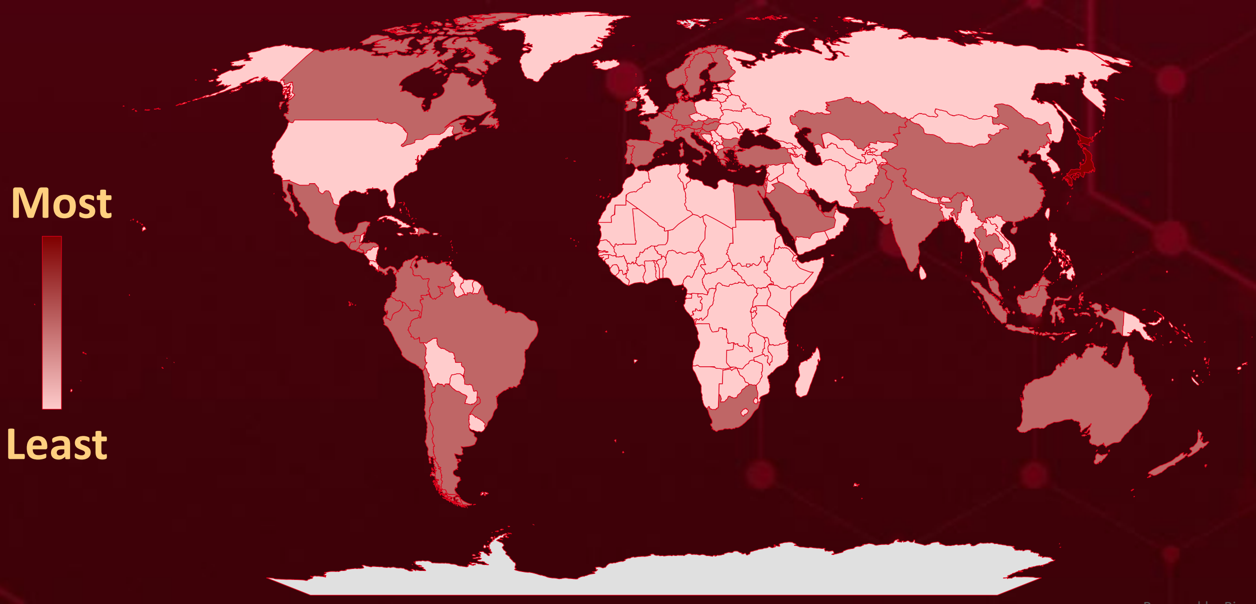
Hannibal Stealer: Rebranded from Sharp and TX Stealer, this malware targets browsers, crypto wallets, and communication apps, bypassing security and blending cybercrime with hacktivism.

Threat Distribution



🟥 RAT ▨ Stealer

Targeted Countries



Powered by Bing

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

	Countries
🟥	Japan
▨	Slovakia
▨	Norway
▨	Andorra
▨	Indonesia
▨	Argentina
▨	Malaysia
▨	Australia
▨	Portugal
▨	Austria
▨	Sweden
▨	Bahrain
▨	Israel
▨	Belgium
▨	United Arab Emirates
▨	Brazil
▨	Netherlands
▨	Bulgaria
▨	Panama
▨	Canada
▨	Saudi Arabia
▨	Chile
▨	South Africa
▨	China

	Countries
▨	Thailand
▨	Colombia
▨	Ireland
▨	Croatia
▨	Italy
▨	Denmark
▨	Kazakhstan
▨	Dominican Republic
▨	Venezuela
▨	Ecuador
▨	Mexico
▨	Egypt
▨	New Zealand
▨	El Salvador
▨	Pakistan
▨	Finland
▨	Peru
▨	France
▨	Qatar
▨	Germany
▨	Singapore
▨	Greece
▨	Slovenia
▨	Guatemala

	Countries
▨	India
▨	Kuwait
▨	Spain
▨	Honduras
▨	Switzerland
▨	Hungary
▨	Turkey
□	Trinidad and Tobago
□	Samoa
□	Côte d'Ivoire
□	Estonia
□	DR Congo
□	Eswatini
□	Congo
□	Ethiopia
□	Cyprus
□	Fiji
□	Barbados
□	Bhutan
□	Syria
□	Bolivia
□	Namibia
□	Gabon
□	North Korea

	Countries
□	Georgia
□	Russian Federation
□	Bosnia and Herzegovina
□	Senegal
□	Ghana
□	Somalia
□	Botswana
□	Sudan
□	Grenada
□	Benin
□	Armenia
□	Tuvalu
□	Guinea
□	Nepal
□	Guinea-Bissau
□	Niger
□	Guyana
□	Costa Rica
□	Haiti
□	Bangladesh
□	Holy See
□	Philippines
□	Brunei

Targeted Industries

No targeted industries tracked this week.

TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1588
Obtain Capabilities

T1588.006
Vulnerabilities

T1505
Server Software Component

T1071
Application Layer Protocol

T1027
Obfuscated Files or Information

T1083
File and Directory Discovery

T1082
System Information Discovery

T1560
Archive Collected Data

T1078
Valid Accounts

T1190
Exploit Public-Facing Application

T1105
Ingress Tool Transfer

T1566.001
Spearphishing Attachment

T1518
Software Discovery

T1068
Exploitation for Privilege Escalation

T1071.001
Web Protocols

T1562.001
Disable or Modify Tools

T1574
Hijack Execution Flow

T1562
Impair Defenses

T1041
Exfiltration Over C2 Channel

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DslogdRAT	DslogdRAT is a new RAT targeting Japanese organizations, installed via a zero-day Ivanti Connect Secure vulnerability (CVE-2025-0282). It deploys with a web shell, enabling command execution and communication with a C2 server.	Exploiting Vulnerabilities	CVE-2025-0282
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System compromise and data exfiltration	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
-			https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

IOC TYPE	VALUE
SHA256	1dd64c00f061425d484dd67b359ad99df533aa430632c55fa7e7617b55dab6a8

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Hannibal Stealer	Hannibal Stealer is a data-stealing malware that extracts credentials, cryptocurrency wallet information, and other sensitive data from infected systems. It targets various applications and also hijacks clipboards for cryptocurrency transactions.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	f69330c83662ef3dd691f730cc05d9c4439666ef363531417901a86e7c4d31c8

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
CVE-2025-0282	✗	Ivanti Connect Secure: 22.7R2 through 22.7R2.4 Ivanti Policy Secure: 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*:*	DslogdRAT
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31324	✗	SAP NetWeaver Version 7.50	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:sap_netweaver:7.50.*.*.*.*.*.*.*	-
SAP NetWeaver Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1505.003: Server Software Component: Web Shell	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-3928	✗	Commvault Versions 11.36.0 - 11.36.45, 11.32.0 - 11.32.88, 11.28.0 - 11.28.140, 11.20.0 - 11.20.216	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:commvault:commvault:*:*:*:*:*:*:*:*	-
Commvault Web Server Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1059: Command and Scripting Interpreter; T1505.003: Server Software Component: Web Shell	https://documentation.commvault.com/11.20/download_software.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38475	✗	SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*	-
Apache HTTP Server Improper Escaping of Output Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-116	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://httpd.apache.org/download.cgi

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-44221	✗	SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*	-
SonicWall SMA100 Appliances OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

Adversaries in Action

No Active Adversaries tracked this week.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the malware **DslogdRAT, Hannibal Stealer.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the malware **DslogdRAT, Hannibal Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

DslogdRAT Malware Exploits Ivanti Connect Secure Zero-Day Vulnerability

Critical CVE-2025-31324 Flaw in SAP NetWeaver Under Active Attack

Hannibal Stealer: Rebranded, Resurrected, and Ruthless

Web Shell Threat in Commvault: Patch CVE-2025-3928 Now

Urgent Patch Required: Active Attacks Exploiting SonicWall SMA Vulnerabilities

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)

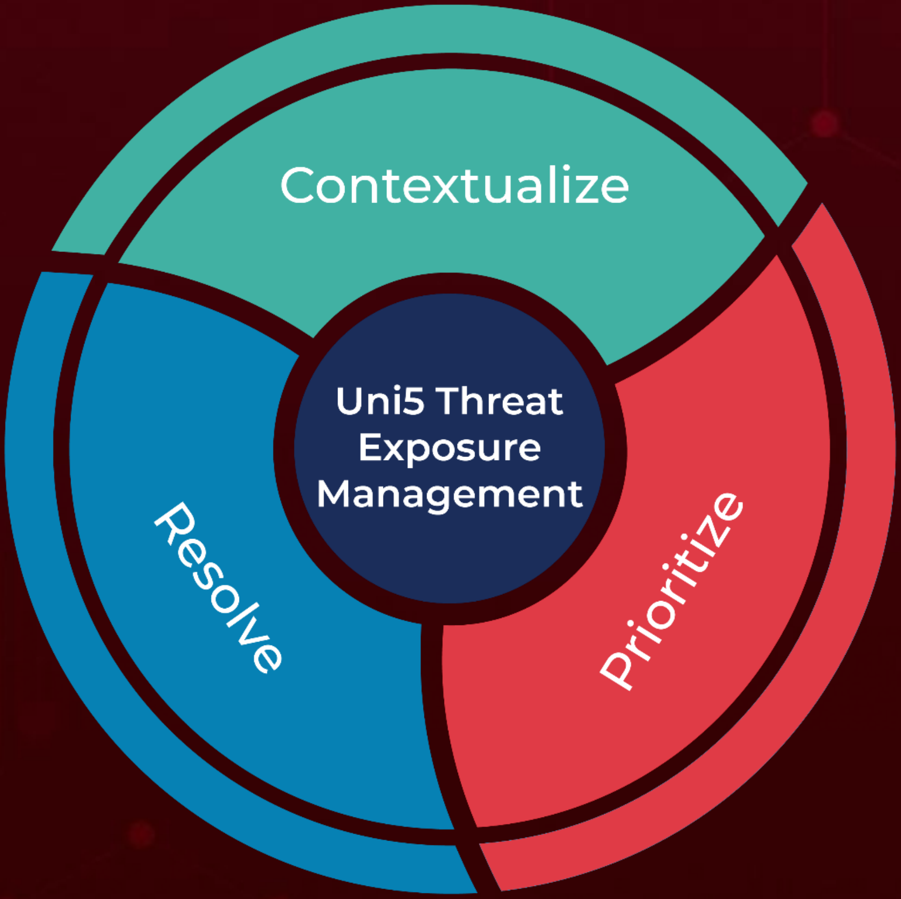
Attack Name	TYPE	VALUE
DslogdRAT	SHA256	1dd64c00f061425d484dd67b359ad99df533aa430632c55fa7e7617b55dab6a8
Hannibal Stealer	SHA256	f69330c83662ef3dd691f730cc05d9c4439666ef363531417901a86e7c4d31c8

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

May 5, 2025 • 6:00 AM

More at www.hivepro.com