Date of Publication
February 23, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

16 to 22 February 2026

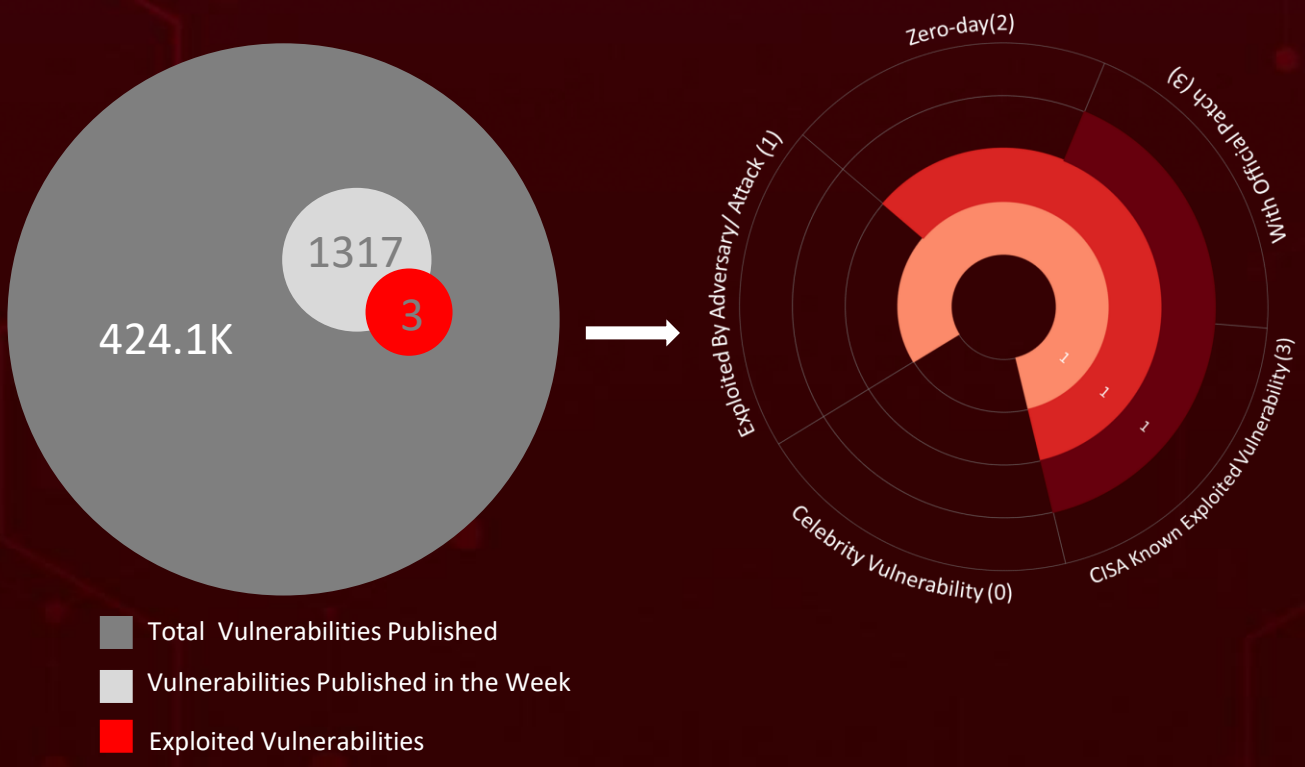
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **thirteen** major attacks were detected, **three** critical vulnerabilities were actively exploited, and **two** threat actors were closely monitored, reflecting an alarming escalation in malicious activities.

CVE-2026-1731 is being actively exploited to achieve unauthenticated RCE against BeyondTrust appliances, posing a critical risk of full remote compromise to exposed, unpatched systems. **CVE-2026-2441** is an actively exploited use-after-free flaw in the Chromium CSS engine, allowing drive-by remote code execution via a malicious webpage, immediate browser updates are critical to mitigate risk.

Meanwhile, A **ClickFix** campaign is deploying Matanbuchus 3.0 to deliver AstarionRAT, enabling stealthy initial access with encrypted C2, credential theft, and proxy capabilities, reinforcing the growing commercialization and sophistication of MaaS-driven intrusions. **UNC6201** exploited **CVE-2026-22769** to gain unauthenticated root access to infrastructure appliances, deploying advanced backdoors and maintaining long-term stealthy persistence aligned with PRC intelligence objectives. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

13
Attacks Executed

3
Vulnerabilities Exploited

2
Adversaries in Action

- WAVESHAPER
- SUGARLOADER
- SILENCELIFT
- HYPERCALL
- DEEPBREATH
- CHROMEPUSH
- Matanbuchus 3.0
- AstarionRAT
- OysterLoader
- BRICKSTORM
- GRIMBOLT
- SLAYSTYLE
- Cuckoo Stealer

- CVE-2026-1731
- CVE-2026-2441
- CVE-2026-22769

- UNC1069
- UNC6201

Insights

ClickFix is spreading Matanbuchus 3.0 and AstarionRAT, enabling stealthy, encrypted remote access and credential theft via MaaS operations.

CVE-2026-2441 enables drive-by RCE in Chromium-based browsers and is actively exploited.

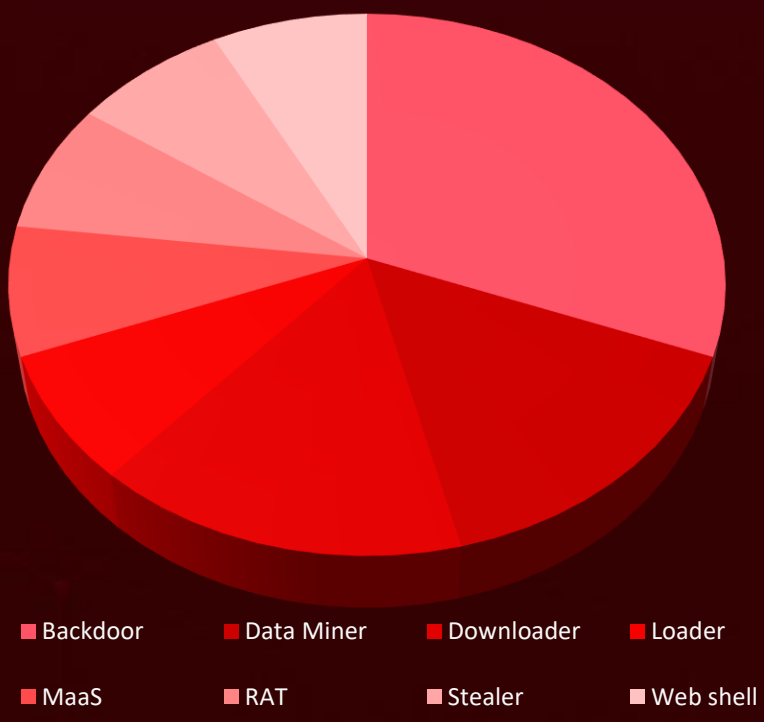
OysterLoader is advancing its obfuscation and signed delivery methods to spread ransomware and stealers via malvertising campaigns.

UNC6201 exploited CVE-2026-22769 for root-level appliance access, deploying custom backdoors for long-term stealth persistence.

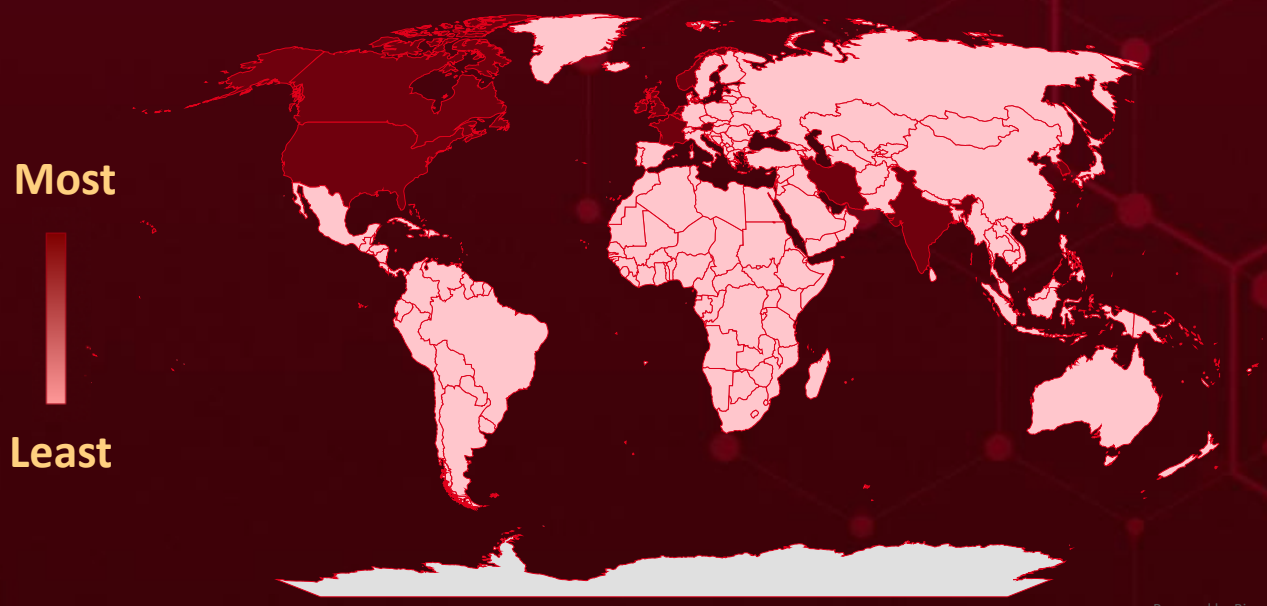
UNC1069 leveraged deepfake video, compromised messaging accounts, and ClickFix social engineering to deploy multi-stage malware for large-scale cryptocurrency theft, highlighting escalating sophistication in DPRK-linked financial targeting.

CRESCENTHARVEST campaign targets Iranian protest supporters through covert social engineering and surveillance operations.

Threat Distribution

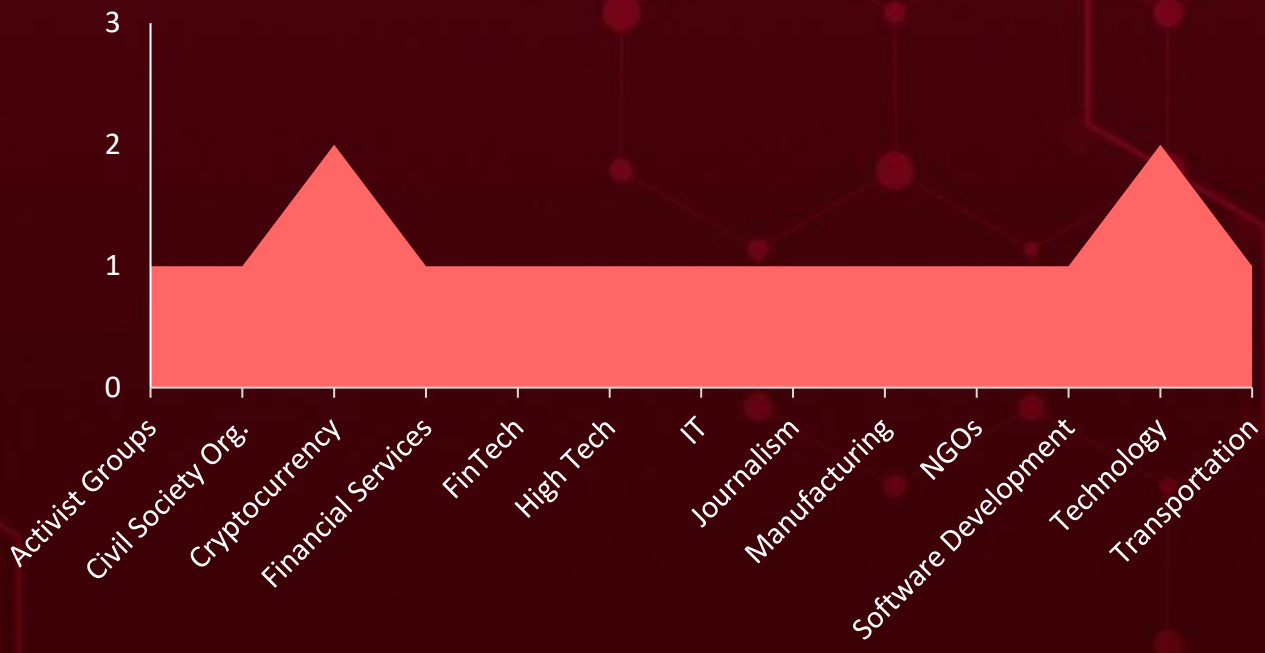


Targeted Countries



Countries	Countries	Countries	Countries
United Kingdom	New Zealand	North Korea	Costa Rica
Iran	Belize	Cabo Verde	Mozambique
United States	Singapore	Paraguay	Côte d'Ivoire
Canada	Benin	Cambodia	Nepal
Austria	Lithuania	Russia	Croatia
Ireland	Bhutan	Cameroon	Niger
Monaco	Montenegro	Senegal	Cuba
Norway	Bolivia	Andorra	Bangladesh
Belgium	Pakistan	Somalia	Cyprus
Israel	Bosnia and Herzegovina	Central African Republic	Panama
Luxembourg	Samoa	Sudan	Czech Republic
France	Botswana	Chad	Philippines
Netherlands	Spain	Timor-Leste	Denmark
India	Brazil	Chile	Republic of Congo
South Korea	Tunisia	Uganda	Djibouti
Portugal	Brunei	China	Saint Kitts & Nevis
Marshall Islands	Malaysia	Madagascar	Dominica
Syria	Bulgaria	Colombia	Sao Tome & Principe
Algeria	Micronesia	Mali	Dominican Republic
Mexico	Burkina Faso	Comoros	Seychelles
	Namibia	Mauritius	DR Congo
	Burundi	Congo	Slovenia
		Bahamas	Ecuador
			Barbados

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1566 Phishing

T1588 Obtain Capabilities

T1071 Application Layer Protocol

T1190 Exploit Public-Facing Application

T1021 Remote Services

T1059.001 PowerShell

T1555 Credentials from Password Stores

T1204 User Execution

T1552 Unsecured Credentials

T1071.001 Web Protocols

T1027 Obfuscated Files or Information

T1078 Valid Accounts

T1083 File and Directory Discovery

T1566.001 Spearphishing Attachment

T1068 Exploitation for Privilege Escalation

T1204.001 Malicious Link

T1588.006 Vulnerabilities

T1041 Exfiltration Over C2 Channel

T1082 System Information Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
WAVESHAPER	WAVESHAPER is a C++ backdoor malware, primarily targeting macOS, used by North Korea-linked UNC1069 in cryptocurrency theft campaigns. It runs as a background daemon, collects system details like username, hardware, and processes, then exfiltrates data via HTTP/HTTPS using curl.	ClickFix	-
		IMPACT	AFFECTED PRODUCT
TYPE		Initial access, Payload delivery, System compromise	macOS
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC1069			-
IOC TYPE	VALUE		
SHA256	b525837273dde06b86b5f93f9aeC2C29665324105b0b66f6df81884754f8080d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SUGARLOADER	SUGARLOADER is a C++-based downloader malware historically linked to North Korean threat actors like UNC1069. It deploys secondary payloads, such as CHROMEPUSH or KANDYKORN, by checking for and decrypting a local config file before connecting to a C2 server.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	AFFECTED PRODUCT
TYPE		Payload Delivery, Persistence	macOS
Downloader			
ASSOCIATED ACTOR			PATCH LINK
UNC1069			-
IOC TYPE	VALUE		
SHA256	1a30d6cdb0b98feed62563be8050db55ae0156ed437701d36a7b46aabf086ede		

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
SILENCELIFT	SILENCELIFT is a minimal C/C++ backdoor newly identified in the UNC1069 intrusion toolkit. Beacons host information and lock-screen status to a hardcoded C2 server. When run with root privileges, it can also interrupt Telegram communications on the host. Represents lightweight persistent access alongside the heavier WAVESHAPER backdoor. New to UNC1069's observed toolset.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Access, Reconnaissance	macOS
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-
IOC TYPE	**VALUE**		
SHA256	c3e5d878a30a6c46e22d1dd2089b32086c91f13f8b9c413aa84e1dbaa03b9375		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HYPERCALL	HYPERCALL is a Golang-based downloader that reads RC4-encrypted configuration and connects to C2 over WebSockets on TCP port 443. Downloads malicious dynamic libraries and reflectively loads them into memory, avoiding disk-based detection. Delivers HIDDENCALL backdoor, SUGARLOADER downloader, and SILENCELIFT beacon during intrusions.	Deployed by WAVESHAPER	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload Delivery	macOS
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-
IOC TYPE	**VALUE**		
SHA256	c8f7608d4e19f6cb03680941bbd09fe969668bcb09c7ca985048a22e014dffcd, 03f00a143b8929585c122d490b6a3895d639c17d92C2223917e3a9ca1b8d30f9		

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
DEEPBREATH	DEEPBREATH is a Swift-based data miner that bypasses macOS Transparency, Consent, and Control (TCC) by staging and modifying the TCC database through Finder's Full Disk Access. Steals iCloud Keychain credentials, browser data from Chrome, Brave, and Edge, Telegram databases, and Apple Notes content. Deployed by HIDDENCALL backdoor as part of UNC1069's credential harvesting toolkit.	Deployed via HYPERCALL (ClickFix chain)	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential theft, Data exfiltration	macOS, Windows
Data Miner			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

IOC TYPE	VALUE
SHA256	b452C2da7c012eda25a1403b3313444b5eb7C2c3e25eee489f1bd256f8434735

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CHROMEPUSH	CHROMEPUSH is a C++ browser stealer that installs itself as a native messaging host disguised as a Google Docs Offline extension targeting Chromium browsers. Logs keystrokes, captures credentials, extracts cookies, and can record screenshots before exfiltrating data via HTTP POST. Deployed exclusively by SUGARLOADER as the final data theft component in the UNC1069 attack chain.	Deployed via SUGARLOADER	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data theft	macOS, Windows
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
UNC1069			-

IOC TYPE	VALUE
SHA256	603848f37ab932dccef98ee27e3c5af9221d3b6ccfe457ccf93cb572495ac325

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
Matanbuchus 3.0	Matanbuchus 3.0 Is a MaaS loader with ChaCha20-encrypted strings, in-memory stealth, LOLBin abuse via regsvr32/rundll32, and CMD/PowerShell reverse shell support. Delivered via DLL sideloading through renamed Notepad++ updater, uses MurmurHash3 for dynamic API resolution and Salsa20-encrypted C2 domains. Deploys ransomware precursors like Cobalt Strike, QakBot, DanaBot, and the new AstarionRAT.	ClickFix, Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
MaaS		Ransomware Staging, Payload Delivery	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	6ffae128e0dbf14c00e35d9ca17c9d6c81743d1fc5f8dd4272a03c66ecc1ad1f, ea378496135318ac5ad667a032fa4a9686add9d27fe4a7c549c937611b5099e5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AstarionRAT	AstarionRAT is a newly discovered full-featured RAT delivered by Matanbuchus 3.0 in a February 2026 ClickFix intrusion. Supports 24 commands covering credential theft, SOCKS5 proxy tunneling, port scanning, in-memory reflective payload execution, and shell access. Uses RSA-encrypted C2 communications disguised as application telemetry. Reached domain controllers in under 40 minutes post-infection.	ClickFix	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote control, Credential theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	eecc83add16f3d513a9701e9a646b1885014229ac6f86addd6b10afb64d1d2af		

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
OysterLoader	OysterLoader is multi-stage C++ loader (aka Broomstick/CleanUp) distributed via fake PuTTY, WinSCP, and Google Authenticator sites as signed MSI installers. Uses TextShell packer for in-memory shellcode loading, custom LZMA decompression, and multiple environment checks before C2 communication. Primarily leads to Rhysida ransomware deployment and also distributes Vidar infostealer.	Fake software websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Loader		Payload delivery, Ransomware deployment	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
URLs	hxxps[:]//grandideapay[.]com/api/v2/facade, hxxp[:]//nucleusgate[.]com/api/v2/facade, hxxps[:]//cardlowestgroup[.]com/api/v2/facade, hxxps[:]//socialcloudguru[.]com/api/v2/facade

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">BRICKSTORM</td><td rowspan="6">BRICKSTORM is a sophisticated Go/Rust-based backdoor targeting VMware vCenter and ESXi hosts, using DNS-over-HTTPS, nested TLS, WebSockets, and SOCKS proxy for stealth C2 and lateral movement. Self-monitoring function automatically reinstalls or restarts if disrupted, with persistence via modified VMware init scripts. Used to steal VM snapshots for credential extraction and create hidden rogue VMs across government and IT sectors.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-22769</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Espionage, Persistent access, Data exfiltration</td><td>Dell RecoverPoint for Virtual Machines</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079</td></tr>
<tr><td>UNC6201</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878,
2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df,
320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759,
90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035,
45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">GRIMBOLT</td><td rowspan="6">GRIMBOLT is a C#-based persistent backdoor compiled using Native Ahead-of-Time (AOT) compilation and packed with UPX, replacing BRICKSTORM since September 2025. Removes CIL metadata that security tools typically scan, optimized for resource-constrained edge devices while maintaining remote shell and WebSocket C2 capabilities. Shares command-and-control infrastructure with its predecessor BRICKSTORM.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-22769</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Espionage, Persistent access, Data exfiltration</td><td>Dell RecoverPoint for Virtual Machines</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079</td></tr>
<tr><td>UNC6201</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c, dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591</td></tr>
<tr><td>IPv4</td><td colspan="3">149[.]248[.]11[.]71</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">SLAYSTYLE</td><td rowspan="6">SLAYSTYLE is a Java-based web shell deployed as a malicious WAR file through Apache Tomcat Manager using hardcoded default admin credentials in Dell RecoverPoint appliances. Grants root-level command execution on compromised systems, serving as the initial foothold before BRICKSTORM and GRIMBOLT deployment. Attackers then implement iptables-based covert channels and create temporary network interfaces for VMware infrastructure pivoting.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-22769</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="4">Data theft</td><td>Dell RecoverPoint for Virtual Machines</td></tr>
<tr><td>Web Shell</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079</td></tr>
<tr><td>UNC6201</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a</td></tr>
</table>

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
Cuckoo Stealer	Cuckoo Stealer is a macOS-specific infostealer and spyware malware active since early 2024, targeting both Intel and Apple Silicon systems via trojanized apps like cleaners and media converters. It steals sensitive data such as Safari credentials, cookies, Keychain passwords, and screenshots, while using obfuscation (XOR-encrypted strings), AppleScript for fake prompts, and Launch Agents for persistence.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Stealer		Data theft	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	545dd5cba264bf242bc837330ca34247e202f7ac25f03eec63bf5842357519f1		

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-2026-1731		BeyondTrust Remote Support: Before 25.3.2 BeyondTrust Privileged Remote Access: Before 25.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:*	-
BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-2441	✗	Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium CSS Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-By Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-22769	✗	Dell RecoverPoint for Virtual Machines (RP4VMs) versions before 6.0.3.1 HF1	UNC6201
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:dell:recoverpoint_for_virtual_machines:*:*:*:*:*:*:*:*	BRICKSTORM, GRIMBOLT, SLAYSTYLE
Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC1069 (alias CryptoCore, MASAN)	North Korea	Cryptocurrency, FinTech, Financial Services, High Tech, Manufacturing, Transportation	United States, Canada, Norway, Austria, Netherlands, United Kingdom, France, Belgium, Ireland, Luxembourg, Monaco, South Korea, India, Israel, Hong Kong
	MOTIVE		
	Financial Gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	WAVESHAPER, SUGARLOADER, SILENCELIFT, HYPERCALL, DEEPBREATH, CHROMEPUSH	macOS, Windows, Telegram, Chromium-Based Browsers (Google Chrome, Brave, Microsoft Edge), Zoom

TTPs
T1566: Phishing, T1566.003: Spearphishing via Service, T1566.004: Spearphishing Voice, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1059.002: AppleScript, T1218: System Binary Proxy Execution, T1218.005: Mshta, T1543: Create or Modify System Process, T1543.004: Launch Daemon, T1176: Browser Extensions, T1027: Obfuscated Files or Information , T1027.002: Software Packing, T1620: Reflective Code Loading, T1036: Masquerading , T1036.005: Match Legitimate Name or Location, T1555: Credentials from Password Stores, T1555.001: Keychain, T1555.003: Credentials from Web Browsers, T1056: Input Capture T1056.001: Keylogging, T1005: Data from Local System, T1185: Browser Session Hijacking, T1074: Data Staged , T1074.001: Local Data Staging , T1041: Exfiltration Over C2 Channel, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1071.004: DNS, T1102: Web Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC6201</td><td>China</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>CVE-2026-22769</td><td>BRICKSTORM, GRIMBOLT, SLAYSTYLE</td><td>Dell RecoverPoint for Virtual Machines</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1190: Exploit Public-Facing Application, T1078: Valid Accounts T1078.001: Default Accounts, T1059: Command and Scripting Interpreter, T1037: Boot or Logon, Initialization Scripts T1037.004: RC Scripts, T1505: Server Software Component , T1505.003: Web Shell, T1027: Obfuscated Files or Information , T1027.002: Software Packing, T1205: Traffic Signaling , T1205.001: Port Knocking, T1021: Remote Services, T1599: Network Boundary Bridging, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1572: Protocol Tunneling, T1068: Exploitation for Privilege Escalation, T1587: Develop Capabilities , T1587.001: Malware, T1588: Obtain Capabilities , T1588.006: Vulnerabilities</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actor **UNC1069, UNC6201** and malware **WAVESHAPER, SUGARLOADER, SILENCELIFT, HYPERCALL, DEEPBREATH, CHROMEPUSH, Matanbuchus 3.0, AstarionRAT, OysterLoader, BRICKSTORM, GRIMBOLT, SLAYSTYLE, Cuckoo 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

- Running a Scan to discover the assets impacted by the **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to malware **WAVESHAPER, SUGARLOADER, Matanbuchus 3.0, AstarionRAT, OysterLoader, BRICKSTORM, GRIMBOLT, SLAYSTYLE, Cuckoo Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2026-1731: Active Exploitation of BeyondTrust WebSocket RCE

Google Chrome CSS Use-After-Free Zero-Day Vulnerability (CVE-2026-2441)

UNC1069's Social Engineering Operations Focused on Crypto Sector

ClickFix to Control: Matanbuchus Campaign Deploys AstarionRAT in Minutes

OysterLoader Threat Model: Silent, Signed, Systematic

CVE-2026-22769: UNC6201 Exploiting Dell RecoverPoint Zero-Day

Fake Homebrew ClickFix Campaign Delivering Cuckoo Stealer on macOS

CRESCENTHARVEST an Espionage Campaign Disguised as Solidarity

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
WAVESHAPER	SHA256	b525837273dde06b86b5f93f9aeC2C29665324105b0b66f6df81884754f8080d
SUGARLOADER	Domain	breakdream[.]com, dreamdie[.]com
	SHA256	1a30d6cdb0b98feed62563be8050db55ae0156ed437701d36a7b46aabf086ede
SILENCELIFT	Domain	support-zoom[.]us
	SHA256	c3e5d878a30a6c46e22d1dd2089b32086c91f13f8b9c413aa84e1dbaa03b9375
HYPERCALL	Domain	supportzm[.]com, zmsupport[.]com
	SHA256	c8f7608d4e19f6cb03680941bbd09fe969668bcb09c7ca985048a22e014dffcd, 03f00a143b8929585c122d490b6a3895d639c17d92C2223917e3a9ca1b8d30f9
DEEPBREATH	SHA256	b452C2da7c012eda25a1403b3313444b5eb7C2c3e25eee489f1bd256f8434735

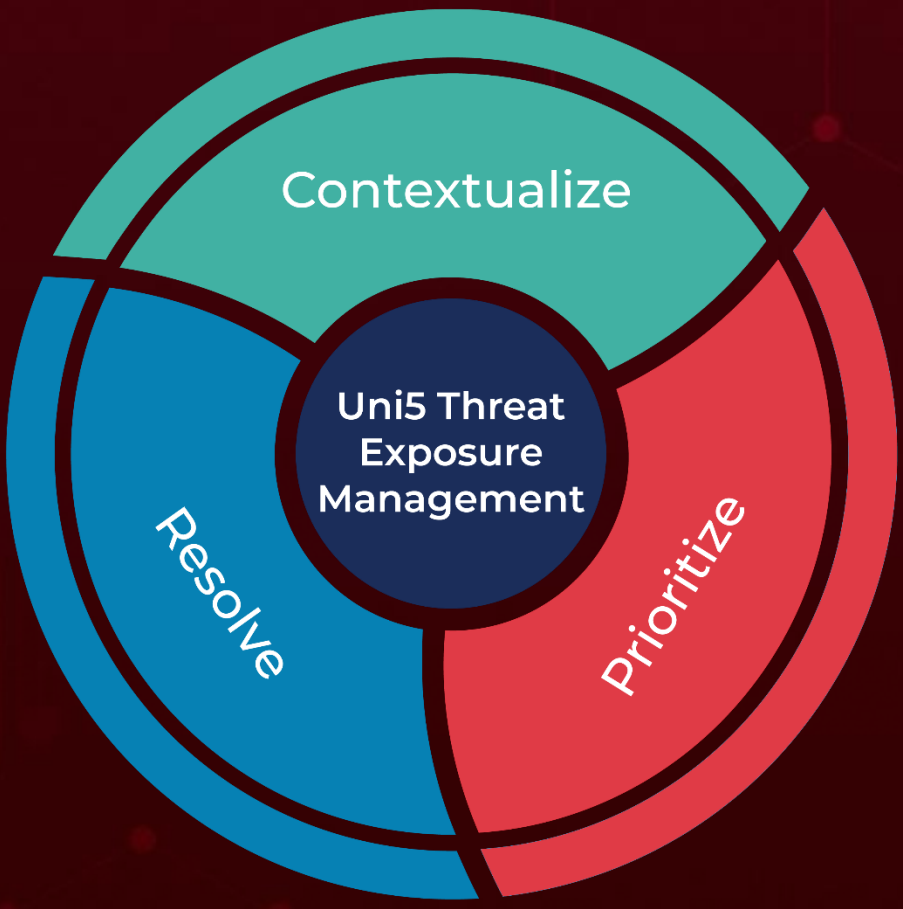
Attack Name	TYPE	VALUE
CHROMEPUSH	Domain	cmailer[.]pro
	SHA256	603848f37ab932dccef98ee27e3c5af9221d3b6ccfe457ccf93cb572495ac325
Matanbuchus 3.0	URL	hxxps[:]//marle[.]io/check/updprofile[.]aspx
	SHA256	6ffae128e0dbf14c00e35d9ca17c9d6c81743d1fc5f8dd4272a03c66ecc1ad1f, ea378496135318ac5ad667a032fa4a9686add9d27fe4a7c549c937611b5099e5
AstarionRAT	Domain	www[.]ndibstersoft[.]com
	SHA256	eecc83add16f3d513a9701e9a646b1885014229ac6f86addd6b10afb64d1d2af
OysterLoader	URLs	hxxps[:]//grandideapay[.]com/api/v2/facade, hxxp[:]//nucleusgate[.]com/api/v2/facade, hxxps[:]//cardlowestgroup[.]com/api/v2/facade, hxxps[:]//socialcloudguru[.]com/api/v2/facade, hxxps[:]//coretether[.]com/api/v2/facade, hxxps[:]//registrywave[.]com/api/v2/facade
BRICKSTORM	SHA256	aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759, 90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830
GRIMBOLT	SHA256	24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c, dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591
	IPv4	149[.]248[.]11[.]71
SLAYSTYLE	SHA256	92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a
Cuckoo Stealer	SHA256	545dd5cba264bf242bc837330ca34247e202f7ac25f03eec63bf5842357519f1

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

February 23, 2026 . 11:30 PM

More at www.hivepro.com