Date of Publication
January 12, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

05 to 11 JANUARY 2026

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 11

Adversaries in Action 13

Recommendations 14

Threat Advisories 15

Appendix 16

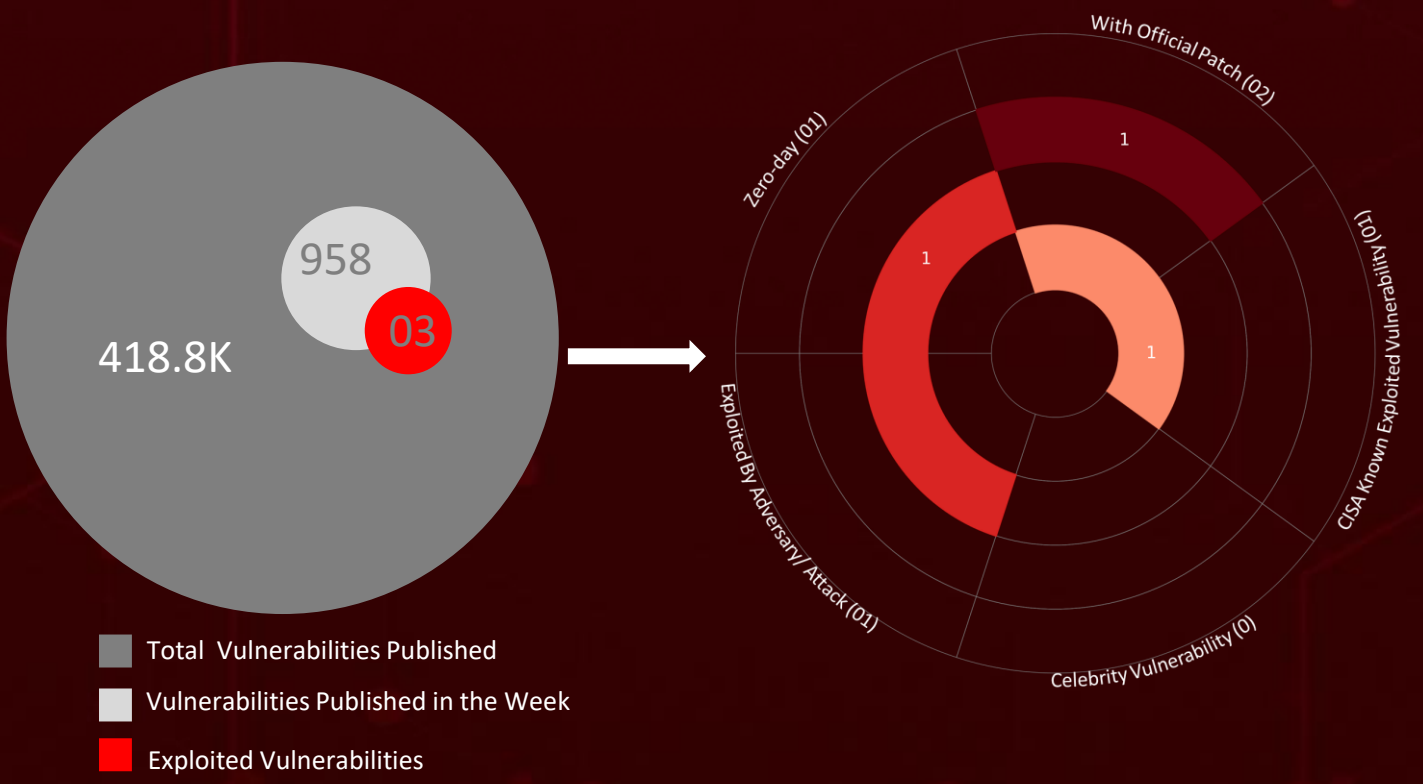
What Next? 17

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **six** major attacks were detected, **three** critical vulnerabilities were publicly disclosed, and **one** active threat actor group was monitored, signaling a concerning escalation in malicious activity.

CVE-2026-0625 is a critical, actively exploited vulnerability in multiple legacy D-Link DSL routers. Exploitation was confirmed in late 2025 and mirrors techniques used in historical **DNSChanger** campaigns. All affected models reached **end-of-life over six years ago** and will not be patched, leaving any remaining deployments permanently exposed. Device replacement is the only viable risk elimination measure.

CVE-2025-37164 is a critical unauthenticated remote code execution flaw in HPE OneView that allows complete compromise of the infrastructure management platform over the network. Recent **APT36** operations demonstrate how minimal user interaction can facilitate persistent, stealthy espionage. The campaign reflects APT36's shift toward more resilient and security-aware intrusion frameworks. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

6
Attacks Executed

3
Vulnerabilities Exploited

1
Adversaries in Action

- VVS Stealer
- DNSChanger
- GhostDNS
- DCRat
- GoBruteforcer
- Astaroth

- CVE-2025-13915
- CVE-2026-0625
- CVE-2025-37164

- APT36

Insights

Click Once, Compromised Forever: APT36's Long-Game Espionage Strategy

Lessons from CVE-2026-0625: Why Router End-of-Life Is a Security Deadline

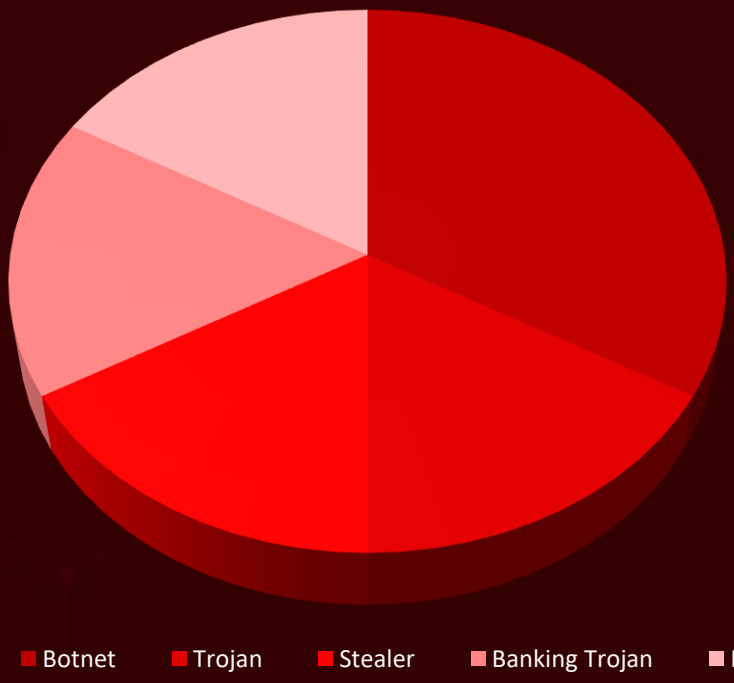
CVE-2025-13915: The IBM API Connect Flaw That Breaks Enterprise Trust

PHALT#BLYX: How **Hospitality** Networks Are Being Breached by Design

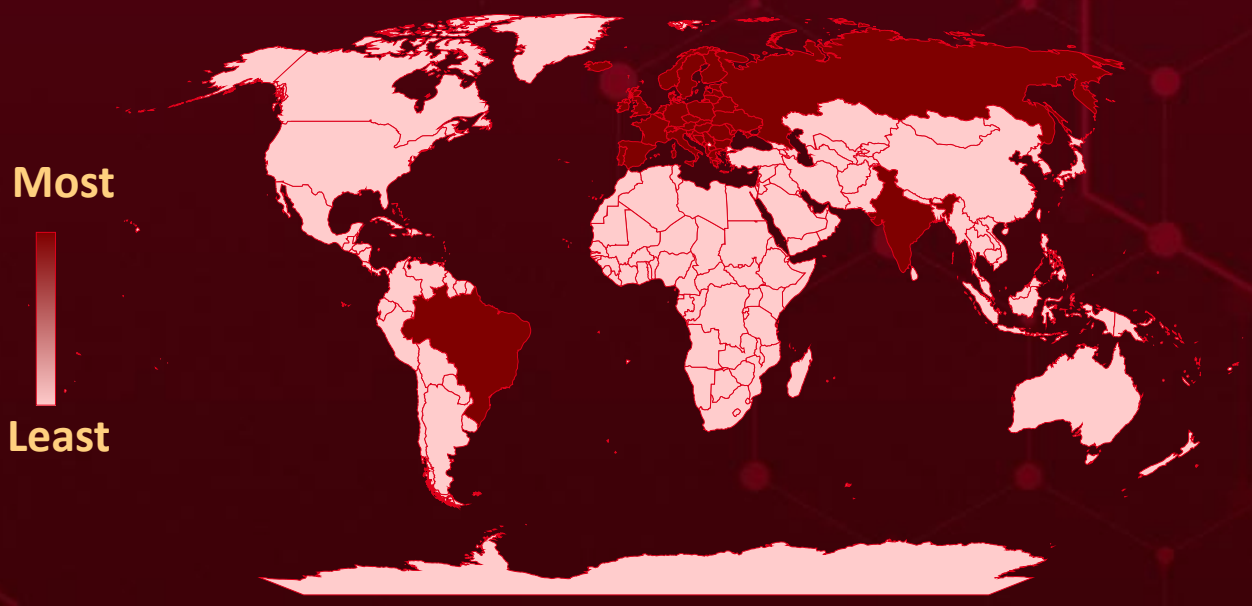
Banking Trojan Goes Social: Inside the **WhatsApp**-Powered **Boto Cor-de-Rosa** Campaign

OneView, Total Control: Inside HPE's **CVE-2025-37164** Critical RCE Exposure

Threat Distribution

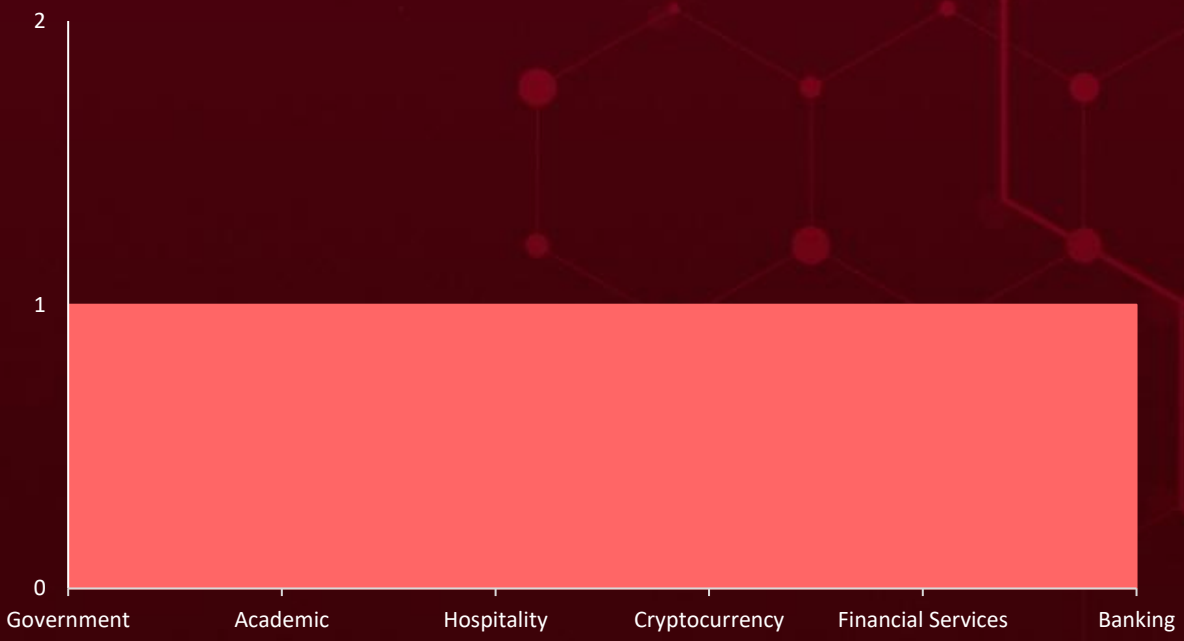


Targeted Countries



Countries	Countries	Countries	Countries
Brazil	Estonia	Saudi Arabia	Angola
India	Monaco	Egypt	North Korea
Denmark	Finland	Palestine	Ghana
United Kingdom	Netherlands	El Salvador	Pakistan
Ukraine	France	Tuvalu	Antigua and Barbuda
North Macedonia	Norway	Equatorial Guinea	
Liechtenstein	Germany	Nepal	Paraguay
Slovakia	Portugal	Eritrea	Grenada
Albania	Greece	Central African Republic	Chile
Moldova	Russia		Guatemala
Andorra	Holy See	Bahrain	Rwanda
Romania	Serbia	Philippines	Guinea
Austria	Hungary	Eswatini	Comoros
Switzerland	Slovenia	Saint Lucia	Guinea-Bissau
Belarus	Iceland	Ethiopia	Congo
Luxembourg	Sweden	Sierra Leone	Guyana
Belgium	Ireland	Fiji	Costa Rica
Montenegro	Italy	South Sudan	Haiti
Bosnia and Herzegovina	Latvia	Bangladesh	South Africa
	Thailand	Cyprus	Belize
Poland	China	Barbados	Sri Lanka
San Marino	Niger	Trinidad and Tobago	Honduras
Bulgaria	Dominica	Gabon	Suriname
Spain	Solomon Islands	Bahamas	Benin
Croatia	Dominican Republic	Gambia	Tajikistan
Czech Republic	DR Congo	Namibia	Bhutan
Lithuania	Panama	Georgia	Togo
Malta	Ecuador	New Zealand	Turkey

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1036** Masquerading	**T1005** Data from Local System	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel	**T1190** Exploit Public-Facing Application	**T1547** Boot or Logon Autostart Execution	**T1095** Non-Application Layer Protocol
T1566 Phishing	**T1059.004** Unix Shell	**T1204** User Execution	**T1059.006** Python	**T1547.001** Registry Run Keys / Startup Folder
T1027.002 Software Packing	**T1082** System Information Discovery	**T1204.002** Malicious File	**T1566.001** Spearphishing Attachment	**T1555** Credentials from Password Stores

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VVS Stealer	VVS Stealer is a Python-based information-stealing malware targeting Discord users to exfiltrate credentials, tokens, and browser data. It uses PyArmor obfuscation to evade static and signature-based detection and is distributed as a PyInstaller executable requiring no external dependencies. Core capabilities include Discord token theft, session hijacking via JavaScript injection, browser credential harvesting, screenshot capture, and persistence through the Windows Startup folder.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Account compromise, Privacy loss, Credential exposure	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	307d9cefa7a3147eb78c69eded273e47c08df44c2004f839548963268d19dd87		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DNSChanger	DNSChanger operates by modifying DNS server settings to redirect systems to attacker-controlled servers instead of legitimate ISP or organizational DNS servers. It is distributed using steganography techniques and, rather than directly infecting the PC, primarily compromises unsecured routers once introduced into the environment.	Exploiting Vulnerability	CVE-2026-0625
TYPE		**IMPACT**	**AFFECTED PLATFORMS**
Trojan		Traffic redirection, Persistent compromise, Surveillance	D-Link DSL-2740R, D-Link DSL-2640B, D-Link DSL-2780B, D-Link DSL-526B
ASSOCIATED ACTOR			**PATCH LINK**
-			EOL

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
GhostDNS	GhostDNS scans for router IP addresses using weak or no passwords, accesses their settings, and replaces the default DNS configuration with attacker-controlled servers.	Exploiting Vulnerability	CVE-2026-0625
		IMPACT	AFFECTED PRODUCTS
TYPE		Network-wide compromise, Credential theft, Service disruption	D-Link DSL-2740R, D-Link DSL-2640B, D-Link DSL-2780B, D-Link DSL-526B
Botnet			PATCH LINK
ASSOCIATED ACTOR			EOL
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DCRat	DCRat is a Russian-linked remote access trojan capable of remote control, keylogging, and process injection, including process hollowing into legitimate binaries such as aspnet_compiler.exe.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Full remote control, Data exfiltration	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			

IOC TYPE	VALUE
SHA256	91696f9b909c479be23440a9e4072dd8c11716f2ad3241607b542b202ab831ce

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
GoBruteforcer	GoBruteforcer is a modular Go-based botnet that compromises Linux servers by brute-forcing weak credentials on internet-exposed services such as FTP, MySQL, PostgreSQL, and phpMyAdmin, spreading through a structured infection chain that includes web shells, downloaders, IRC bots, and dedicated brute-forcer modules.	Brute Force	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Server takeover, Data compromise, Credential theft	Linux
Botnet			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	ab468da7e50e6e73b04b738f636da150d75007f140e468bf75bc95e8592468e5, 4fbea12c44f56d5733494455a0426b25db9f8813992948c5fbb28f38c6367446		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Astaroth (aka Guildma)	Astaroth banking malware has evolved to include WhatsApp-based worm propagation capabilities. This campaign abuses WhatsApp Web to harvest victim contact lists and distribute malicious ZIP archives containing obfuscated Visual Basic Script downloaders. The malware operates with dual functionality: a propagation module that sustains self-reinforcing infection loops through social engineering, and a banking module that silently monitors browsing activity to steal financial credentials when victims access banking URLs.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Banking credential theft, Stealthy persistence	WhatsApp
Banking Trojan			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	bb0f0be3a690b61297984fc01befb8417f72e74b7026c69ef262d82956df471e, 9081b50af5430c1bf5e84049709840c40fc5fdd4bb3e21eca433739c26018b2e		

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-13915</td><td>  </td><td rowspan="2">IBM API Connect V10.0.8.0 - V10.0.8.5, V10.0.11.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ibm:api_connect:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">IBM API Connect Authentication Bypass Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-305</td><td>T1556: Modify Authentication Process, T1136: Create Account, T1190: Exploit Public-Facing Application</td><td>https://www.ibm.com/support/pages/node/7255149</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-0625	✗	D-Link DSL-526B (versions <= 2.01), D-Link DSL-2640B (versions <= 1.07), D-Link DSL-2740R (versions < 1.17), D-Link DSL-2780B (versions <= 1.01.14)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:dlink:dsl:*:*:*:*:*:*:*:*	DNSChanger, GhostDNS
D-Link DSL Gateway Command Injection via DNS Configuration Endpoint Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584.002: DNS Server	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-37164	✗	HPE OneView (Before 11.0)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:hpe:oneview:*:*:*:*:*:*:*:*	-
Hewlett Packard Enterprise OneView Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US, https://myenterpriselicense.hpe.com/cwp-ui/product-details/HPE_OV_CVE_37164_Z7550-98077/-/sw_free, https://support.hpe.com/connect/s/softwaredetails?collectionId=MTX-64daeb5ed0df44a0&tab=releaseNotes

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT36 (aka Transparent Tribe, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134)	Pakistan	Government, Academic	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1112: Modify Registry; T1055: Process Injection; T1036: Masquerading; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1202: Indirect Command Execution; T1497: Virtualization/Sandbox Evasion; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1555: Credentials from Password Stores; T1539: Steal Web Session Cookie; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1113: Screen Capture; T1115: Clipboard Data; T1005: Data from Local System; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1565.001: Stored Data Manipulation; T1047: Windows Management Instrumentation

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploitable vulnerabilities** and block the indicators related to the threat actor **APT36,** and malware **VVS Stealer, DNSChanger, GhostDNS, DCRat, GoBruteforcer, and Astaroth.**

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 **three exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT36,** and malware **VVS Stealer, DCRat, and Astaroth** in Breach and Attack Simulation(BAS).

Threat Advisories

Silent Clicks, Lasting Access: APT36's Fileless Espionage Playbook

VVS Stealer Exposed: Inside a Stealthy Discord Credential Theft Operation

CVE-2025-13915: Authentication Bypass Puts IBM API Connect at Risk

CVE-2026-0625: A Decade-Long Risk in D-Link DSL Routers Enabling Full System Compromise

PHALT#BLYX: Fake BSOD Campaign Targets Hospitality

GoBruteforcer Exposed: How Weak Credentials Power a Silent Linux Botnet

Astaroth Reimagined: Weaponizing WhatsApp for Scalable Banking Fraud

CVE-2025-37164: Critical RCE in HPE OneView Under Active Exploitation

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)

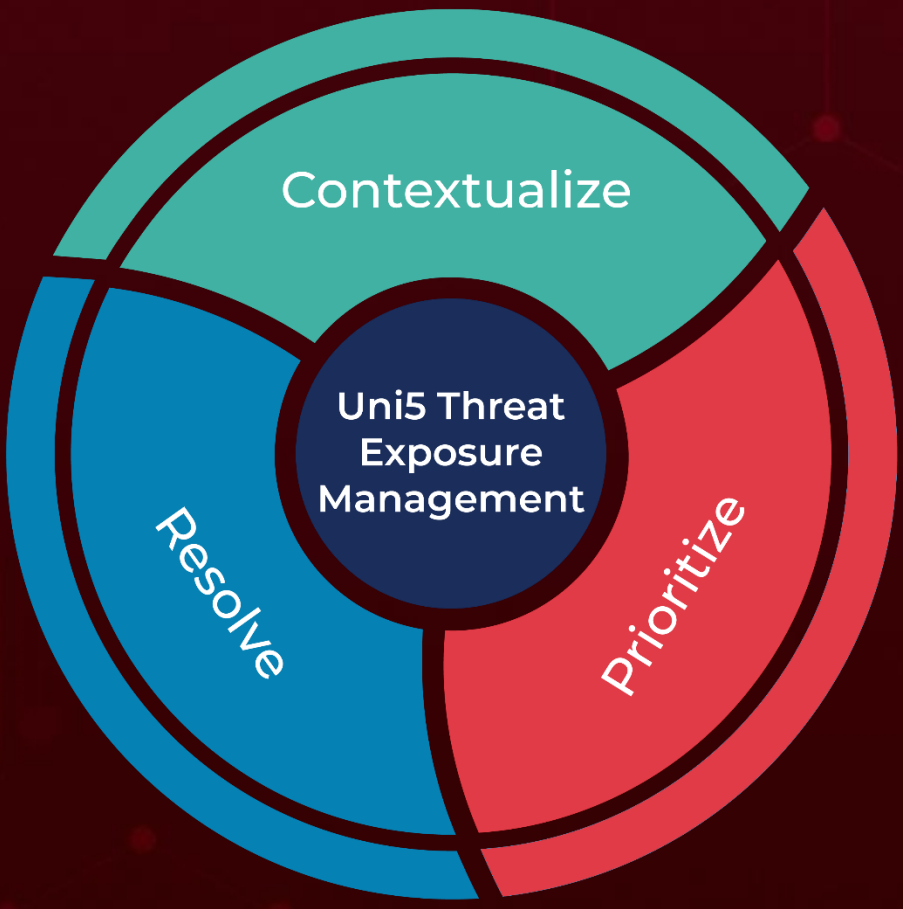
Attack Name	TYPE	VALUE
VVS Stealer	SHA256	307d9cefa7a3147eb78c69eded273e47c08df44c2004f839548963268d19dd87, 7a1554383345f31f3482ba3729c1126af7c1d9376abb07ad3ee189660c166a2b, c7e6591e5e021daa30f949a6f6e0699ef2935d2d7c06ea006e3b201c52666e07
DCRat	SHA256	91696f9b909c479be23440a9e4072dd8c11716f2ad3241607b542b202ab831ce, bf374d8e2a37ff28b4dc9338b45bbf396b8bf088449d05f00aba3c39c54a3731, 11c1cfce546980287e7d3440033191844b5e5e321052d685f4c9ee49937fa688
GoBruteforcer	SHA256	ab468da7e50e6e73b04b738f636da150d75007f140e468bf75bc95e8592468e5, 4fbea12c44f56d5733494455a0426b25db9f8813992948c5fbb28f38c6367446
Astaroth	SHA256	bb0f0be3a690b61297984fc01befb8417f72e74b7026c69ef262d82956df471e, 9081b50af5430c1bf5e84049709840c40fc5fdd4bb3e21eca433739c26018b2e

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

January 12, 2026 • 9:00 AM

More at www.hivepro.com