Date of Publication
January 27, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

19 to 25 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 10

Adversaries in Action 12

Recommendations 13

Threat Advisories 14

Appendix 15

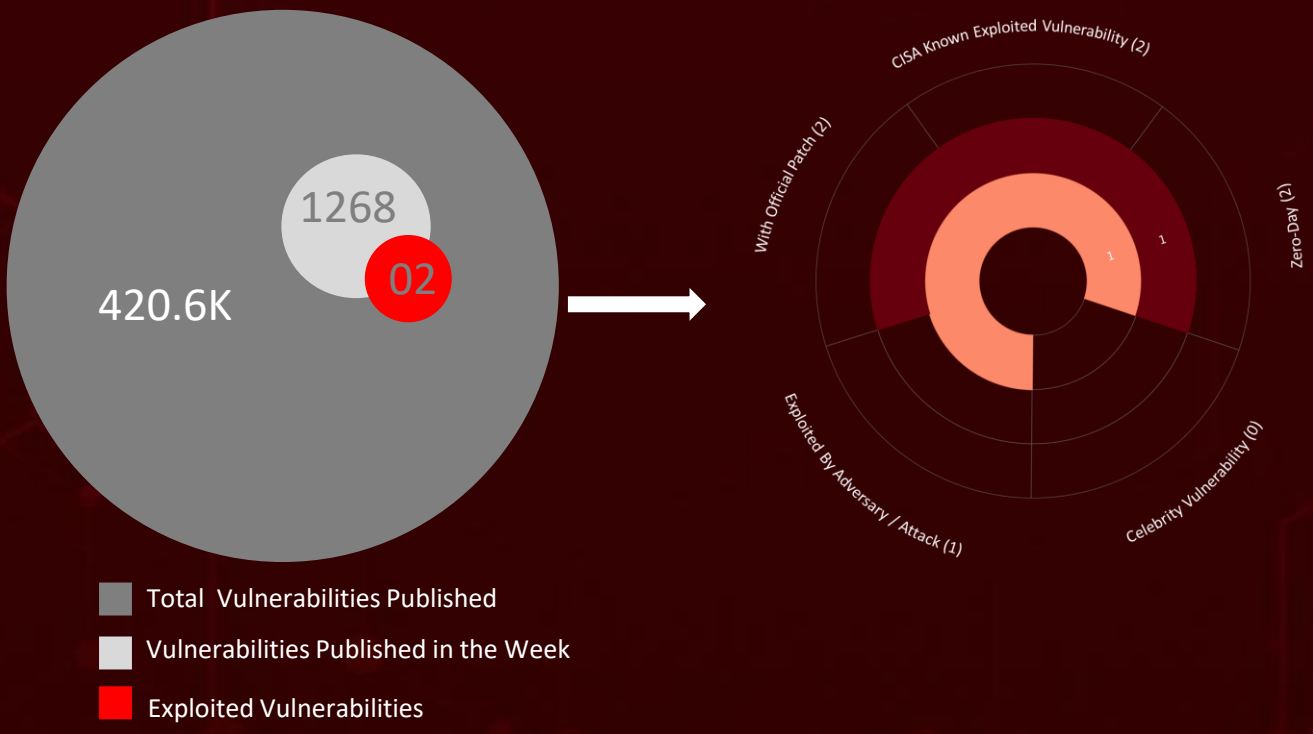
What Next? 16

Summary

HiveForce Labs has flagged a worrying surge in cyber activity, underscoring how global threats are growing both faster and more complex. In the past week, we tracked **three** significant attacks alongside **two** critical vulnerabilities, clear signs that adversaries are accelerating their operations and expanding their reach across sectors and regions.

At the vulnerability level, Cisco environments have come under strain. **CVE-2026-20045** exposes multiple Cisco Unified Communications products to unauthenticated remote code execution through flawed input validation, with active exploitation already observed against internet-facing systems to gain OS-level access. Even more severe, **CVE-2025-20393** is a CVSS 10.0 zero-day in Cisco AsyncOS affecting Secure Email Gateway and management appliances, enabling attackers to execute commands as root via the Spam Quarantine interface. This flaw has been exploited since late November 2025; Cisco released patches on January 15, 2026, and urged immediate upgrades.

Beyond vulnerabilities, several highly orchestrated attack campaigns reveal how threat actors are abusing trust rather than code. One espionage operation leverages U.S.-Venezuela political tensions to deliver the stealthy **LOTUSLITE** backdoor via DLL sideloading, while other targets are developers through trojanized Visual Studio Code extensions to deploy the **Evelyn Stealer**. A separate multi-stage campaign shows how complete system compromise can be achieved without a single exploit using social engineering, cloud-hosted payloads, Defender abuse via Defendnot, and ultimately **Amnesia RAT** for long-term surveillance and data theft before ransomware locks victims out. Taken together, these developments reinforce a simple reality: rapid patching, continuous visibility, and layered defenses are no longer optional in an increasingly aggressive threat landscape.



High Level Statistics

3
Attacks Executed

2
Vulnerabilities Exploited

0
Adversaries in Action

- LOTUSLITE
- Evelyn Stealer
- Amnesia RAT
- CVE-2026-20045
- CVE-2025-20393

Insights

LOTUSLITE slips in via DLL sideloading, camouflaging itself inside legitimate software to avoid suspicion.

CVE-2026-20045 Cisco RCE Flaw: Active exploitation is already targeting internet-facing deployments in the wild.

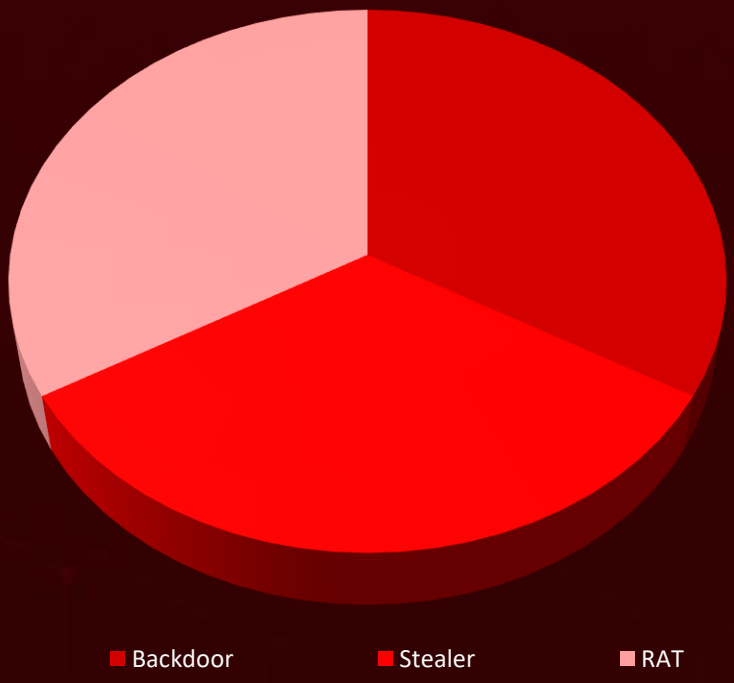
Chrome extensions masquerading as HR and ERP tools quietly undermine platforms like Workday and NetSuite.

Data first, damage later: **Amnesia RAT** prepares the ground before unleashing ransomware and system-locking payloads.

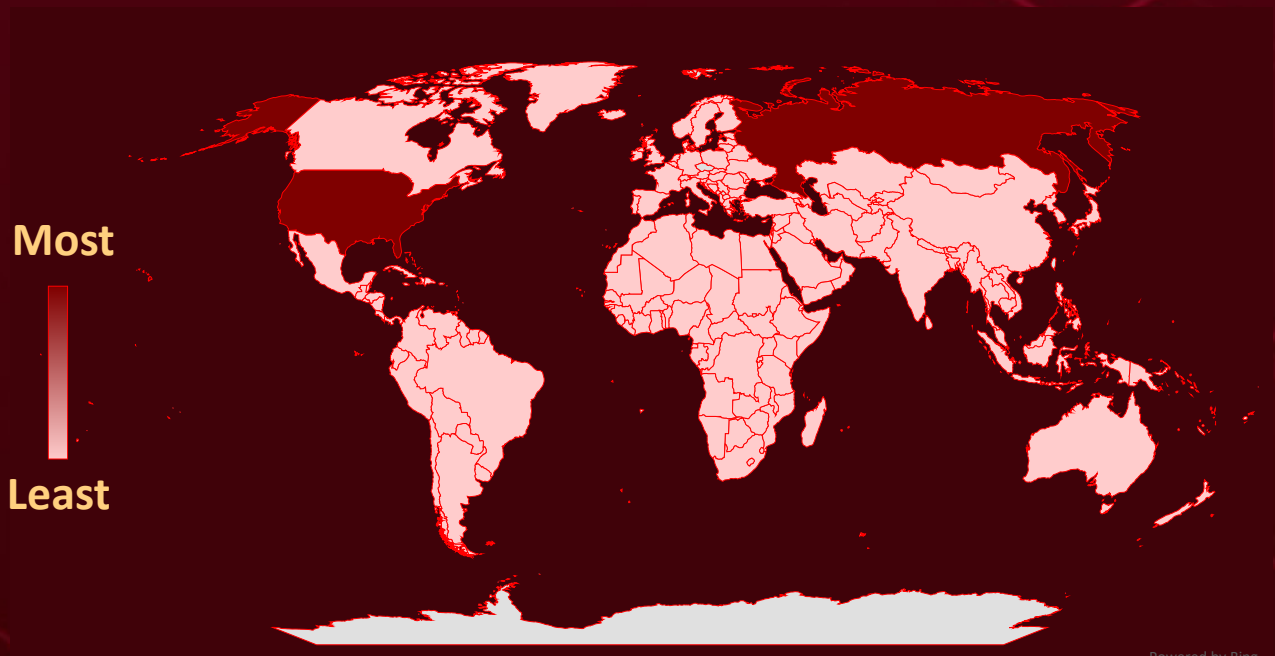
CVE-2025-20393 demands immediate patching: Cisco's January 15, 2026, fixes are critical to stopping in-the-wild exploitation.

Trojanized VS Code add-ons act as the initial delivery vector for the **Evelyn Stealer.**

Threat Distribution



Targeted Countries



Countries	Countries	Countries	Countries
Russia	Bangladesh	Singapore	United Arab Emirates
United States	Mauritius	India	United Kingdom
Norway	Barbados	Slovenia	Uruguay
Afghanistan	Mozambique	Indonesia	Laos
South Sudan	Belarus	Somalia	Uzbekistan
Andorra	Niger	Iran	Latvia
Monaco	Belgium	South Korea	Venezuela
Angola	Panama	Iraq	Lebanon
Saint Lucia	Belize	Spain	Yemen
Antigua and Barbuda	Romania	Ireland	Lesotho
Trinidad and Tobago	Benin	St. Vincent & Grenadines	Zimbabwe
Argentina	Saudi Arabia	Israel	Liberia
Mali	Bhutan	Sudan	Libya
Armenia	Solomon Islands	Italy	Pakistan
Nepal	Bolivia	Sweden	Chad
Australia	State of Palestine	Jamaica	Paraguay
Philippines	Bosnia and Herzegovina	Syria	Chile
Austria	Thailand	Japan	Portugal
Sierra Leone	Botswana	Tanzania	China
Azerbaijan	Tuvalu	Jordan	Rwanda
Switzerland	Brazil	Timor-Leste	Colombia
Bahamas	Vietnam	Kazakhstan	San Marino
Algeria	Brunei	Tonga	Comoros
Bahrain	Lithuania	Kenya	Serbia
Madagascar	Bulgaria	Tunisia	

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1071
Application Layer Protocol

T1071.001
Web Protocols

T1027
Obfuscated Files or Information

T1041
Exfiltration Over C2 Channel

T1566
Phishing

T1059.001
PowerShell

T1547
Boot or Logon Autostart Execution

T1588.006
Vulnerabilities

T1068
Exploitation for Privilege Escalation

T1555
Credentials from Password Stores

T1057
Process Discovery

T1588
Obtain Capabilities

T1036
Masquerading

T1539
Steal Web Session Cookie

T1562.001
Disable or Modify Tools

T1547.001
Registry Run Keys / Startup Folder

T1566.001
Spearphishing Attachment

T1562
Impair Defenses

T1574.001
DLL

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSLITE	LOTUSLITE is a C++ backdoor designed for covert espionage operations, communicating with a hard-coded, IP-based command-and-control server to receive instructions and exfiltrate collected data. While its functionality remains deliberately minimal, it supports essential remote tasking and data theft capabilities, complemented by a reliable persistence mechanism that allows it to survive system reboots.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft, System Compromise	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	2c34b47ee7d271326cfff9701377277b05ec4654753b31c89be622e80d225250		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Evelyn Stealer	Evelyn Stealer is a data-harvesting malware tailored to siphon sensitive information from developer environments, with a particular focus on credentials and cryptocurrency-related assets. Once deployed, it gathers detailed system information and abuses DLL injection to extract browser-stored credentials, while also stealing files, clipboard contents, and saved Wi-Fi credentials. The malware further expands its capabilities by capturing screenshots and targeting cryptocurrency wallets, enabling comprehensive data theft, with all stolen data exfiltrated to attacker-controlled infrastructure over FTP.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Steal Data	Windows
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	aba7133f975a0788dd2728b4bbb1d7d948e50571a033a1e8f47a2691e98600c5		

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">Amnesia RAT</td><td rowspan="6">Amnesia RAT is a multifunctional remote access trojan designed for large-scale data theft and sustained system surveillance. It targets browser credentials and active sessions, Telegram Desktop accounts, seed phrases exposed via files or clipboard activity, application data from platforms such as Discord and Steam, and cryptocurrency wallets and financial assets. In parallel, the malware gathers system intelligence and enables real-time monitoring through screen, audio, and activity capture, while also supporting process control and strong persistence. This combination of credential theft, session hijacking, financial targeting, and continuous surveillance allows attackers to achieve full account takeover, identity abuse, and launch follow-on compromise campaigns.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="3">System Compromise</td><td rowspan="2">Microsoft Windows</td></tr>
<tr><td>RAT</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">359fe8df31c903153667fbe93795929ad6172540b3ee7f9eff4bcc1da6d08478</td></tr>
</table>

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 PRODUCT	ASSOCIATED ACTORS
CVE-2026-20045	✗	Cisco Unified Communications Manager, Unified Communications Manager Session Management Edition, Unified Communications Manager IM & Presence Service, Unity Connection, Webex Calling Dedicated Instance: versions before 14SU5, 15SU4	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:unified_communications_manager_im_and_presence_service:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:unity_connection:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:webex_calling_dedicated_instance:*:*:*:*:*:*:*:*	-
Cisco Unified Communications Products Code Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20393		Cisco Secure Email Gateway (SEG): Versions prior to 15.0.5-016, 15.5.4-012, 16.0.4-016 Cisco Secure Email and Web Manager (SEWM): Versions prior to 15.0.2-007, 15.5.4-007, 16.0.4-010	UAT-9686
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:secure_email_and_web_manager_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_and_web_manager:-:*:*:*:*:*:*:* cpe:2.3:h:cisco:secure_email_gateway:-:*:*:*:*:*:*:* cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*:*	AquaShell, AquaTunnel, AquaPurge, and Chisel
Cisco Multiple Products Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4

Adversaries in Action

No Active Adversaries this week.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploitable vulnerabilities** and block the indicators related to the threat actor and malware **LOTUSLITE, Evelyn Stealer,** and **Amnesia RAT.**

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 **two exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors and malware **LOTUSLITE, Evelyn Stealer,** and **Amnesia RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Geopolitics as Bait: LOTUSLITE Backdoor Targets U.S. Entities

Malicious Chrome Extensions Hijacking Enterprise HR Platforms

Evelyn Stealer’s Stealth Campaign Against Developers

CVE-2026-20045: Critical Cisco Unified Communications Actively Exploited

A Stealthy Campaign Blending RAT, Ransomware, and Cloud Infrastructure

CVE-2025-20393: Critical Cisco AsyncOS Zero-Day Actively Exploited

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)

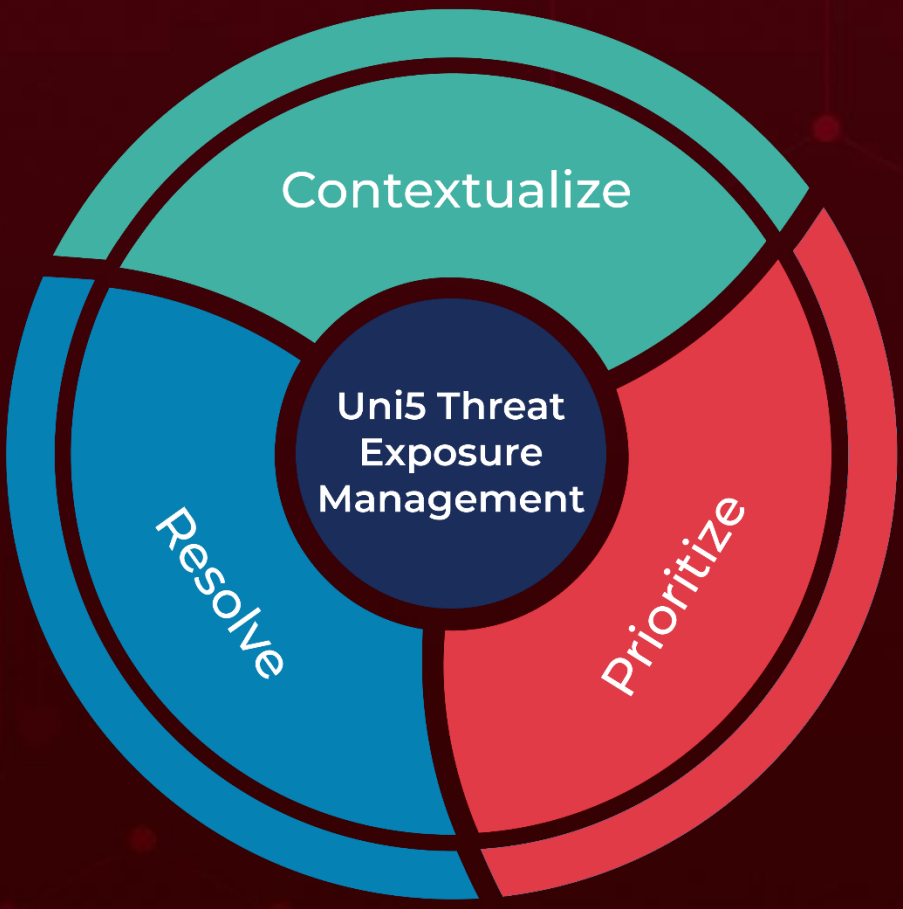
Attack Name	TYPE	VALUE
LOTUSLITE	SHA256	2c34b47ee7d271326cfff9701377277b05ec4654753b31c89be622e80d225250
Evelyn Stealer	SHA256	aba7133f975a0788dd2728b4bbb1d7d948e50571a033a1e8f47a2691e98600c5, 92af258d13494f208ccf76f53a36f288060543f02ed438531e0675b85da00430
Amnesia	SHA256	359fe8df31c903153667fbe93795929ad6172540b3ee7f9eff4bcc1da6d08478

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 27, 2026 . 7:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com