Date of Publication
November 9, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

02 to 08 NOVEMBER 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 12

Adversaries in Action 19

Recommendations 22

Threat Advisories 23

Appendix 24

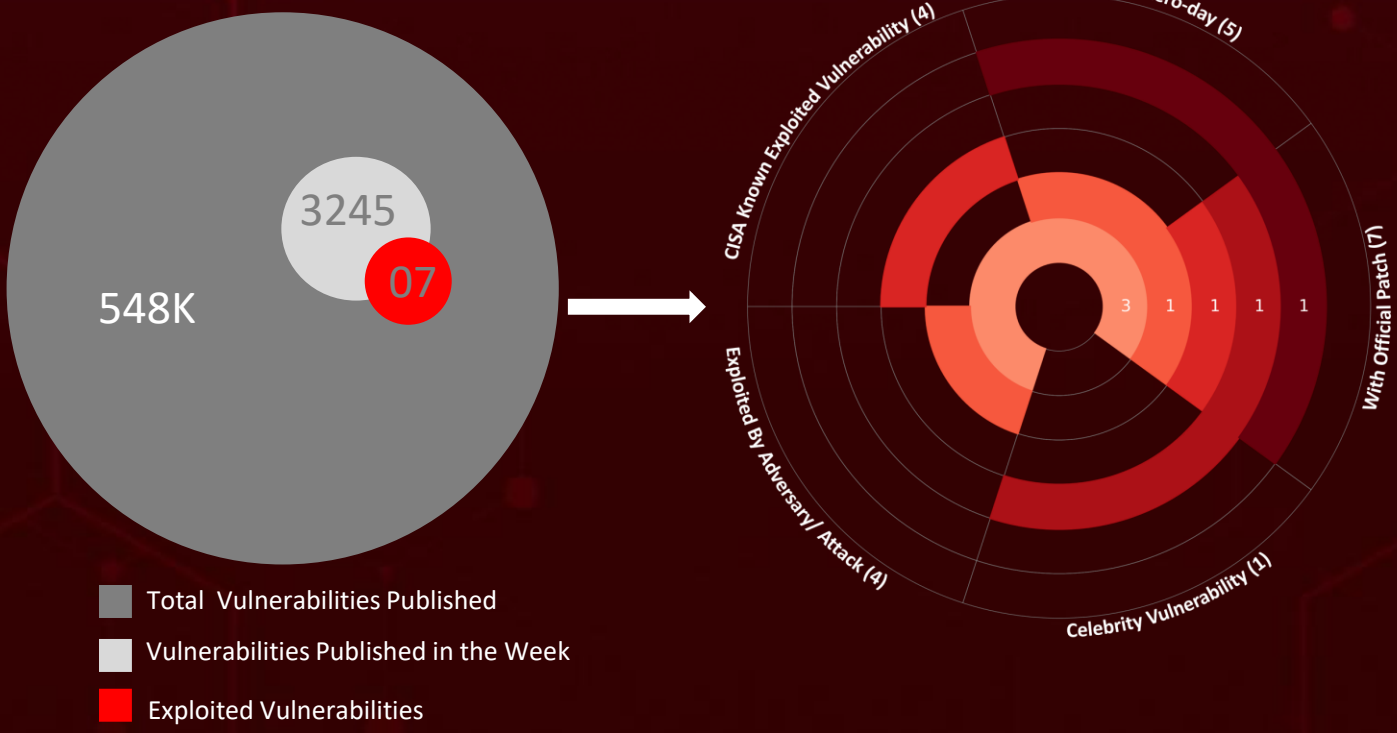
What Next? 25

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **four** major attacks were detected, **seven** vulnerabilities were actively exploited, and **three** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Ivanti patched **three chained zero-days in Connect Secure** that together give unauthenticated attackers root on fully updated appliances; the previously unknown actor UTA0576 exploited the chain while blending into ordinary HTTPS traffic. A separate authentication bypass in **Alpine Linux** lets network attackers open an interactive shell as a legitimate user, with official tiny-cloud images escalating straight to root and exposure stretching across containers, CI runners, IoT devices and other musl-based platforms.

On the espionage front, Russia-aligned **Gorbag** is phishing Ukrainian government, defense and transport organizations with tax, conscription and drone-procurement lures, exploiting WinRAR flaw **CVE-2025-8088** to drop **Prime ReverseShell and BeautyStealer** in grab-and-go raids that hint at access brokering for other Russian groups. China-aligned **SlippyNunchucks** took a quieter route, hijacking DNS so that Sogou Input Method's plain-HTTP update check silently loaded the **DarkVigil backdoor**. Rounding out the week, **3AM ransomware** struck a UK school estate, harvesting credentials from backup servers and domain controllers and planting backdoor domain admins ahead of double extortion. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

4
Attacks Executed

7
Vulnerabilities Exploited

3
Adversaries in Action

- DarkVigil
- 3AM Ransomware
- Prime ReverseShell
- BeautyStealer

- CVE-2026-111357
- CVE-2026-118527
- CVE-2026-118539
- CVE-2026-119977
- CVE-2025-8088
- CVE-2026-120422
- CVE-2026-123158

- UTA0576
- Gorbag
- SlippyNunchucks

Insights

Ivanti Connect Secure Zero-Day Trio Gave Unauthenticated Attackers Root Access

No Account Needed: CVE-2026-118539 Exposes Drupal Online Stores to Unauthorized Access

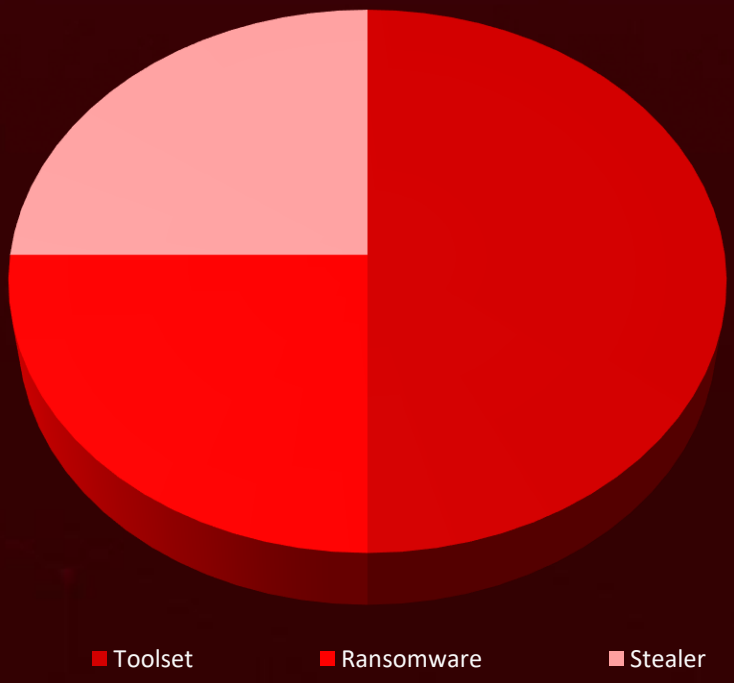
One Long Password to Rule Them All: sshole Alpine Flaw Lets Attackers Skip SSH Authentication

62,969 Attacks in 24 Hours: WordPress Core RCE Flaw CVE-2026-119977 Under Heavy Fire

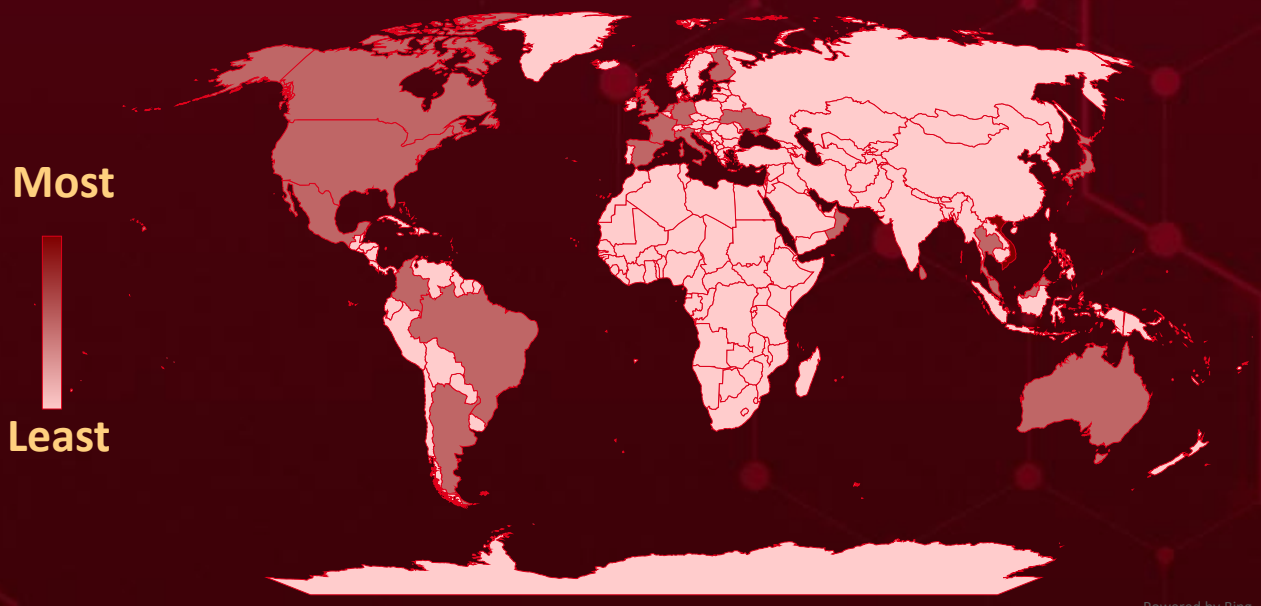
Gorbag Strikes Ukraine: Russia-Aligned Spies Weaponize WinRAR Flaw Against Border Agencies

From LockBit Backup Plan to Main Event: 3AM Ransomware Strikes UK Schools

Threat Distribution



Targeted Countries



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

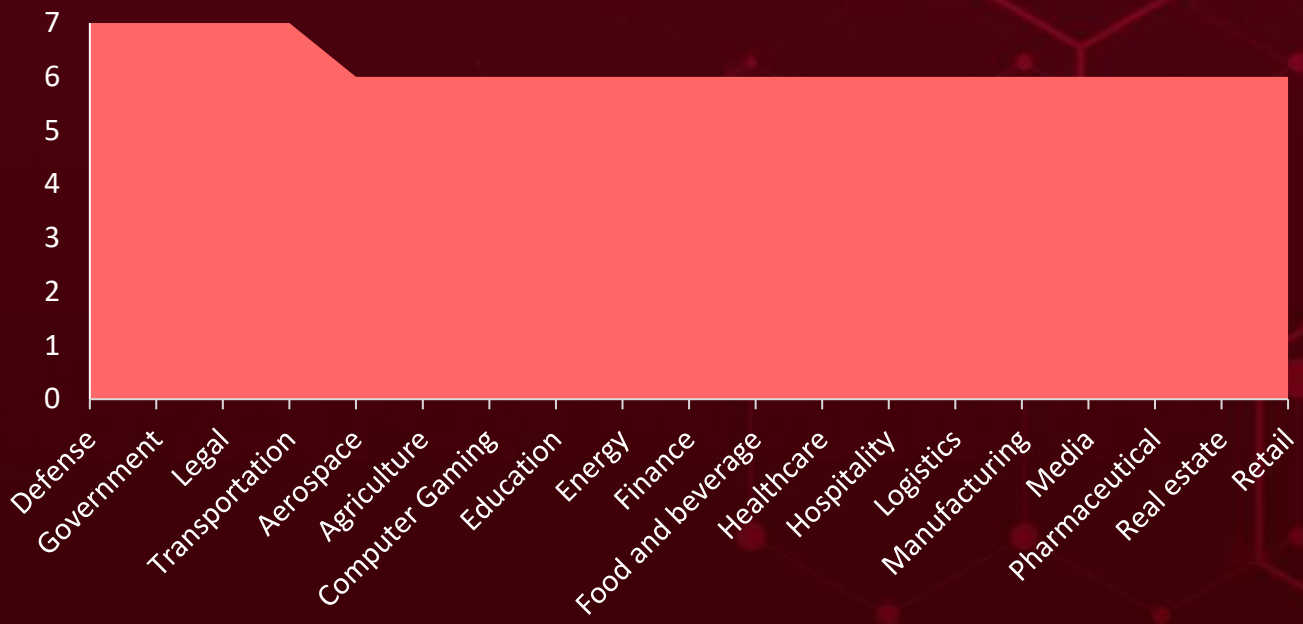
Countries
Vietnam
Oman
Luxembourg
Thailand
Australia
Mexico
Brazil
Spain
Canada
Argentina
United Kingdom
Colombia
Malaysia
Croatia
Netherlands
Finland
Singapore
France
Sri Lanka
Germany
Ukraine
Hong Kong
United States
Italy
Japan

Countries
Lebanon
Pakistan
Vanuatu
South Africa
Myanmar
Algeria
Togo
Bahamas
Brunei
Niger
Bulgaria
Portugal
Burkina Faso
Scotland
Burundi
Switzerland
Cambodia
Uganda
Cameroon
Romania
Chad
Chile
Sierra Leone
China
Sudan
Andorra
Tanzania

Countries
Comoros
Tunisia
Bhutan
Costa Rica
Zambia
Angola
Mauritania
Cuba
Monaco
Curacao
Morocco
Cyprus
Nauru
Czech Republic
New Zealand
North Korea
Denmark
Norway
Djibouti
Panama
Dominica
Philippines
Dominican Republic
Qatar
Ecuador
Rwanda

Countries
Egypt
Saint Lucia
El Salvador
San Marino
Equatorial Guinea
Serbia
Estonia
Slovakia
Ethiopia
Belarus
Faroe Islands
Swaziland
Fiji
Taiwan
Anguilla
Tibet
Antigua and Barbuda
Tonga
French Guiana
Turkmenistan
Gabon
United Arab Emirates

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1071** Application Layer Protocol	**T1036** Masquerading	**T1036.005** Match Legitimate Name or Location
T1140 Deobfuscate/ Decode Files or Information	**T1027** Obfuscated Files or Information	**T1071.001** Web Protocols	**T1560** Archive Collected Data	**T1041** Exfiltration Over C2 Channel
T1588 Obtain Capabilities	**T1564** Hide Artifacts	**T1070** Indicator Removal	**T1083** File and Directory Discovery	**T1005** Data from Local System
T1583 Acquire Infrastructure	**T1098** Account Manipulation	**T1074** Data Staged	**T1078** Valid Accounts	**T1555** Credentials from Password Stores

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DarkVigil	DarkVigil (also known as FDMTP) is a modular toolset written in .NET. It has the main DarkVigil implant plus more than 20 known plugins that add extra features. It is built on the Vigil malware framework, which in turn uses the TouchSocket networking framework. For command-and-control, it uses DMTP, a network protocol that comes with TouchSocket. Stolen data is managed through a web admin panel that is also called Vigil.	-	CVE-2026-120422
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Toolset		Remote access and data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
SlippyNunchucks			https://pinyin.sogou.com/changelog.php

IOC TYPE	VALUE
SHA1	8A60A8E90E1F5F08F28FE5A6DD57BD686C20DC23 3E16BA611782AF6E45576D390488D28FD676BADE

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
3AM Ransomware	3AM (ThreeAM) is a Rust-based ransomware-as-a-service operation active since February 2023. In September 2026, an affiliate breached a UK school estate, stole backup and domain credentials, built rogue two-way trusts between separate domains, exfiltrated finance data and encrypted about 37 machines. The commands suggest a human operator directing an AI agentic loop.	-	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Ransomware		Credential theft, data exfiltration, data encryption, backup deletion	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	882f34f27292dd797fc022eeac28dfb070d408d310f4e9be20a2a0cb1e78620d		

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
Prime ReverseShell	A PowerShell reverse shell built from the public GitHub project PSSW100AVB and packed into a .NET binary with PS2EXE; it runs operator commands and sends the output back to its C&C server over HTTPS.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Toolset		Remote access, data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Gorbag			-
IOC TYPE	**VALUE**		
SHA256	78ea83bfbca85a39e59fa35c8f704873f3fdad3a5278430e75286247530042b8		

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
BeautyStealer	A C++ stealer that takes cookies, saved passwords and local-state data from Chrome, Edge, Opera and Firefox, plus documents, archives, emails, VPN configs and credential files (.ovpn, .kdbx, .rdp, .pfx and others); it sends them to Telegram or, from v1.2, to a FastAPI C&C server, with XOR string encryption in v1.2 and RC4 for stolen data in v2.0, and deletes itself afterwards.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Stealer		Credential theft, data exfiltration	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Gorbag			-
IOC TYPE	**VALUE**		
SHA256	9ce0f41d6e575aca81d290b3d0b89b011da4f9b87276b27d1c7de81695d4c927		

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-2026-111357</td><td></td><td rowspan="2">Ivanti Connect Secure before version 25.1.1.3, and 22.8R2.6</td><td rowspan="2">UTA0576</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:ivanti:connect_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306, CWE-862, CWE-345</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-118527		Ivanti Connect Secure before versions 25.1.1.3 and 22.8R2.6	UTA0576
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-340	T1190: Exploit Public-Facing Application	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-118539		Drupal Commerce Core versions: from 0.0.0 to 2.41, from 3.0.0 to 3.3.13.	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:drupal:commerce_core:*:*:*:*:*:*:*:*	-
Drupal Commerce Core Access Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-862	T1190: Exploit Public-Facing Application, T1213: Data from Information Repositories	https://www.drupal.org/sa-contrib-2026-254

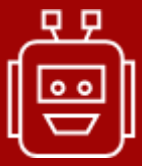
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-119977		WordPress WordPress Core (versions 4.7 through 7.1.3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	-
WordPress WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-367	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8088	 ZERO-DAY	WinRAR versions prior to 7.13	Gorbag
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Prime ReverseShell, BeautyStealer
RARLAB WinRAR Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	T1566: Phishing, T1204: User Execution, T1059: Command and Scripting Interpreter, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1071: Application Layer Protocol	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-120422		Sogou Input Method for Windows (versions prior to 16.10)	SlippyNunchucks
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sogou:input_method:-:*:*:*:*:windows:*:*	DarkVigil
Sogou Input Method Insecure HTTP Configuration Retrieval Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1059: Command and Scripting Interpreter	https://pinyin.sogou.com/changelog.php

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-123158</td><td>sshole</td><td rowspan="2">OpenBSD OpenSSH (portable, musl without PAM); Alpine Linux openssh-server</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:openbsd:openssh:*:*:*:*:*:*:*:*:*, cpe:2.3:o:alpinelinux:alpine_linux:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">sshole (OpenSSH Password Authentication Bypass Vulnerability)</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-394</td><td>T1133: External Remote Services, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1078.003: Local Accounts, T1136: Create Account, T1136.001: Local Account, T1098: Account Manipulation, T1098.004: SSH Authorized Keys, T1548: Abuse Elevation Control Mechanism, T1548.003: Sudo and Sudo Caching, T1021: Remote Services, T1021.004: SSH</td><td>https://www.openssh.org/</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">
UTA0576</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-104935
CVE-2026-111357
CVE-2026-118527</td><td>-</td><td>Ivanti Connect Secure</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1059.006: Python, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1055.009: Proc Memory, T1070: Indicator Removal, T1070.002: Clear Linux or Mac System Logs, T1070.004: File Deletion, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1564: Hide Artifacts, T1564.001: Hidden Files and Directories, T1140: Deobfuscate/Decode Files or Information, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1040: Network Sniffing, T1110: Brute Force, T1110.003: Password Spraying, T1087: Account Discovery, T1087.002: Domain Account, T1016: System Network Configuration Discovery, T1005: Data from Local System, T1560: Archive Collected Data, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">
Gorbag</td><td>Russia</td><td rowspan="3">Transportation and Logistics, Defense, Law Enforcement Agencies, Government</td><td rowspan="3">Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-8088</td><td>Prime ReverseShell, BeautyStealer</td><td>WinRAR</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Stealth, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1586: Compromise Accounts, T1586.002: Email Accounts, T1587: Develop Capabilities, T1587.001: Malware, T1588: Obtain Capabilities, T1588.001: Malware, T1588.005: Exploits, T1566: Phishing, T1566.001: Spearphishing Attachment, T1199: Trusted Relationship, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.005: Visual Basic, T1203: Exploitation for Client Execution, T1204: User Execution, T1204.002: Malicious File, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, T1027: Obfuscated Files or Information, T1027.009: Embedded Payloads, T1027.013: Encrypted/Encoded File, T1140: Deobfuscate/Decode Files or Information, T1564: Hide Artifacts, T1564.004: NTFS File Attributes, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, T1497: Virtualization/Sandbox Evasion, T1497.003: Time Based Checks, T1070: Indicator Removal, T1070.004: File Deletion, T1555: Credentials from Password Stores, T1555.003: Credentials from Web Browsers, T1539: Steal Web Session Cookie, T1217: Browser Information Discovery, T1083: File and Directory Discovery, T1005: Data from Local System, T1074: Data Staged, T1074.001: Local Data Staging, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1095: Non-Application Layer Protocol, T1571: Non-Standard Port, T1567: Exfiltration Over Web Service, T1048: Exfiltration Over Alternative Protocol, T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">
SlippyNunchucks</td><td>China</td><td rowspan="3">-</td><td rowspan="3">Hong Kong, Thailand, Japan, Vietnam, Oman, Sri Lanka</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft & Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-120422</td><td>DarkVigil</td><td>Sogou Input Method for Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0006: Credential Access, TA0005: Stealth, TA0112: Defense Impairment, TA0007: Discovery, TA0011: Command and Control, TA0010: Exfiltration, T1583: Acquire Infrastructure, T1583.001: Domains, T1659: Content Injection, T1557: Adversary-in-the-Middle, T1574: Hijack Execution Flow, T1574.001: DLL, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, T1027: Obfuscated Files or Information, T1112: Modify Registry, T1082: System Information Discovery, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1105: Ingress Tool Transfer, T1573: Encrypted Channel, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actors **UTA0576, Gorbag, SlippyNunchucks,** and the malware **DarkVigil, 3AM Ransomware, Prime ReverseShell,** and **BeautyStealer.**

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 **seven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **UTA0576, Gorbag, SlippyNunchucks,** and malware **Prime ReverseShell, BeautyStealer, 3AM Ransomware,** and **DarkVigil** in Breach and Attack Simulation(BAS).

Threat Advisories

Ivanti Connect Secure Zero-Day Hands Attackers Root Without a Login

Attackers Exploit an Access Bypass in Drupal Commerce Core

WordPress Core RCE Exploited in the Upgrade Window

Gorbag Targets Ukraine with Prime ReverseShell and BeautyStealer

3AM Ransomware Affiliate Breaches UK Schools in Suspected Hybrid AI Intrusion

SlippyNunchucks Poisons Sogou DNS to Plant DarkVigil

SSHole CVE-2026-123158: A 10-Year-Old OpenSSH Flaw Hiding in musl

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
DarkVigil	SHA1	8A60A8E90E1F5F08F28FE5A6DD57BD686C20DC23, 3E16BA611782AF6E45576D390488D28FD676BADE
3AM Ransomware	SHA256	882f34f27292dd797fc022eeac28dfb070d408d310f4e9be20a2a0cb1e78620d
Prime ReverseShell	SHA256	78ea83bfbca85a39e59fa35c8f704873f3fdad3a5278430e75286247530042b8
BeautyStealer	SHA256	9ce0f41d6e575aca81d290b3d0b89b011da4f9b87276b27d1c7de81695d4c927

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 demo of **HivePro**.

REPORT GENERATED ON

November 09, 2026 • 9:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com