Date of Publication
October 26, 2026

Hive Pro

Hiveforce Labs

WEEKLY

# THREAT DIGEST

## Attacks, Vulnerabilities, and Actors

19 to 25 OCTOBER 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 13

Adversaries in Action 22

Recommendations 23

Threat Advisories 24

Appendix 25

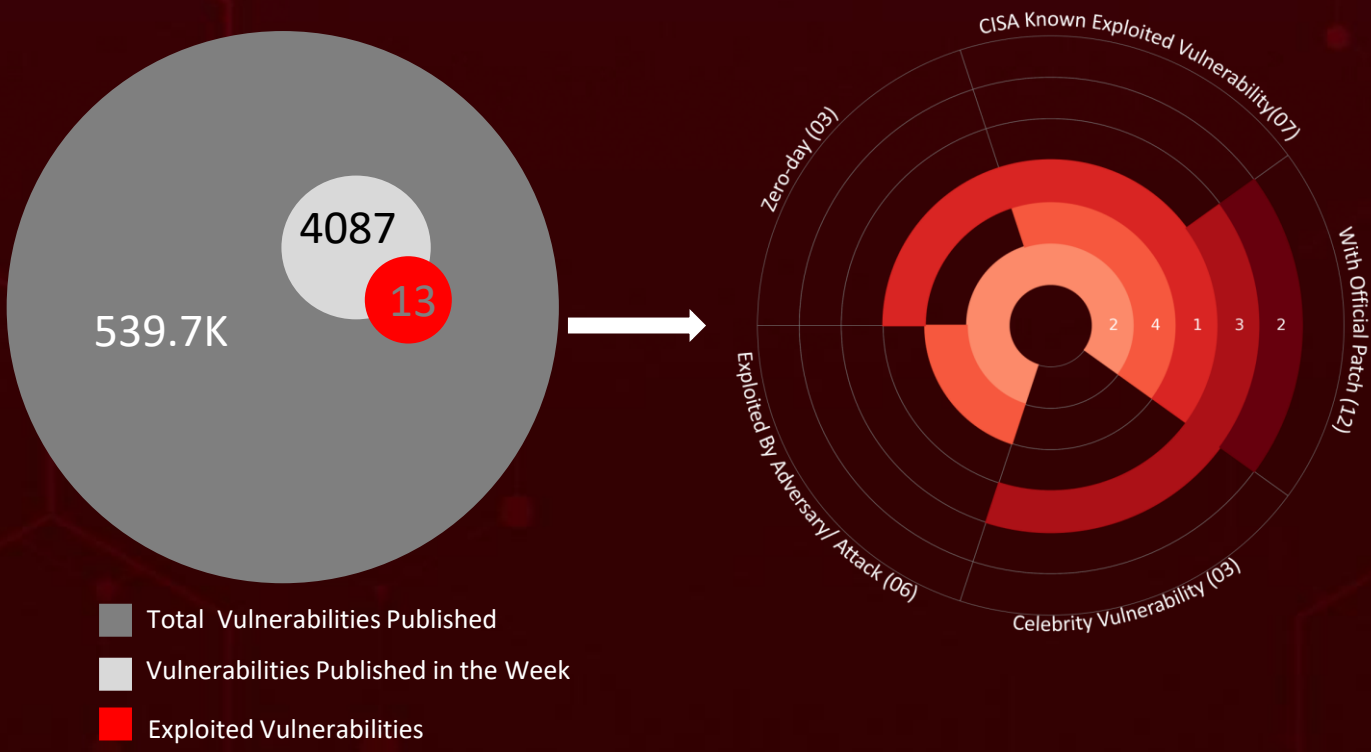
What Next? 28

# 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, **five** major attacks were detected, **thirteen** vulnerabilities were actively exploited, and **one** threat actor group was closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, attackers are actively exploiting **CVE-2026-102764**, a critical authentication bypass flaw in BeyondTrust Remote Support. The suspected China-nexus group Armory Castle used it as a zero-day to plant the SAWFLY web shell, gain root, and harvest stored credentials. Meanwhile, **PHP2Shell** (CVE-2026-109618 and CVE-2026-109619), two critical flaws in the core PHP engine, let unauthenticated attackers run code on nearly every PHP release since 5.4, and exploitation attempts began before patches were released. At the same time, Arista patched CVE-2026-114625, an exploited zero-day in VeloCloud Orchestrator that lets even a lowest-privileged tenant user become a superuser operator.

In a separate supply chain attack, threat actors used stolen engineer tokens to publish a poisoned **LiteLLM** release that stole cloud keys, AI API keys, and CI/CD secrets from systems that installed it. **SafePay ransomware** has also passed 600 victims worldwide, breaking in through stolen credentials and long-known edge-device and backup flaws before wiping backups and encrypting systems. Together, these incidents underscore a growing trend of attacks on trusted infrastructure and the software supply chain, reinforcing the need for timely patching, credential rotation, and layered security defenses.



# High Level Statistics

**5**
Attacks Executed

**13**
Vulnerabilities Exploited

**1**
Adversaries in Action

- Aoki
- SAWFLY
- BARECLAW
- privcollect
- SafePay

- CVE-2026-102764
- CVE-2026-106173
- CVE-2026-109618
- CVE-2026-109619
- CVE-2026-114625
- CVE-2026-115560
- CVE-2020-3259
- CVE-2023-20269
- CVE-2023-27532
- CVE-2024-40711
- CVE-2024-40766
- CVE-2026-111497
- CVE-2026-101767

- ARMORY CASTLE

# Insights

Two hours of a poisoned **LiteLLM** release was enough to steal cloud and AI keys.

**BeyondTrust zero-day** CVE-2026-102764 was exploited for weeks before disclosure, so treat exposed appliances as compromised.

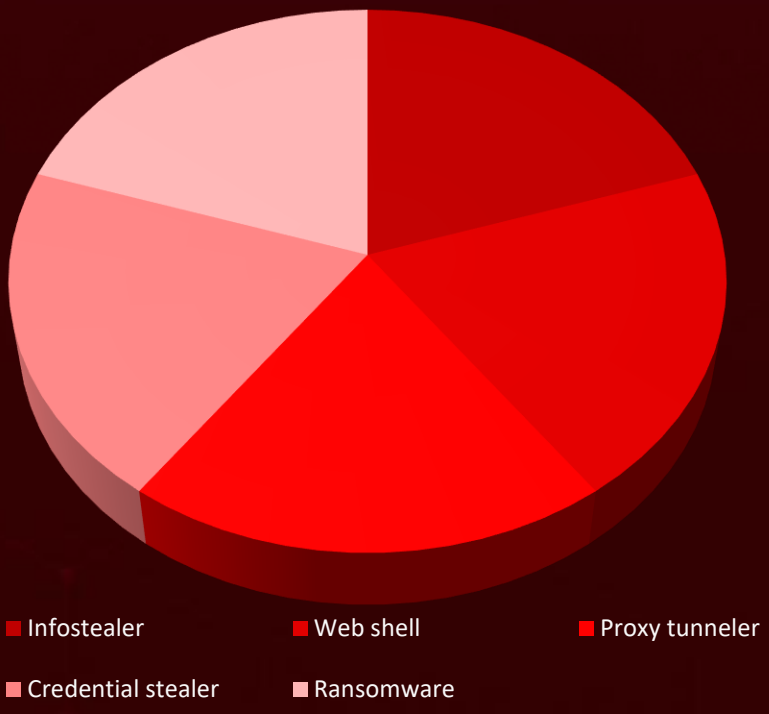
**SafePay** still breaks in through flaws dating back to 2020, so old bugs never expire.

**PHP2Shell** lives in the PHP engine, so clean code on unpatched PHP is still exposed.

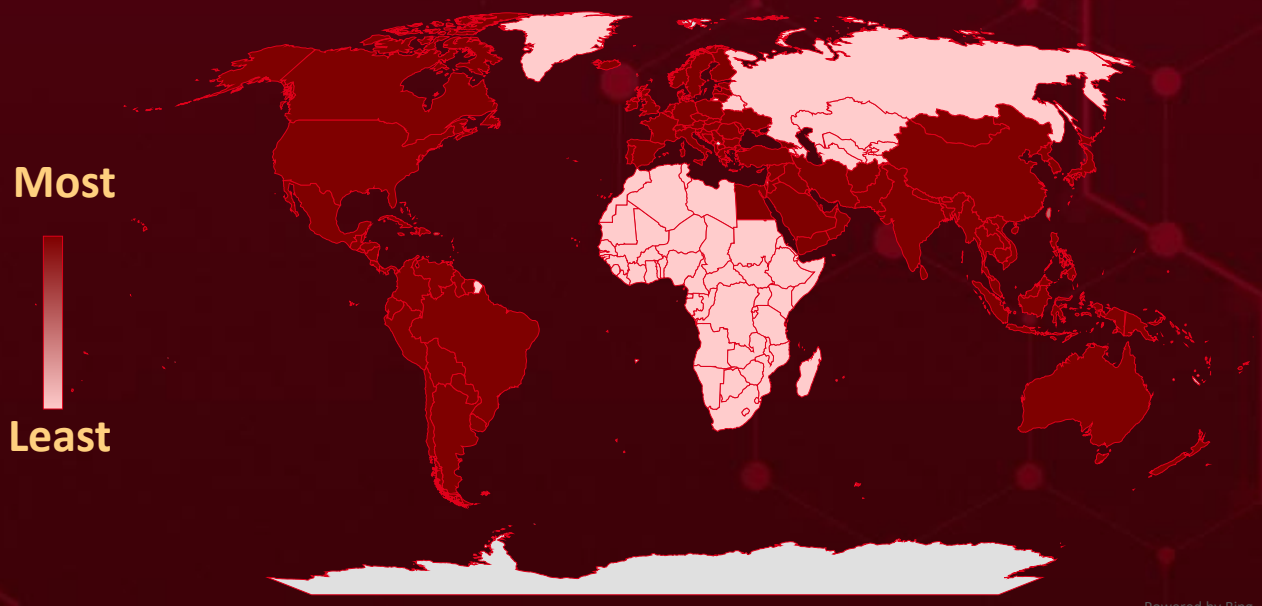
**eMudhra** CA keys could be cracked in under a second, so stale trust stores are now a risk.

**CVE-2026-114625** needs just a read-only VeloCloud account to reach superuser.

## Threat Distribution



# Targeted Countries




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

| Countries | Countries | Countries | Countries |
|---|---|---|---|
| Vietnam | South Korea | Slovenia | Costa Rica |
| Portugal | Belize | Croatia | Montenegro |
| Nepal | Timor-Leste | Sri Lanka | Finland |
| Albania | Bhutan | Cuba | Nauru |
| Sweden | United States | Syria | France |
| Andorra | Bolivia | Cyprus | Netherlands |
| Mexico | Afghanistan | Trinidad and Tobago | Georgia |
| Antigua and Barbuda | Bosnia and Herzegovina | Czech Republic | Nicaragua |
| Pakistan | Malta | United Arab Emirates | Germany |
| Argentina | Brazil | Denmark | North Macedonia |
| Singapore | Moldova | Vanuatu | Greece |
| Australia | Brunei | Dominica | Oman |
| Tuvalu | Myanmar | Liechtenstein | Grenada |
| Austria | Bulgaria | Dominican Republic | Palau |
| Malaysia | New Zealand | Luxembourg | Guatemala |
| Bahamas | Cambodia | Ecuador | Papua New Guinea |
| Mongolia | Norway | Maldives | Guyana |
| Bahrain | Canada | Egypt | Peru |
| North Korea | Panama | Marshall Islands | Haiti |
| Bangladesh | Chile | El Salvador | Poland |
| Paraguay | Philippines | Micronesia | Honduras |
| Barbados | China | Estonia | Qatar |
| Samoa | Romania | Monaco | |
| Belgium | Colombia | | |
| | Saudi Arabia | | |

# Targeted Industries




# TOP MITRE ATT&CK TTPs

| | | | | |
|---|---|---|---|---|
| **T1059** Command and Scripting Interpreter | **T1190** Exploit Public-Facing Application | **T1005** Data from Local System | **T1068** Exploitation for Privilege Escalation | **T1078** Valid Accounts |
| **T1211** Exploitation for Defense Evasion | **T1071** Application Layer Protocol | **T1070** Indicator Removal | **T1071.001** Web Protocols | **T1588** Obtain Capabilities |
| **T1098** Account Manipulation | **T1105** Ingress Tool Transfer | **T1036** Masquerading | **T1027** Obfuscated Files or Information | **T1552** Unsecured Credentials |
| **T1070.004** File Deletion | **T1499** Endpoint Denial of Service | **T1555** Credentials from Password Stores | **T1055** Process Injection | **T1041** Exfiltration Over C2 Channel |

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Aoki | Aoki (aka Aokigahara) is an infostealer, first seen in early 2026, that is still being actively developed. Recent versions add the theft of credential, token and session files from AI coding assistants such as Claude, OpenAI Codex, Cursor, Codeium, Gemini, GitHub Copilot, JetBrains AI Assistant and Kiro, along with AWS credentials. It also steals data from dozens of browsers, cryptocurrency wallets and extensions, password managers, Discord and Telegram clients, gaming platforms, email clients, and VPN and FTP clients. It records which security products are installed. It has no backdoor command list and sends everything it collects to its C&C server through a /gate endpoint. | - | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Infostealer | | Credential Theft, Token Theft, Session Hijacking, Cryptocurrency Theft, Financial Fraud | Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | 752c8e64af60960b85cf00e4bd34eb459e24b7939464f718ec18494df43b4b69<br>bf037920d39b85572ec7e53b51f09c28198c2c0afbc7c7d6cf639b1f047caebf |

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>SAWFLY</td><td rowspan="6">A lightweight PHP web shell deployed after successful compromise of BeyondTrust Remote Support appliances, giving interactive remote access and encrypted two-way command-and-control. The actor uses it as the conduit to escalate privileges, take full administrative control of the appliance, and keep persistence that survives reboots.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-102764</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Web shell</td><td rowspan="3">Remote access, persistence</td><td>BeyondTrust Remote Support ≤26.2.3</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>ARMORY CASTLE</td><td>https://www.beyondtrust.com/trust-center/security-advisories/bt26-05</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">dc14e215269a93fdbc4c1a80b984c23faf7af0911c6dbb85309796a6f2ae95fb</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>BARECLAW</td><td rowspan="6">A custom C-based SOCKS5 proxy tunneler that relays TCP connections between a remote client and destinations through the compromised appliance. The actor modifies the appliance's HAProxy configuration so the tunneler can be reached directly from the internet.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-102764</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Proxy tunneler</td><td rowspan="3">Covert tunnelling, internal pivoting</td><td>BeyondTrust Remote Support ≤26.2.3</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>ARMORY CASTLE</td><td>https://www.beyondtrust.com/trust-center/security-advisories/bt26-05</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">1f19b9a27d79c11bda00a1e8faf74a7fdd683d38ccef1b60df2fd0307e3aa462</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>privcollect</td><td rowspan="6">privcollect is a Python credential stealer delivered through a supply-chain compromise of LiteLLM 1.107.0 on October 21, 2026. Using stolen GitHub OAuth tokens, attackers built the release from a lookalike repository (Berri-AI/litellm). The package drops startup hooks that run on every Python launch. They steal browser, cloud, CI/CD, SSH, and AI tool credentials, along with process environment variables and LiteLLM proxy API keys. The stolen data is encrypted and exfiltrated to www.litellm[.]dev. A secondary loader polls a GitHub dead drop hourly to fetch and run remote code.</td><td>Software supply-chain compromise</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Credential stealer</td><td rowspan="3">Credential Theft, Data Exfiltration, API Key Theft</td><td>LiteLLM (BerriAI) version 1.107.0</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">03ac2a8b752605d1d7710979c17ff18b03dd978203ba23ba97fd8ce3d6f897ea, 9dd0a3926f96a37eb86cf1ee2310d9be93139cc4ebef3ef9e2efe9531390be25</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 |
|---|---|---|---|
| SafePay | SafePay is a ransomware operation active since August 2024 and among the most active of 2026. It has hit at least 600 victims across critical infrastructure sectors in North America, South America, Europe and Australia. It steals data before encryption, then encrypts files with a hybrid of ChaCha20 and RSA and appends the .SafePay extension. Before encrypting, it stops Volume Shadow Copy and factory-resets NAS backup devices. | Stolen credentials, edge-device exploits | CVE-2020-3259<br>CVE-2023-20269<br>CVE-2023-27532<br>CVE-2024-40711<br>CVE-2024-40766 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Ransomware | | Data theft, encryption, backup destruction | Cisco ASA & FTD, Veeam Backup & Replication, SonicWall SonicOS |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC, https://www.veeam.com/kb4424, https://www.veeam.com/kb4649, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015 |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae, 6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a | | |

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-2026-102764 |  | BeyondTrust Remote Support (26.2.3 and prior) | ARMORY CASTLE (aka UNC5221, WARP PANDA) |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:* | SAWFLY, BARECLAW |
| BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-290 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.beyondtrust.com/trust-center/security-advisories/bt26-05 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-106173 |  | Fortinet FortiSIEM (7.5.0, before 7.5.1) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*:* | - |
| Fortinet FortiSIEM Path Traversal Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-22 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://fortiguard.fortinet.com/psirt/FG-IR-26-180 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-109618 | PHP2Shell | PHP Group PHP (5.4 through 8.5.11) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:* | - |
| PHP2Shell (PHP Out-of-Memory Corruption Vulnerability) |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1325 CWE-416 CWE-755 CWE-824 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.php.net/archive/2026.php#2026-10-21-5 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-109619 | PHP2Shell | PHP Group PHP (5.4 through 8.5.11) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:* | - |
| PHP2Shell (PHP Remote Code Execution Vulnerability) |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1325 CWE-416 CWE-755 CWE-824 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.php.net/archive/2026.php#2026-10-21-5 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-114625 |  | Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.18, 6.1.x before 6.1.3.10, 6.4.x before 6.4.2.12) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*:*:* | - |
| Arista VeloCloud Orchestrator SQL Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-89 | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation | https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-115560 |  | PHP (affected versions not disclosed by vendor) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:* | - |
| PHP Remote Code Execution Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | - | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter |  |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2020-3259 |  | Cisco ASA and FTD | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*, cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* | SafePay Ransomware |
| Cisco ASA and FTD Information Disclosure Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-200 | T1190: Exploit Public-Facing Application, T1212: Exploitation for Credential Access | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2023-20269 |  | Cisco Adaptive Security Appliance and Firepower Threat Defense | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*, cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:* | SafePay Ransomware |
| Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-288 | T1190: Exploit Public-Facing Application, T1110: Brute Force, T1133: External Remote Services | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2023-27532</td><td></td><td rowspan="2">Veeam Backup & Replication, Veeam Cloud Connect</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:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">Veeam Backup & Replication Cloud Connect 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</td><td>T1190: Exploit Public-Facing Application, T1212: Exploitation for Credential Access</td><td>https://www.veeam.com/kb4424</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-40711 |  | Veeam Backup and Replication | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:* | SafePay Ransomware |
| Veeam Backup and Replication Deserialization Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-502 | T1190: Exploit Public-Facing Application, T1136.001: Create Account: Local Account | https://www.veeam.com/kb4649 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-40766 |  | SonicWall SonicOS | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:* | SafePay Ransomware |
| SonicWall SonicOS Improper Access Control Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-284 | T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1078: Valid Accounts | https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-111497 | Node2Shell | Node.js (22.x before 22.23.4, 24.x before 24.22.1, 26.x before 26.12.1, and End-of-Life versions), Bun (before 1.4.4), Google Brotli (1.0.3 through 1.2.0) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:* cpe:2.3:a:google:brotli:*:*:*:*:*:*:*:* | - |
| Node.js Brotli Decoder Out-of-Bounds Write Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-787 CWE-252 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://nodejs.org/en/blog/release/v22.23.4/, https://nodejs.org/en/blog/release/v24.22.1/, https://nodejs.org/en/blog/release/v26.12.1/, https://bun.com/blog/bun-v1.4.4 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-101767 |  | Oracle E-Business Suite (Oracle Application Object Library) 12.2.3 to 12.2.15 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:oracle:application_object_library:*:*:*:*:*:*:*:* | - |
| Oracle E-Business Suite SQL Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-287 CWE-306 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.oracle.com/security-alerts/cpuoct2026.html |

# Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"><br><u>ARMORY CASTLE (aka UNC5221, WARP PANDA)</u></td><td>China (suspected)</td><td rowspan="3">-</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Cyber espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-102764</td><td>SAWFLY, BARECLAW</td><td>BeyondTrust Remote Support</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0009: Collection, TA0011: Command and Control, T1584: Compromise Infrastructure, T1584.008: Network Devices, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell, T1098: Account Manipulation, T1548: Abuse Elevation Control Mechanism, T1548.001: Setuid and Setgid, T1078: Valid Accounts, T1070: Indicator Removal, T1070.002: Clear Linux or Mac System Logs, T1070.004: File Deletion, T1555: Credentials from Password Stores, T1005: Data from Local System, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1573: Encrypted Channel, T1090: Proxy, T1572: Protocol Tunneling, T1105: Ingress Tool Transfer, T1219: Remote Access Tools, T1219.002: Remote Desktop Software</td></tr>
</table>

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **thirteen exploited vulnerabilities** and block the indicators related to the threat actor **ARMORY CASTLE** and malware **Aoki, SAWFLY, BARECLAW, privcollect,** and **SafePay.**

**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 **thirteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **ARMORY CASTLE,** and malware **Aoki** and **SafePay** in Breach and Attack Simulation(BAS).

# Threat Advisories

Aoki Infostealer Expands Its Haul to AI Assistants

CVE-2026-102764: BeyondTrust Zero-Day Exploited in Espionage Attacks

Path Traversal in FortiSIEM Gives Attackers a Direct Route to Command Execution

Stolen GitHub Tokens Fuel LiteLLM Supply Chain Breach

PHP2Shell: Your Application Code Is Clean, But the Engine Underneath It Isn't

Oracle's October 2026 Critical Patch Update Spans 1,295 Fixes Across Its Portfolio

Arista Patches an Actively Exploited VeloCloud Orchestrator Zero-Day

SafePay Ransomware Surges Past 600 Victims Worldwide

Back-to-Back PHP Warnings Continue With an Unpatched Code Execution Flaw

Node2Shell: Node.js Brotli Flaw Turns Compressed Data into Code Execution

Number Four Holds the Keys: eMudhra Intermediate CA Compromise

# 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 |
|---|---|---|
| Aoki | SHA256 | 752c8e64af60960b85cf00e4bd34eb459e24b7939464f718ec18494df43b4b69, bf037920d39b85572ec7e53b51f09c28198c2c0afbc7c7d6cf639b1f047caebf, 0adc8e83b2416c275b1283916d70568faddeb6d718eb45f9addfb0938db245b3, 6655b89b9885483d459c73f2a52e3cec121de5c5956172a8676a0f4c2de94999, 780bbdbb119befd4eb16e0c2ec0c64e7bedc1b53ce4f85804aea091a6e3af519, 2fb80e2221bd304e7cd5ac04169e71807ad92d19836f1aaf7885295cb90b2d94, 73dbac0907e8a092cd978f2787ab1994946f5da1e08f2bdbd05ea52e80cdb896 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| Aoki | SHA256 | 07bc2e3a1d14743cc44f1dc4c78d15d0f2b458b39fb48422b13df40fc662ba21, c533570fd7cd7eaf5478317b03ea5750d03797aa4d11ebd96555b6cb708c63f2, 6350dfee6975a9b159c5a57a3e97f757b0b02fd2dc708016fa6d7270e720c865, 36af3acc78058023cdcf9307bc15be640be9425de97e574fdaf42d03d308725b, 039240551f88b0064b2615dffdc1321b1e7c58e3f617ac138a65a6d59400b331, 0e38bd3c30a4ca08641240ce95b5b6ba593e131213ca1b2a28da4e0385fcabc4, 3b4547f0d7549274f366cd9568b3d302c1e80e1b89359da681beb47260ec7975, b590235493487c51f7050b341c9b2450e4f761ad6055207e4f6daf0ceccae271c, e374f9ff5094f728528efa566c3de1b7fea7d95f497242a01fffa6c70b5eb768, f779314b1a5a0b297fd4e2a5f9c1e40d387b3e7c401d42324b556a70f813840e |
| SAWFLY | SHA256 | dc14e215269a93fdbc4c1a80b984c23faf7af0911c6dbb85309796a6f2ae95fb |
| | File Name | mangoapi.php |
| | File Path | /%SITE_SERVICE_ACCOUNT%/ingredi/app/laravel/public/mangoapi.php |
| | HTTP POST Parameter | _c94mfe |
| | YARA Rule | G_Hunting_Webshell_SAWFLY_1 |
| BARECLAW | SHA256 | 1f19b9a27d79c11bda00a1e8faf74a7fdd683d38ccef1b60df2fd0307e3aa462 |
| privcollect | SHA256 | 03ac2a8b752605d1d7710979c17ff18b03dd978203ba23ba97fd8ce3d6f897ea |

| Attack Name | TYPE | VALUE |
|---|---|---|
| privcollect | SHA256 | 9dd0a3926f96a37eb86cf1ee2310d9be93139cc4ebef3ef9e2efe9531390be25 |
| SafePay | SHA256 | 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae, 6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a, e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346, 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917, a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526 |
| | SHA1 | 07353237350c35d6dc2c8f143b649cd07c71f62b, b498a2683640c983bb069fa2ea9e67cef4a3797d, BBFED53E3BB1F306F4DA97D995CF4AE5B73AD081 |
| | IPv4 | 77[.]37[.]49[.]40, 167[.]235[.]225[.]149, 5[.]255[.]11[.]134, 37[.]10[.]71[.]188, 88[.]119[.]167[.]239 |
| | Email | ColinSolomon[@]protonmail[.]com |
| | Filename | locker.dll, soc.dll, readme_safepay.txt, Socks_werfault.exe, DYRasWtb.exe |
| | Hostname | WIN-SBOE3CPNALE, WIN-3IUUOFVTQAR, WIN-DK18BI83M0S, WIN-I1HRRJHCEIV |

*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

**October 26, 2026 • 11:50 AM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com