

Date of Publication  
May 27, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities, and Actors**

19 to 25 MAY 2025

# Table Of Contents

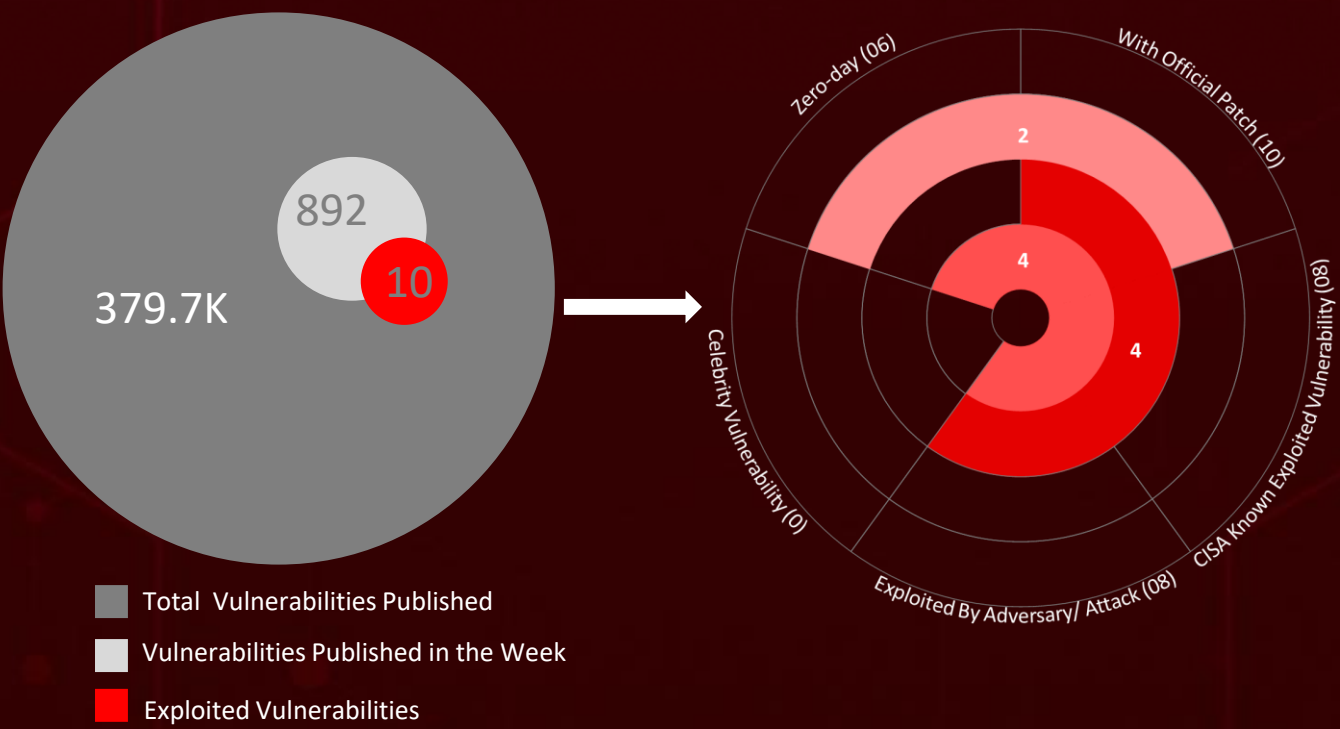
|                                  |    |
|----------------------------------|----|
| <u>Summary</u>                   | 03 |
| <u>High Level Statistics</u>     | 04 |
| <u>Insights</u>                  | 05 |
| <u>Targeted Countries</u>        | 06 |
| <u>Targeted Industries</u>       | 07 |
| <u>Top MITRE ATT&amp;CK TTPs</u> | 07 |
| <u>Attacks Executed</u>          | 08 |
| <u>Vulnerabilities Exploited</u> | 16 |
| <u>Adversaries in Action</u>     | 23 |
| <u>Recommendations</u>           | 29 |
| <u>Threat Advisories</u>         | 30 |
| <u>Appendix</u>                  | 31 |
| <u>What Next?</u>                | 35 |

# Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **fifteen** major attacks were detected, **ten** critical vulnerabilities were actively exploited, and **seven** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the notable incidents, **Operation RoundPress**, Russian state-backed hackers **APT28** exploited known vulnerabilities in email platforms like Roundcube, Horde, and Zimbra to conduct a covert webmail espionage campaign, compromising sensitive communications. Compounding these risks, Mozilla was forced to issue emergency updates after **two critical vulnerabilities** in Firefox were discovered to be under active exploitation before their public disclosure.

Adding to the growing list of cyber threats, the Chinese-speaking threat actor **UAT-6382** exploited **CVE-2025-0994**, a zero-day in **Trimble Cityworks**, enabling remote code execution and deploying malware for persistent access in critical infrastructure. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



# High Level Statistics

15

Attacks  
Executed

10

Vulnerabilities  
Exploited

7

Adversaries in  
Action

- [SpyPress](#)
  - [LOSTKEYS](#)
  - [StealerBot](#)
  - [Interlock](#)
  - [Nitrogen](#)
  - [PureHVNC](#)
  - [PureRAT](#)
  - [PureLogs](#)
  - [PureCrypter](#)
  - [TetraLoader](#)
  - [KrustyLoader](#)
  - [Qilin](#)
  - [BianLian](#)
  - [RansomExx](#)
  - [PipeMagic](#)
- [CVE-2023-43770](#)
  - [CVE-2020-35730](#)
  - [CVE-2024-11182](#)
  - [CVE-2024-27443](#)
  - [CVE-2025-4918](#)
  - [CVE-2025-4919](#)
  - [CVE-2017-0199](#)
  - [CVE-2017-11882](#)
  - [CVE-2025-0994](#)
  - [CVE-2025-31324](#)
- [APT28](#)
  - [COLDRIVER](#)
  - [SideWinder](#)
  - [UAT-6382](#)
  - [UNC5221](#)
  - [UNC5174](#)
  - [CL-STA-0048](#)



# Insights

## PureHVNC

**RAT** Delivered via  
Deceptive Kling AI  
Promotion Campaign

## Russia-backed COLDRIVER

unleashes stealthy **LOSTKEYS** malware  
in bold new espionage campaign

## PureRAT Malware

Campaign Quietly  
Compromises  
Russian Business  
Networks

## Old Microsoft Office flaws

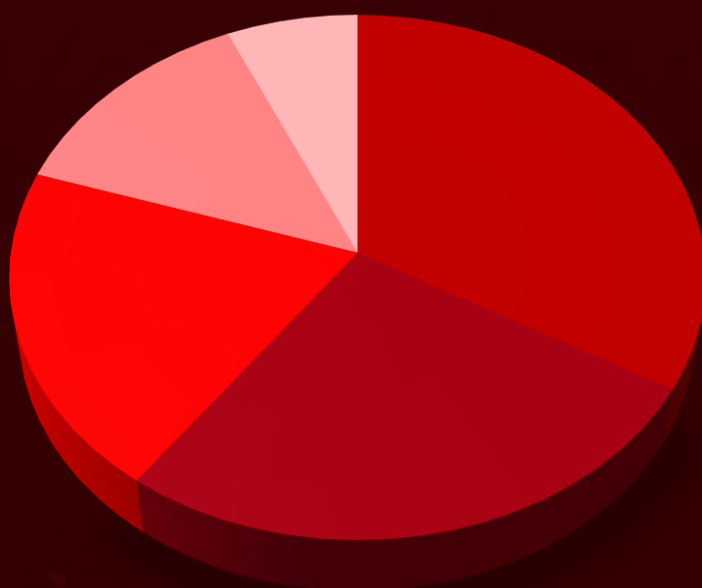
exploited as **SideWinder** targets  
military and government systems

**Military Data Breached as  
Interlock Ransomware  
Expands Operations**

## Nitrogen Ransomware

Uses Legitimate  
Tools to Slip Past  
Security Measures

## Threat Distribution



■ Ransomware ■ Stealer ■ Loader ■ RAT ■ Trojan

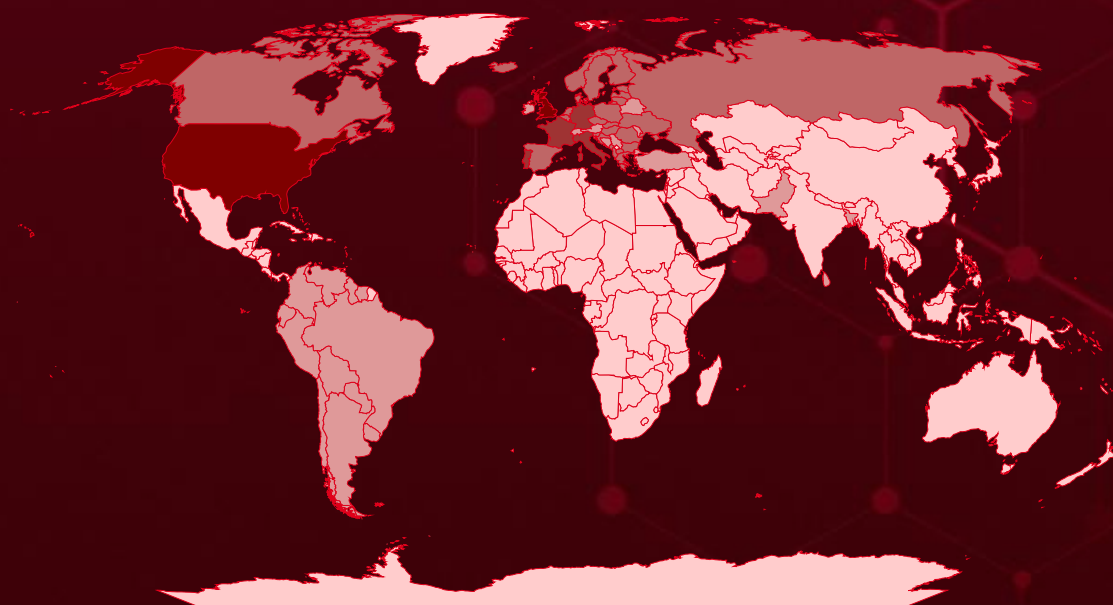


# Targeted Countries

Most



Least



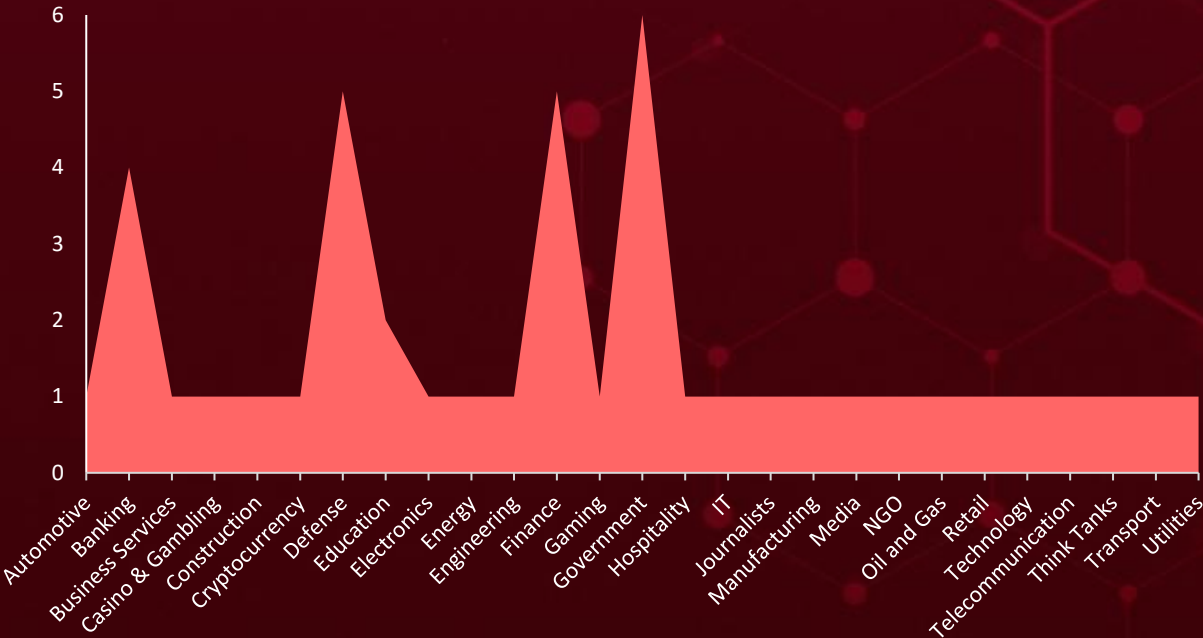
Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

| Countries       | Countries              | Countries             | Countries           |
|-----------------|------------------------|-----------------------|---------------------|
| United States   | Luxembourg             | Suriname              | Haiti               |
| United Kingdom  | Czech Republic         | Liechtenstein         | Timor-Leste         |
| Portugal        | Montenegro             | Turkey                | Côte d'Ivoire       |
| France          | Latvia                 | Uruguay               | French Guiana       |
| Germany         | Monaco                 | Malta                 | Honduras            |
| Italy           | San Marino             | Philippines           | Nicaragua           |
| Norway          | Paraguay               | Gabon                 | Antigua and Barbuda |
| Sweden          | Chile                  | Syria                 | Dominican Republic  |
| Russia          | Switzerland            | Gambia                | Barbados            |
| Denmark         | Colombia               | Oman                  | Palau               |
| Netherlands     | Bosnia and Herzegovina | Georgia               | India               |
| Estonia         | Argentina              | Saint Lucia           | El Salvador         |
| Canada          | Brazil                 | Bahamas               | Indonesia           |
| Finland         | Ecuador                | South Korea           | Eritrea             |
| Slovenia        | Sri Lanka              | Ghana                 | Iran                |
| Albania         | Austria                | Tunisia               | Rwanda              |
| Croatia         | Moldova                | Bahrain               | Iraq                |
| Belgium         | Guyana                 | Nigeria               | Samoa               |
| North Macedonia | Bolivia                | Grenada               | Cuba                |
| Greece          | Holy See               | Panama                | Senegal             |
| Poland          | Pakistan               | Guatemala             | Israel              |
| Hungary         | Bangladesh             | Brunei                | Singapore           |
| Romania         | Peru                   | Guinea                | Cyprus              |
| Iceland         | Ireland                | Sao Tome and Principe | Somalia             |
| Slovakia        | Andorra                | Guinea-Bissau         | Jamaica             |
| Bulgaria        | Belarus                | Burundi               | Cabo Verde          |
| Spain           | Serbia                 | Costa Rica            | Japan               |
| Lithuania       | Venezuela              | Sudan                 | Cambodia            |



# Targeted Industries



# TOP MITRE ATT&CK TTPs

## T1059

Command and Scripting Interpreter

## T1027

Obfuscated Files or Information

## T1566

Phishing

## T1588

Obtain Capabilities

## T1041

Exfiltration Over C2 Channel

## T1082

System Information Discovery

## T1588.006

Vulnerabilities

## T1190

Exploit Public-Facing Application

## T1203

Exploitation for Client Execution

## T1071.001

Web Protocols

## T1005

Data from Local System

## T1071

Application Layer Protocol

## T1486

Data Encrypted for Impact

## T1059.001

PowerShell

## T1132.001

Standard Encoding

## T1547

Boot or Logon Autostart Execution

## T1204

User Execution

## T1036

Masquerading

## T1059.007

JavaScript

## T1132

Data Encoding





# Attacks Executed

| NAME                | OVERVIEW  | DELIVERY METHOD                   | TARGETED CVEs  |
|---------------------|---|-----------------------------------|--|
| <u>SpyPress</u>     | SpyPress is a collection of JavaScript payloads designed to target various webmail platforms. Each version connects to a group of hardcoded command-and-control (C2) servers, using obfuscated JavaScript and standard HTTP POST requests to stealthily extract sensitive data. | Loaded by the XSS Vulnerabilities | CVE-2023-43770<br>CVE-2020-35730<br>CVE-2024-11182<br>CVE-2024-27443   |
|                     |   | IMPACT                            | AFFECTED PRODUCTS  |
| TYPE                |   | Sensitive Data Exfiltration       | Roundcube Webmail, MDAemon Email Server, Zimbra Collaboration (ZCS)  |
| Information Stealer |   |                                   | PATCH LINKS  |
| ASSOCIATED ACTOR    |   |                                   |  |
| APT28               |   |                                   | <a href="https://roundcube.net/news/2023/09/15/security-update-1.6.3-released">https://roundcube.net/news/2023/09/15/security-update-1.6.3-released</a> ,<br><a href="https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13">https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13</a> ,<br><a href="https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html">https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html</a> ,<br><a href="https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes">https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes</a> |
| IOC TYPE            | VALUE   |                                   |  |
| SHA1                | 41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C, 1078C587FE2B246D618AF74D157F941078477579, F95F26F1C097D4CA38304ECC692DBAC7424A5E8D  |                                   |  |
| IPv4                | 185[.]225[.]69[.]223, 193[.]29[.]104[.]152, 45[.]137[.]222[.]24   |                                   |  |
| SHA256              | 335b1cd7708284fc1c2c6678f2f8d6737d68935ec992d680ff540f2e72774665  |                                   |  |

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 CVEs     |
|---------------------|--|---------------------|-------------------|
| <u>LOSTKEYS</u>     | LOSTKEYS can steal files from specific directories and file types defined in its code. It also sends system information and a list of running processes back to the attacker.                        | Phishing Emails     | -                 |
|                     |  | IMPACT              | AFFECTED PRODUCTS |
| TYPE                |  | Targeted File Theft | -                 |
| Information Stealer |  |                     | PATCH LINK        |
| ASSOCIATED ACTOR    |  |                     |                   |
| COLDRIIVER          |  |                     | -                 |
| IOC TYPE            | VALUE  |                     |                   |
| SHA256              | 13f7599c94b9d4b028ce02397717a1282a46f07b9d3e2f8f2b3213fa8884b029, 4c7accba35edd646584bb5a40ab78f963de45e5fc816e62022cd7ab1b01dae9c, 6b85d707c23d68f9518e757cc97adb20adc8accb33d0d68faf1d8d56d7840816 |                     |                   |

| NAME               | OVERVIEW  | DELIVERY METHOD   | TARGETED CVEs  |
|--------------------|---|---|--|
| <u>StealerBot</u>  | StealerBot is a credential stealer that collects system information, checks for antivirus software, and exfiltrates data to attackers. It uses techniques like Base64 encoding, XOR encryption, and hides in DLLs loaded by trusted Windows applications, blending classic espionage tactics with cybercrime-driven credential theft. | Spearphishing Attachment                                  | CVE-2017-0199<br>CVE-2017-11882  |
|                    |   | IMPACT  | AFFECTED PRODUCTS  |
| TYPE               |   | Information Theft, System Profiling, and Security Evasion | Microsoft Office and WordPad   |
| Credential Stealer |   |   | PATCH LINKS  |
| ASSOCIATED ACTOR   |   |   |  |
| SideWinder         |   |   | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199</a> ,<br><a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882</a> |

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 CVEs     |
|---------------------------|---|---|-------------------|
| <a href="#">Interlock</a> | INTERLOCK is an emerging ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. While the Windows variant is most common, INTERLOCK stands out for its rare focus on FreeBSD. The group employs refined double-extortion tactics and runs a leak site called “Worldwide Secrets Blog” to publish stolen data and pressure victims into negotiations. | Phishing  | -                 |
|                           |   | IMPACT  | AFFECTED PRODUCTS |
|                           |   | Financial Loss, Data Encryption, and Operational Disruption | -                 |
| TYPE                      |   |   | PATCH LINK        |
| Ransomware                |   |   |                   |
| ASSOCIATED ACTOR          |   |   |                   |
| -                         |   |   | -                 |
| IOC TYPE                  | VALUE   |   |                   |
| IPv4                      | 23[.]95[.]182[.]59, 195[.]201[.]21[.]34, 159[.]223[.]46[.]184   |   |                   |

| NAME                     | OVERVIEW  | DELIVERY METHOD   | TARGETED CVEs     |
|--------------------------|---|---|-------------------|
| <a href="#">Nitrogen</a> | The Nitrogen ransomware group runs a highly active and aggressive campaign. Similar to the earlier LukaLocker ransomware, it uses a double-extortion model. Its threat comes from both encrypting critical data and using legitimate system tools to bypass defenses and evade detection. | Malvertising Campaigns                                      | -                 |
|                          |   | IMPACT  | AFFECTED PRODUCTS |
|                          |   | Financial Loss, Data Encryption, and Operational Disruption | Windows           |
| TYPE                     |   |   | PATCH LINK        |
| Ransomware               |   |   |                   |
| ASSOCIATED ACTOR         |   |   |                   |
| -                        |   |   | -                 |
| IOC TYPE                 | VALUE   |   |                   |
| SHA256                   | 5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac7a71d321, 9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdfbede83051692e63, ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d8507ffe2c   |   |                   |

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 CVEs            |
|---|--|--|--------------------------|
| <b>PureHVNC</b><br><br><b>TYPE</b><br>RAT<br><b>ASSOCIATED ACTOR</b><br>- | PureHVNC is a customized Remote Access Trojan (RAT) that gives attackers full control over infected systems. Often obfuscated with .NET Reactor, it enables keylogging, data theft, and remote desktop access for surveillance and system control. | Malvertising Campaigns                 | -                        |
|   |  | <b>IMPACT</b>                          | <b>AFFECTED PRODUCTS</b> |
|   |  | Full Remote Control, Information Theft | -                        |
|   |  |  | <b>PATCH LINK</b>        |
| -   |  |  | -                        |
| IOC TYPE  | VALUE  |  |                          |
| SHA256  | b33e162a78b7b8e7dbbab5d1572d63814077fa524067ce79c37f52441b8bd384, 0c9228983fbd928ac94c057a00d744d6be4bd4c1b39d1465b7d955b7d35bf496, 839371cd5a5d66828ac9524182769371dede9606826ad7c22c3bb18fb2ee91cb   |  |                          |

| NAME   | OVERVIEW  | DELIVERY METHOD  | TARGETED CVEs            |
|--|---|--|--------------------------|
| <b>PureRAT</b><br><br><b>TYPE</b><br>RAT<br><b>ASSOCIATED ACTOR</b><br>- | PureRAT is a remote access trojan that communicates with its command-and-control (C2) servers using encrypted, protobuf-formatted data. It collects detailed system information such as OS version, antivirus status, device IDs, and IP address. Built for stealth and persistence, PureRAT can execute commands to self-delete, restart, or shut down the host. It also monitors active applications for specific keywords like “password,” “bank,” or “WhatsApp,” making it especially invasive. | Phishing Emails  | -                        |
|  |   | <b>IMPACT</b>  | <b>AFFECTED PRODUCTS</b> |
|  |   | Full System Surveillance, Data Collection and Exfiltration | -                        |
|  |   |  | <b>PATCH LINK</b>        |
| -  |   |  | -                        |
| IOC TYPE   | VALUE   |  |                          |
| IPv4:Port  | 195[.]26[.]227[.]209[:]56001  |  |                          |

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 CVEs     |
|------------------|--|---|-------------------|
| <u>PureLogs</u>  | PureLogs is a potent information stealer that extracts sensitive data from browsers, email clients, messaging apps, VPNs, and cryptocurrency wallets. In addition to data theft, it functions as a downloader, allowing attackers to deploy additional payloads after infection. This dual capability increases its threat level, especially in enterprise environments, where it can enable long-term access and follow-up attacks. | Phishing<br>Emails                          | -                 |
|                  |  | IMPACT                                      | AFFECTED PRODUCTS |
| TYPE             |  | Extensive Data Theft,<br>Payload Deployment | -                 |
| Stealer          |  |   | PATCH LINK        |
| ASSOCIATED ACTOR |  |   |                   |
| -                |  |   | -                 |
| IOC TYPE         | VALUE  |   |                   |
| IPv4:Port        | 195[.]26[.]227[.]209[:]23075   |   |                   |
| SHA256           | df38f29f1f511ac9a5ecae5d4734732c039c17ec06137fade7b1e2b48899c681   |   |                   |

| NAME               | OVERVIEW   | DELIVERY METHOD                          | TARGETED CVEs     |
|--------------------|--|--|-------------------|
| <u>PureCrypter</u> | PureCrypter functions as a loader, downloading disguised payloads often masked as harmless media files then decrypting and executing them directly in memory to evade disk-based detection. It maintains persistence by copying itself to %AppData% as "Action.exe" and adding a startup script to run automatically at each reboot. | Phishing<br>Emails                       | -                 |
|                    |  | IMPACT                                   | AFFECTED PRODUCTS |
| TYPE               |  | Malware Deployment,<br>Persistent Access | -                 |
| Loader             |  |  | PATCH LINK        |
| ASSOCIATED ACTOR   |  |  |                   |
| -                  |  |  | -                 |
| IOC TYPE           | VALUE  |  |                   |
| URL                | hxxps[:]//apstori[.]ru/panel/uploads/Bghwwhmlr[.]wav   |  |                   |

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   |
|--------------------|---|--------------------------|--|
| <u>TetraLoader</u> | TetraLoader is a custom loader built on the MaLoader framework, written in Simplified Chinese. It allows attackers to package shellcode and other payloads within Rust-based binaries, enabling stealthy deployment of advanced tools while avoiding detection. | Exploiting Vulnerability | CVE-2025-0994  |
| TYPE               |   | IMPACT                   | AFFECTED PRODUCT   |
| Loader             |   | Payload Delivery         | Trimble Cityworks  |
| ASSOCIATED ACTOR   |   |                          | PATCH DETAILS  |
| UAT-6382           |   |                          | Trimble Cityworks version 15.8.9 and Cityworks with office companion version 23.10 |
| IOC TYPE           | VALUE   |                          |  |
| SHA256             | 14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64c4f4611f, 4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9  |                          |  |

| NAME                | OVERVIEW   | DELIVERY METHOD                        | TARGETED CVE  |
|---------------------|--|--|---|
| <u>KrustyLoader</u> | KrustyLoader is a Rust-based malware loader designed to deliver backdoors during post-exploitation. It focuses on evading detection and maintaining persistence on compromised Linux systems. Upon execution, it performs anti-analysis and environment checks to avoid discovery. | Exploiting Vulnerability               | CVE-2025-31324  |
| TYPE                |  | IMPACT                                 | AFFECTED PRODUCTS   |
| Loader              |  | Backdoor Deployment, Persistent Access | SAP NetWeaver   |
| ASSOCIATED ACTOR    |  |  | PATCH LINK  |
| UNC5221             |  |  | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |
| IOC TYPE            | VALUE  |  |   |
| SHA256              | f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec, 47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04, 3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce   |  |   |

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  |
|-----------------------|--|--|---|
| <a href="#">Qilin</a> | Qilin ransomware was originally developed in Go but has since transitioned to Rust, improving its performance, stealth, and resistance to reverse engineering. The Rust-based variants feature advanced capabilities like remote execution, enhanced propagation in virtualized environments, and sophisticated evasion techniques to bypass modern security defenses. | Exploiting Vulnerability                   | CVE-2025-31324  |
| TYPE                  |  | IMPACT                                     | AFFECTED PRODUCT  |
| Ransomware            |  | Data Encryption and Operational Disruption | SAP NetWeaver   |
| ASSOCIATED ACTOR      |  |  | PATCH LINK  |
| -                     |  |  | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |
| IOC TYPE              | VALUE  |  |   |
| URL                   | hxxp[:]//184[.]174[.]96[.]70   |  |   |
| IPv4                  | 180[.]131[.]145[.]73   |  |   |

| NAME                     | OVERVIEW   | DELIVERY METHOD          | TARGETED CVE  |
|--------------------------|--|--------------------------|---|
| <a href="#">BianLian</a> | BianLian is a ransomware group steadily expanding its victim base, demonstrating advanced operational security and expertise in network infiltration. Notably, it has shifted its focus from encrypting files to leveraging data-leak extortion. | Exploiting Vulnerability | CVE-2025-31324  |
| TYPE                     |  | IMPACT                   | AFFECTED PRODUCT  |
| Ransomware               |  | Data Theft and Exposure  | SAP NetWeaver   |
| ASSOCIATED ACTOR         |  |                          | PATCH LINK  |
| -                        |  |                          | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |
| IOC TYPE                 | VALUE  |                          |   |
| IPv4:Port                | 64[.]190[.]113[.]215[:]443, 15[.]237[.]93[.]235[:]443, 94[.]198[.]40[.]6[:]20033   |                          |   |

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  |
|---------------------------|--|--|---|
| <a href="#">RansomExx</a> | RansomExx is a ransomware variant operating under a ransomware-as-a-service (RaaS) model, recently redeveloped in Rust to enhance stealth and reduce detection by antivirus solutions.               | Exploiting Vulnerability                   | CVE-2025-31324  |
| TYPE                      |  | IMPACT                                     | AFFECTED PRODUCT  |
| Ransomware                |  | Data Encryption and Operational Disruption | SAP NetWeaver   |
| ASSOCIATED ACTOR          |  |  | PATCH LINK  |
| -                         |  |  | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |
| IOC TYPE                  | VALUE  |  |   |
| SHA256                    | bb12b7c4169e2a86a67a86f03048baa282688d36ef0ae3251bc1ace317c26af9, 6b667bb7e4f3f2cb6c6f2d43290f32f41ae9f0d6ed34b818d78490050f7582a1, 78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d |  |   |

| NAME                      | OVERVIEW  | DELIVERY METHOD                                  | TARGETED CVE  |
|---------------------------|---|--|---|
| <a href="#">PipeMagic</a> | PipeMagic is an advanced backdoor Trojan crafted in Rust. It employs encrypted communication via named pipes, granting attackers remote access and facilitating subsequent infections such as ransomware deployment or data exfiltration. | Exploiting Vulnerability                         | CVE-2025-31324  |
| TYPE                      |   | IMPACT   | AFFECTED PRODUCT  |
| Trojan                    |   | Remote Control, Data Exfiltration and Data Theft | SAP NetWeaver   |
| ASSOCIATED ACTOR          |   |  | PATCH LINK  |
| -                         |   |  | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |
| IOC TYPE                  | VALUE   |  |   |
| SHA256                    | 945a02cdbbd8772f5b0a30f047ae6450ee77a14fef5046af252565a9b524c88f, d9cb912e6ca4dc22515b9dfddced01a96f6de2fd51169597d437d390d5d868f1, 2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe                                      |  |   |




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  |
|---|-------------------------|---|---|
| <u>CVE-2023-43770</u>   |                         | Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3 | APT28   |
|   | ZERO-DAY                |   |   |
|   |                         | AFFECTED CPE  | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEV                | cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*                             | SpyPress  |
| Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability |                         |   |   |
|   | CWE ID                  | ASSOCIATED TTPs   | PATCH LINK  |
|   | CWE-79                  | T1588.006: Vulnerabilities, T1204: User Execution                   | <a href="https://roundcube.net/news/2023/09/15/security-update-1.6.3-released">https://roundcube.net/news/2023/09/15/security-update-1.6.3-released</a> |




| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|--|---|--|---|
| <u>CVE-2020-35730</u>                                      |  | Roundcube: 1.2.0 - 1.4.9   | APT28   |
|  | ZERO-DAY  |  |   |
|  |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME   | CISA KEV  | cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*  | SpyPress  |
| Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability |  |  |   |
|  | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|  | CWE-79  | T1059: Command and Scripting Interpreter, T1059.007: JavaScript/JScript, T1557: Man-in-the-Browser, T1189: Drive-by Compromise, T1204: User Execution, T1204.001: Malicious Link | <a href="https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13">https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13</a> |




| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|---|---|---|---|
| <u>CVE-2024-11182</u>   |  | MDaemon Email Server before version 24.5.1c                     | APT28   |
|   | ZERO-DAY  |   |   |
|   |  | AFFECTED CPE  | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEV  | cpe:2.3:a:mdaemon:mdaemon:*:*:*:*:*:*                           | SpyPress  |
| MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability |  |   |   |
|   | CWE ID  | ASSOCIATED TTPs   | PATCH LINK  |
|   | CWE-79  | T1059: Command and Scripting Interpreter, T1204: User Execution | <a href="https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html">https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html</a> |




| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|---|---|---|---|
| <u>CVE-2024-27443</u>   |  | Zimbra Collaboration (ZCS) 9.0 and 10.0                         | APT28   |
|   | ZERO-DAY  |   |   |
|   |  | AFFECTED CPE  | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEV  | cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*                  | SpyPress  |
| Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability |  |   |   |
|   | CWE ID  | ASSOCIATED TTPs   | PATCH LINK  |
|   | CWE-79  | T1059: Command and Scripting Interpreter, T1204: User Execution | <a href="https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes">https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes</a> |






| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|---|---|--|---|
| <u>CVE-2025-4919</u>                                      |  | Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1 | -   |
|   | ZERO-DAY  |  |   |
|   |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEV  | cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*<br>cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*                                     | -   |
| Mozilla Firefox Out-of-Bounds Read or Write Vulnerability |  |  |   |
|   | CWE ID  | ASSOCIATED TTPs  | PATCH LINKS   |
|   | CWE-787<br>CWE-125  | T1203: Exploitation for Client Execution,<br>T1055: Process Injection  | <a href="https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/">https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/</a><br><a href="https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/">https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/</a><br><a href="https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/">https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/</a> |

| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|--|---|--|---|
| <u>CVE-2017-0199</u>   |  | Microsoft Office and WordPad   | SideWinder  |
|  | ZERO-DAY  |  |   |
|  |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME   | CISA KEY  | cpe:2.3:a:microsoft:microsoft_office:*.:.:.:.:.:.:.*                               | StealerBot  |
| Microsoft Office and WordPad Remote Code Execution Vulnerability |  | cpe:2.3:o:microsoft:windows:*.:.:.:.:.:.:.*  |   |
|  | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|  | CWE-20  | T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199</a> |

| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|--|---|--|---|
| <u>CVE-2017-11882</u>                            |  | Microsoft Office   | SideWinder  |
|  | ZERO-DAY  |  |   |
|  |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME   | CISA KEY  | cpe:2.3:a:microsoft:office:-*.:.:.:.*.:  | StealerBot  |
| Microsoft Office Memory Corruption Vulnerability |  |  |   |
|  | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|  | CWE-119   | T1203: Exploitation for Client Execution, T1190: Exploit Public-Facing Application, T1055: Process Injection | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882</a> |


| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR   |
|---|---|--|--|
| <u>CVE-2025-0994</u>                            |  | Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10 | UAT-6382   |
|   | ZERO-DAY  |  |  |
|   |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE  |
| NAME  | CISA KEV  | cpe:2.3:a:trimble:cityworks:*.~*.~*.~*.~*.~*.~*.~*   | TetraLoader  |
| Trimble Cityworks Deserialization Vulnerability |  |  |  |
|   | CWE ID  | ASSOCIATED TTPs  | PATCH DETAILS  |
|   | CWE-502   | T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution                     | Trimble Cityworks version 15.8.9 and Cityworks with office companion version 23.10 |

| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|--|---|--|---|
| <u>CVE-2025-31324</u>                                |  | SAP NetWeaver Version 7.50   | UNC5221, UNC5174, CL-STA-0048   |
|  | ZERO-DAY  |  |   |
|  |  | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME   | CISA KEV  | cpe:2.3:a:sap:sap_netweaver:7.50.*~.*~.*~.*~.*~.*~.*~*   | KrustyLoader, Qilin ransomware, BianLian, RansomExx, PipeMagic  |
| SAP NetWeaver Unrestricted File Upload Vulnerability |  |  |   |
|  | CWE ID  | ASSOCIATED TTPs  | PATCH LINK  |
|  | CWE-434   | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1505: Server Software Component, T1505.003: Web Shell | <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html</a> |







# Adversaries in Action


| NAME  | ORIGIN   | TARGETED INDUSTRIES  | TARGETED REGIONS  |
|---|--|--|---|
| <div></div> <div><u>APT28 (aka Sednit group, Sofacy, Fancy Bear, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)</u></div> | Russia   | Governmental Entities, Defense Companies, Telecommunication, Academic, Military, Transport | Eastern Europe, Governments in Africa, Europe, and South America    |
|   | MOTIVE   |  |   |
|   | Information theft and espionage                                      |  |   |
|   | TARGETED CVE   | ASSOCIATED ATTACKS/RANSOM WARE   | AFFECTED PRODUCT  |
|   | CVE-2023-43770<br>CVE-2020-35730<br>CVE-2024-11182<br>CVE-2024-27443 | SpyPress   | Roundcube Webmail, MDaemon Email Server, Zimbra Collaboration (ZCS) |


## TTPs


TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1587: Develop Capabilities; T1587.004: Exploits; T1587.001: Malware; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1027: Obfuscated Files or Information; T1187: Forced Authentication; T1556: Modify Authentication Process; T1556.006: Multi-Factor Authentication; T1087: Account Discovery; T1087.003: Email Account; T1056: Input Capture; T1056.003: Web Portal Capture; T1119: Automated Collection; T1114: Email Collection; T1114.002: Remote Email Collection; T1114.003: Email Forwarding Rule; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1071.003: Mail Protocols; T1132: Data Encoding; T1132.001: Standard Encoding; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1566: Phishing; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpreter; T1059.007: JavaScript


| NAME   | ORIGIN                          | TARGETED INDUSTRIES                                     | TARGETED REGION   |
|--|---------------------------------|---|---|
|  <p><u><b>COLDRIVER (aka Star Blizzard, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, UNC4057)</b></u></p>  | Russia                          | Governments, Militaries, Journalists, Think Tanks, NGOs | Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, Ukraine, United Kingdom, United States |
|  | <b>MOTIVE</b>                   |   |   |
|  | Information theft and espionage |   |   |
|  | <b>TARGETED CVE</b>             | <b>ASSOCIATED ATTACKS/RANS OMWARE</b>                   | <b>AFFECTED PRODUCTS</b>  |
|  | -                               | LOSTKEYS  | -   |
| <b>TTPs</b>  |                                 |   |   |
| TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1027: Obfuscated Files or Information; T1497.001: System Checks; T1497: Virtualization/Sandbox Evasion; T1082: System Information Discovery; T1057: Process Discovery; T1005: Data from Local System; T1119: Automated Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel |                                 |   |   |

| NAME  | ORIGIN                          | TARGETED INDUSTRIES                                     | TARGETED REGION                    |
|---|---------------------------------|---|------------------------------------|
|  <p><u>SideWinder (aka Rattlesnake, Razor Tiger, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)</u></p>  | India                           | Government Institutions, Military Institutions, Banking | Sri Lanka, Bangladesh and Pakistan |
|   | <b>MOTIVE</b>                   |   |                                    |
|   | Information theft and espionage | <b>ASSOCIATED ATTACKS/RANSOM WARE</b>                   | <b>AFFECTED PRODUCTS</b>           |
|   | <b>TARGETED CVE</b>             |   |                                    |
|   | CVE-2017-0199<br>CVE-2017-11882 | StealerBot  | Microsoft Office and WordPad       |
| <b>TTPs</b>   |                                 |   |                                    |
| TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1566: Phishing; T1566.001: Spearphishing Attachment; T1574: Hijack Execution Flow; T1574.001: DLL; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1036: Masquerading; T1656: Impersonation; T1590: Gather Victim Network Information; T1218.011: Rundll32; T1140: Deobfuscate/Decode Files or Information; T1082: System Information Discovery; T1132: Data Encoding; T1132.001: Standard Encoding; T1518: Software Discovery; T1518.001: Security Software Discovery; T1027: Obfuscated Files or Information; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder |                                 |   |                                    |

| NAME  | ORIGIN                          | TARGETED INDUSTRIES                   | TARGETED REGION          |
|---|---------------------------------|---------------------------------------|--------------------------|
| <br><u>UAT-6382</u>  | Chinese-speaking                | Government                            | United States            |
|   | <b>MOTIVE</b>                   |                                       |                          |
|   | Information theft and espionage |                                       |                          |
|   | <b>TARGETED CVE</b>             | <b>ASSOCIATED ATTACKS/RANSOM WARE</b> | <b>AFFECTED PRODUCTS</b> |
|   | CVE-2025-0994                   | TetraLoader                           | Trimble Cityworks        |
| <b>TTPs</b>   |                                 |                                       |                          |
| TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1505: Server Software Component; T1505.003: Web Shell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1074: Data Staged; T1041: Exfiltration Over C2 Channel; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1588.005: Exploits; T1505.004: IIS Components; T1588.006: Vulnerabilities |                                 |                                       |                          |

| NAME   | ORIGIN                          | TARGETED INDUSTRIES                   | TARGETED REGION          |
|--|---------------------------------|---------------------------------------|--------------------------|
| <br><b>UNC5221 (aka UTA0178, Red Dev 61)</b>  | China                           | Government, Finance, Oil and Gas      | Worldwide                |
|  | <b>MOTIVE</b>                   |                                       |                          |
|  | Information theft and espionage |                                       |                          |
|  | <b>TARGETED CVE</b>             | <b>ASSOCIATED ATTACKS/RANSOM WARE</b> | <b>AFFECTED PRODUCTS</b> |
|  | CVE-2025-31324                  | KrustyLoader                          | SAP NetWeaver            |
| <b>TTPs</b>  |                                 |                                       |                          |
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0003: Persistence; TA0011: Command and Control; T1068: Exploitation for Privilege Escalation; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1588.005: Exploits; T1588.006: Vulnerabilities; T1070.004: File Deletion; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1204: User Execution; T1059: Command and Scripting Interpreter |                                 |                                       |                          |

| NAME  | ORIGIN                     | TARGETED INDUSTRIES                   | TARGETED REGION          |
|---|----------------------------|---------------------------------------|--------------------------|
| <br><b>UNC5174 (aka Uteus)</b>   | China                      | Government, Finance, Oil and Gas      | Worldwide                |
|   | <b>MOTIVE</b>              |                                       |                          |
|   | Espionage, Financial Gains |                                       |                          |
|   | <b>TARGETED CVE</b>        | <b>ASSOCIATED ATTACKS/RANSOM WARE</b> | <b>AFFECTED PRODUCTS</b> |
|   | CVE-2025-31324             | -                                     | SAP NetWeaver            |
| <b>TTPs</b>   |                            |                                       |                          |
| TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; T1105: Ingress Tool Transfer; T1136: Create Account; T1059: Command and Scripting Interpreter; T1531- Account Access Removal; T1190: Exploit Public-Facing Application; T1082: System Information Discovery; T1083: File and Directory Discovery |                            |                                       |                          |

| NAME  | ORIGIN         | TARGETED INDUSTRIES                  | TARGETED REGIONS    |
|---|----------------|--------------------------------------|---------------------|
| <div></div> <div><u>CL-STA-0048</u></div>  | China          | Government, Finance,<br>Oil and Gas  | Worldwide           |
|   | MOTIVE         |                                      |                     |
|   | Espionage      |                                      |                     |
|   | TARGETED CVE   | ASSOCIATED<br>ATTACKS/RANSOM<br>WARE | AFFECTED<br>PRODUCT |
|   | CVE-2025-31324 | -                                    | SAP NetWeaver       |
| TTPs  |                |                                      |                     |
| TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1204: User Execution; T1059: Command and Scripting Interpreter; T1547: Boot or Logon Autostart Execution; T1548: Abuse Elevation Control Mechanism; T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1562: Impair Defenses; T1003: OS Credential Dumping; T1552: Unsecured Credentials; T1083: File and Directory Discovery; T1057: Process Discovery; T1570: Lateral Tool Transfer; T1021: Remote Services; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1048: Exfiltration Over Alternative Protocol; T1041: Exfiltration Over C2 Channel |                |                                      |                     |

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **APT28, COLDRIVER, SideWinder, UAT-6382, UNC5221, UNC5174, CL-STA-0048**, and malware **SpyPress, LOSTKEYS, StealerBot, Interlock, Nitrogen, PureHVNC, PureRAT, PureLogs, PureCrypter, TetraLoader, KrustyLoader, Qilin, BianLian, RansomExx, PipeMagic**.

## 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 **ten exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT28, COLDRIVER, SideWinder, UAT-6382, UNC5221, UNC5174, CL-STA-0048**, and malware **SpyPress, LOSTKEYS, Nitrogen, PureLogs, TetraLoader** in Breach and Attack Simulation(BAS).



# Threat Advisories

[Operation RoundPress: APT28's Webmail Espionage Exposed](#)

[COLDRIVER Creeps Closer with LOSTKEYS Malware](#)

[Firefox Users at Risk: Two Major Flaws Found and Fixed](#)

[SideWinder's Silent War Using Old Exploits on New Targets](#)

[Interlock Ransomware Blurs Line Between Cybercrime and Espionage](#)

[Nitrogen Ransomware Is Breaking In Without Triggering Any Alarms](#)

[When AI Turns Against You: The Malvertising Trap of Kling AI](#)

[Pure RAT's Stealthy Campaign Sweeps Russian Enterprises](#)

[Chinese Hackers Leverage Cityworks Bug to Take Over Vital Systems](#)

[Critical CVE-2025-31324 Flaw in SAP NetWeaver Under Active Attack](#)

# 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  |
|------------------------|---------|--|
| <b><u>SpyPress</u></b> | SHA1    | 41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C,<br>1078C587FE2B246D618AF74D157F941078477579,<br>F95F26F1C097D4CA38304ECC692DBAC7424A5E8D,<br>B6C340549700470C651031865C2772D3A4C81310,<br>65A8D221B9ECED76B9C17A3E1992DF9B085CECD7,<br>8E6C07F38EF920B5154FD081BA252B9295E8184D,<br>AD3C590D1C0963D62702445E8108DB025EEBEC70,<br>EBF794E421BE60C9532091EB432C1977517D1BE5,<br>F81DE9584F0BF3E55C6CF1B465F00B2671DAA230 |
|                        | IPv4    | 185[.]225[.]69[.]223,<br>193[.]29[.]104[.]152,<br>45[.]137[.]222[.]24,<br>91[.]237[.]124[.]164,<br>185[.]195[.]237[.]106,<br>91[.]237[.]124[.]153,<br>146[.]70[.]125[.]79,<br>89[.]44[.]9[.]74,<br>111[.]90[.]151[.]167  |
|                        | Domains | sqj[.]fr,<br>tgh24[.]xyz,<br>tuo[.]world,<br>lsjb[.]digital,<br>jiaw[.]shop,<br>hfuu[.]de,<br>raxia[.]top,<br>rnl[.]world,<br>hijx[.]xyz,<br>ikses[.]net   |

| Attack Name      | TYPE   | VALUE  |
|------------------|--------|--|
| <u>SpyPress</u>  | SHA256 | 335b1cd7708284fc1c2c6678f2f8d6737d68935ec992d680ff540f2e72774665   |
| <u>LOSTKEYS</u>  | SHA256 | 13f7599c94b9d4b028ce02397717a1282a46f07b9d3e2f8f2b3213fa8884b029,<br>4c7accba35edd646584bb5a40ab78f963de45e5fc816e62022cd7ab1b01dae9c,<br>6b85d707c23d68f9518e757cc97adb20adc8accb33d0d68faf1d8d56d7840816,<br>3233668d2e4a80b17e6357177b53539df659e55e06ba49777d0d5171f27565dd,<br>6bc411d562456079a8f1e38f3473c33ade73b08c7518861699e9863540b64f9a,<br>28a0596b9c62b7b7aca9cac2a07b067109f27d327581a60e8cb4fab92f8f4fa9,<br>b55cdce773bc77ee46b503dbd9430828cc0f518b94289fbfa70b5fb b02ab1847,<br>02ce477a07681ee1671c7164c9cc847b01c2e1cd50e709f7e861eaa b89c69b6f,<br>8af28bb7e8e2f663d4b797bf3ddbbee7f0a33f637a33df9b31fbb4c1c e71b2fee                             |
| <u>Interlock</u> | IPv4   | 23[.]95[.]182[.]59,<br>195[.]201[.]21[.]34,<br>159[.]223[.]46[.]184,<br>23[.]227[.]203[.]162,<br>65[.]109[.]226[.]176,<br>65[.]38[.]120[.]47,<br>216[.]245[.]184[.]181,<br>212[.]237[.]217[.]182,<br>168[.]119[.]96[.]41,<br>216[.]245[.]184[.]170,<br>65[.]108[.]80[.]58,<br>84[.]200[.]24[.]41,<br>206[.]206[.]123[.]65,<br>49[.]12[.]102[.]206,<br>193[.]149[.]180[.]158,<br>85[.]239[.]52[.]252,<br>5[.]252[.]177[.]228,<br>80[.]87[.]206[.]189,<br>65[.]108[.]80[.]58,<br>212[.]104[.]133[.]72,<br>140[.]82[.]14[.]117,<br>64[.]94[.]84[.]85,<br>49[.]12[.]69[.]80,<br>96[.]62[.]214[.]11,<br>177[.]136[.]225[.]153,<br>188[.]34[.]195[.]44,<br>45[.]61[.]136[.]202 |

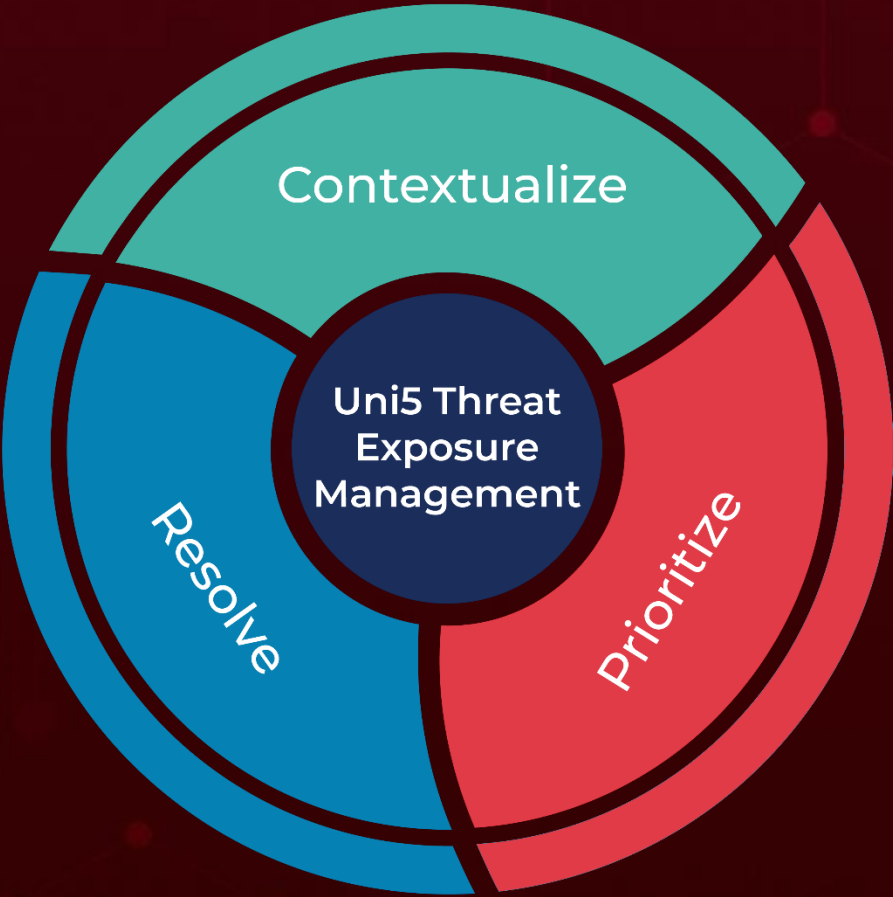
| Attack Name         | TYPE      | VALUE   |
|---------------------|-----------|---|
| <u>Nitrogen</u>     | SHA256    | 5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac7a71d321,<br>9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdafbede83051692e63,<br>ab366a7c4a343a798490c4451d1d8e42aea2b894cb3162b5c59e08d8507ffe2c,<br>c94b70dff50e69639b0ef1e828621c5fddcf144fea93e27520f48264dd33273,<br>0db5c55ef52e89401a668f59bf4f69391f4632447c51483bb64749d7f2123916,<br>779576719a9c400a7a4abed0386e2111eb331160572c91a2fd8eaa1a7d6e6c63,<br>e6a498b89aa04d7c25cbfa96599a4cd9bdcc79e73bf7b09906e5ca85bda2bff6,<br>55f3725ebe01ea19ca14ab14d747a6975f9a6064ca71345219a14c47c18c88be,<br>fa3eca4d53a1b7c4cfcd14f642ed5f8a8a864f56a8a47acbf5cf11a6c5d2afa2 |
| <u>PureHVNC</u>     | SHA256    | b33e162a78b7b8e7dbbab5d1572d63814077fa524067ce79c37f52441b8bd384,<br>0c9228983fbd928ac94c057a00d744d6be4bd4c1b39d1465b7d955b7d35bf496,<br>839371cd5a5d66828ac9524182769371dede9606826ad7c22c3bb18fb2ee91cb,<br>9dab2badfdae86963b2f13ce8942fe78dd66ec497f8d82dd40c0cb5bec4fb2a7,<br>cee3f98b5f175219d025a92eddec4fd8bcaae31e6ad99321ae7c00b822063fc3,<br>a5baceb97a2be17dd0c282292ebb0b5a56a555013a4c8fffc2335c504780fb,<br>3fba4a0942244e9c3ad25a57a21f91b06f8732a2ca36da948ae5f0afa51dc72b,<br>557becfcc7eccaa5a7368a6d5583404af26aadede2c345d6070e6e9fab44a641   |
| <b>PureRAT</b>      | IPv4:Port | 195[.]26[.]227[.]209[:.]56001   |
| <b>PureLogs</b>     | IPv4:Port | 195[.]26[.]227[.]209[:.]23075   |
|                     | SHA256    | df38f29f1f511ac9a5ecae5d4734732c039c17ec06137fade7b1e2b48899c681  |
| <b>PureCrypter</b>  | URL       | hxxps[:]//apstori[.]ru/panel/uploads/Bghwwhmlr[.]wav  |
| <u>TetraLoader</u>  | SHA256    | 14ed3878b6623c287283a8a80020f68e1cb6bfc37b236f33a95f3a64c4f4611f,<br>4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9   |
| <u>KrustyLoader</u> | SHA256    | f92d0cf4d577c68aa615797d1704f40b14810d98b48834b241dd5c9963e113ec,<br>47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04,<br>3f14dc65cc9e35989857dc1ec4bb1179ab05457f2238e917b698edb4c57ae7ce,   |

| Attack Name         | TYPE      | VALUE   |
|---------------------|-----------|---|
| <u>KrustyLoader</u> | SHA256    | 91f66ba1ad49d3062afdcc80e54da0807207d80a1b539edcdbd6e1bf99e7a2ca,<br>c71da1dfea145798f881afd73b597336d87f18f8fd8f9a7f524c6749a5c664e4,<br>b8e56de3792dbd0f4239b54cfaad7ece3bd42affa4fbbdd7668492de548b5df8,<br>0c2c8280701706e0772cb9be83502096e94ad4d9c21d576db0bc627e1e84b579,<br>5f3d1f17033d85b85f3bd5ae55cb720e53b31f1679d52986c8d635fd1ce0c08a  |
|                     | Domains   | brandnav-cms-storage[.]s3[.]amazonaws[.]com,<br>abode-dashboard-media[.]s3[.]ap-south-1.amazonaws[.]com,<br>applr-malbbal[.]s3[.]ap-northeast-2[.]amazonaws[.]com   |
| <u>Qilin</u>        | URL       | hxxp[:]//184[.]174[.]96[.]70  |
|                     | IPv4      | 180[.]131[.]145[.]73  |
| <u>BianLian</u>     | IPv4:Port | 64[.]190[.]113[.]215[:]:443,<br>15[.]237[.]93[.]235[:]:443,<br>94[.]198[.]40[.]6[:]:20033,<br>94[.]198[.]40[.]6[:]:20007,<br>139[.]162[.]1[.]232[:]:8443,<br>49[.]232[.]6[.]238[:]:443,<br>170[.]64[.]148[.]46[:]:443   |
| <u>RansomExx</u>    | SHA256    | bb12b7c4169e2a86a67a86f03048baa282688d36ef0ae3251bc1ace317c26af9,<br>6b667bb7e4f3f2cb6c6f2d43290f32f41ae9f0d6ed34b818d78490050f7582a1,<br>78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d,<br>08113ca015468d6c29af4e4e4754c003dacc194ce4a254e15f38060854f18867,<br>cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849,<br>843b8434ab69089970530b0d1a9865a89d25aed88bc98d91845bfe41a6dfc31b |
| <u>PipeMagic</u>    | SHA256    | 945a02cdbbd8772f5b0a30f047ae6450ee77a14fef5046af252565a9b524c88f,<br>d9cb912e6ca4dc22515b9dfddced01a96f6de2fd51169597d437d390d5d868f1,<br>2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe  |

# 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  
**May 27, 2025 • 3:30 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)