

Date of Publication  
June 30, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

23 to 29 JUNE 2025

# Table Of Contents

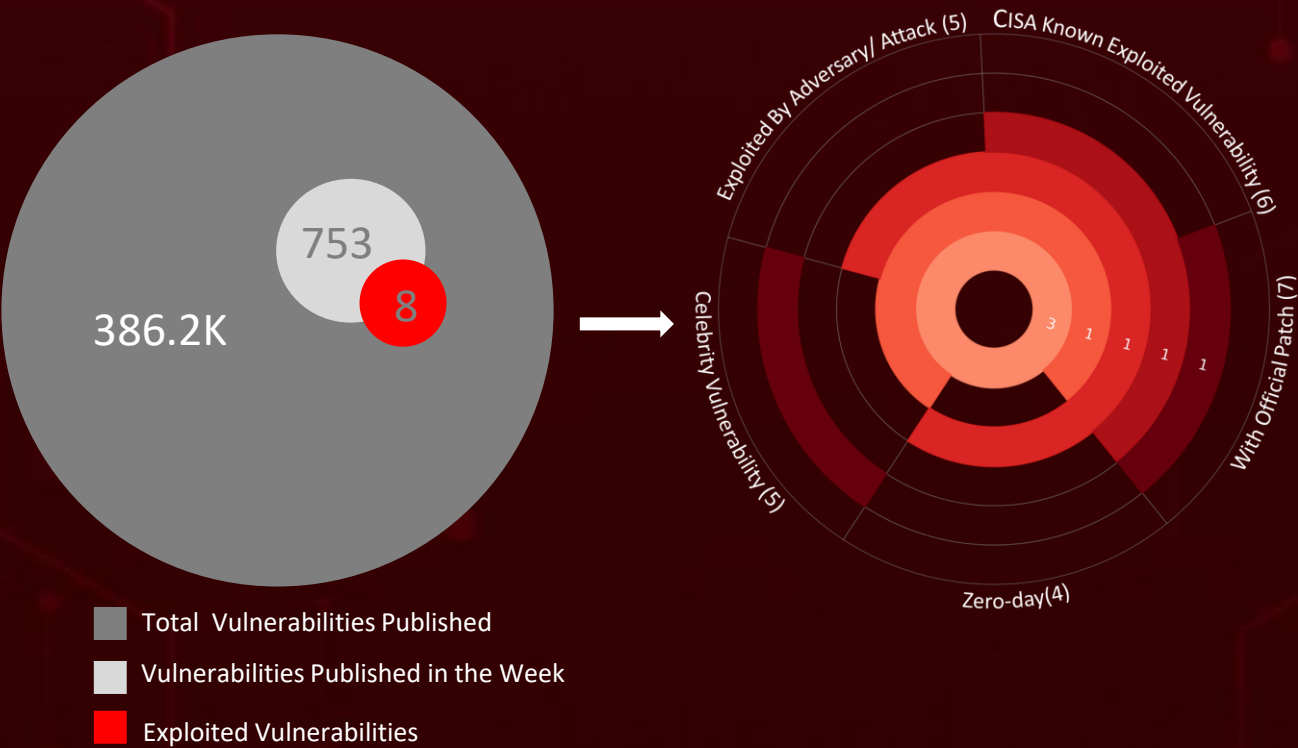
|                                  |    |
|----------------------------------|----|
| <u>Summary</u>                   | 03 |
| <u>High Level Statistics</u>     | 04 |
| <u>Insights</u>                  | 05 |
| <u>Targeted Countries</u>        | 06 |
| <u>Targeted Industries</u>       | 07 |
| <u>Top MITRE ATT&amp;CK TTPs</u> | 07 |
| <u>Attacks Executed</u>          | 08 |
| <u>Vulnerabilities Exploited</u> | 14 |
| <u>Adversaries in Action</u>     | 20 |
| <u>Recommendations</u>           | 22 |
| <u>Threat Advisories</u>         | 23 |
| <u>Appendix</u>                  | 24 |
| <u>What Next?</u>                | 27 |

# Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **nine** attacks, reported **eight** vulnerabilities, and identified **two** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Recent Citrix NetScaler flaws, **CVE-2025-6543** (memory overflow) and CVE-2025-5777 (CitrixBleed 2), pose severe threats like DoS, session hijacking, and MFA bypass. CVE-2025-6543 is actively exploited, CVE-2025-5777 may soon be weaponized. Google patched **CVE-2025-2783**, a Chrome flaw exploited by TaxOff in Operation ForumTroll. The group uses the Trinper backdoor for data theft and control.

Additionally, **APT28** targeted government agencies using spear-phishing via Signal to deploy BEARDSHELL and COVENANT malware. Using fileless techniques and cloud services, they achieved stealthy, persistent access. **BERT ransomware**, active since March 2025, is a multi-platform threat using REvil code and demanding Bitcoin via Session messenger. Its double-extortion tactics and rapid spread across critical sectors pose a growing risk to global enterprises. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

9

Attacks  
Executed

8

Vulnerabilities  
Exploited

2

Adversaries in  
Action

- [BERT Ransomware](#)
- [Prometei](#)
- [PoshC2](#)
- [Chisel](#)
- [Classroom Spy](#)
- [BeardShell](#)
- [Covenant](#)
- [SlimAgent](#)
- [Trinper](#)
- [CVE-2021-27065](#)
- [CVE-2021-26858](#)
- [CVE-2017-0144](#)
- [CVE-2019-0708](#)
- [CVE-2025-2783](#)
- [CVE-2025-49144](#)
- [CVE-2025-6543](#)
- [CVE-2025-5777](#)
- [APT28](#)
- [TaxOff](#)



# Insights

## CVE-2025-49144

is a flaw in the Notepad++ installer that allows attackers to hijack installations via malicious files in the Downloads folder.

## APT28

targeted government agencies via Signal app to deliver BEARDSHELL and COVENANT malware, enabling stealthy remote access and data exfiltration via cloud services.

## Prometei v3,

a Monero-mining botnet, had infected over 10,000 systems by early 2023. In March 2025, it evolved with new Linux-specific variants, extending its reach and threat capabilities.

Google fixed **CVE-2025-2783**, a Chrome flaw exploited by TaxOff using the Trinper backdoor.

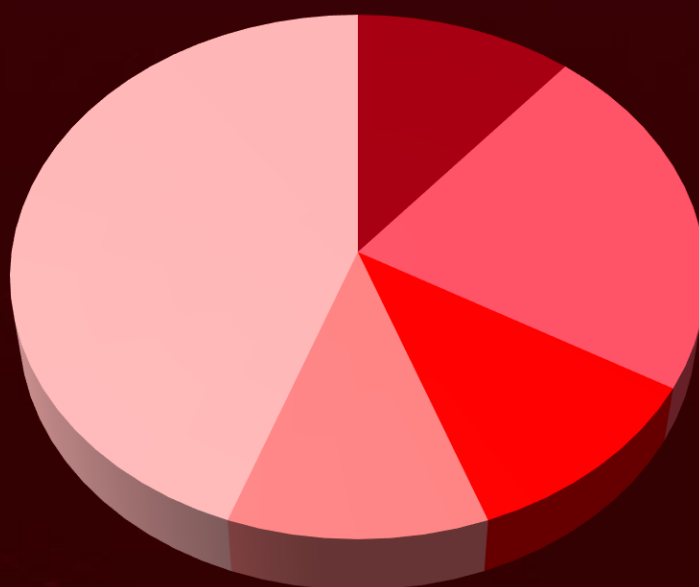
## CL-CRI-1014

targets Africa's financial sector using disguised open-source tools for covert access and darknet monetization, amid rising regional cybercrime.

## BERT

**ransomware**, active since March 2025, uses REvil code and double-extortion tactics, demanding Bitcoin via Session. It poses a rising threat across critical sectors.

## Threat Distribution



■ Ransomware ■ Backdoor ■ Botnet ■ Framework ■ Tool

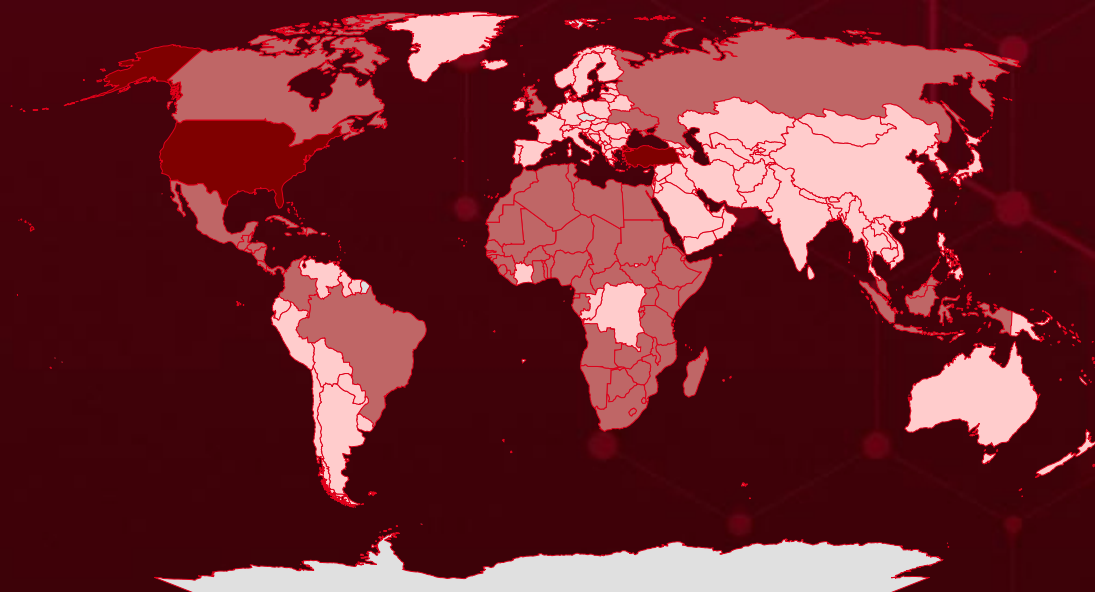


# Targeted Countries

Most



Least



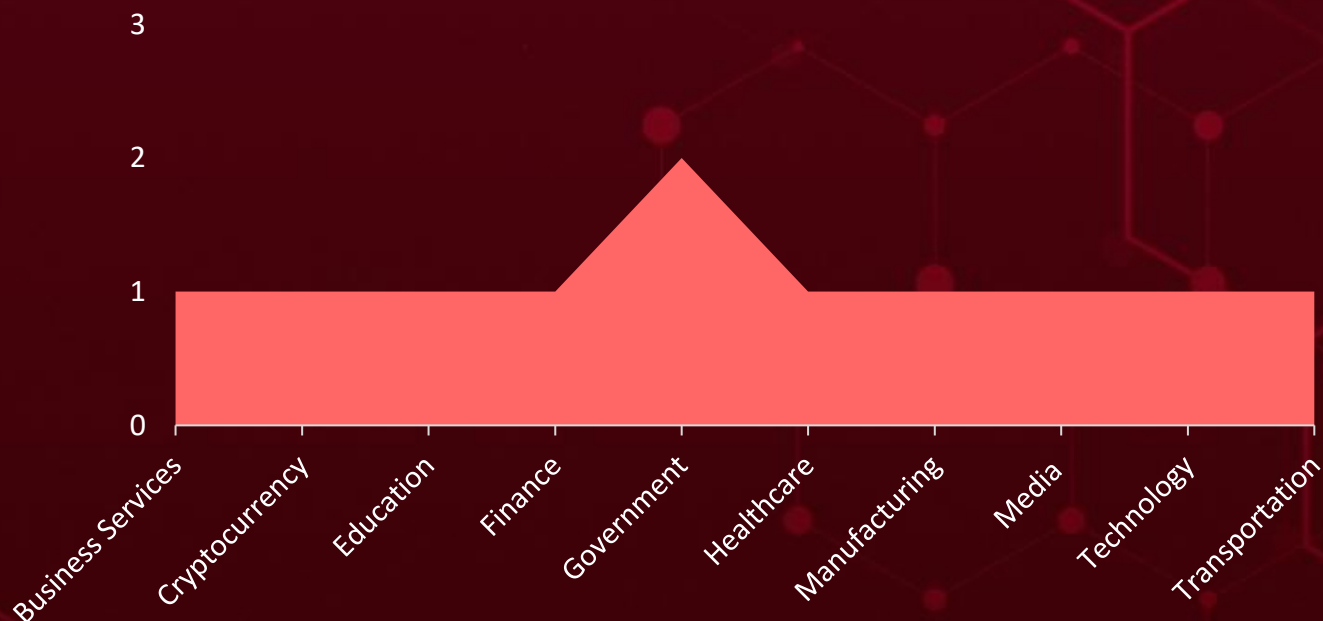
Powered by Bing

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

| Countries             | Countries                        | Countries             | Countries        |
|-----------------------|----------------------------------|-----------------------|------------------|
| Turkey                | Cabo Verde                       | Dominica              | Somalia          |
| United States         | Morocco                          | Malaysia              | Guatemala        |
| South Africa          | Cameroon                         | Dominican Republic    | South Sudan      |
| Namibia               | Niger                            | Mauritania            | Guinea           |
| Malawi                | Canada                           | Egypt                 | Taiwan           |
| Bahamas               | Russia                           | Mexico                | Guinea-Bissau    |
| Saint Kitts and Nevis | Central African Republic         | El Salvador           | Togo             |
| Barbados              | Saint Vincent and the Grenadines | Mozambique            | Haiti            |
| Antigua and Barbuda   | Chad                             | Equatorial Guinea     | Tunisia          |
| Belize                | Sierra Leone                     | Nicaragua             | Honduras         |
| Mauritius             | Colombia                         | Eritrea               | Uganda           |
| Benin                 | Sudan                            | Nigeria               | Indonesia        |
| Panama                | Comoros                          | Eswatini              | United Kingdom   |
| Botswana              | Trinidad and Tobago              | Republic of the Congo | Ivory Coast      |
| Senegal               | Costa Rica                       | Ethiopia              | Zambia           |
| Brazil                | Ukraine                          | Rwanda                | Jamaica          |
| Tanzania              | Cuba                             | Gabon                 | Yemen            |
| Angola                | Zimbabwe                         | Saint Lucia           | Peru             |
| Lesotho               | Democratic Republic of the Congo | Gambia                | Palau            |
| Burkina Faso          | Liberia                          | Sao Tome and Principe | India            |
| Libya                 | Djibouti                         | Ghana                 | Fiji             |
| Burundi               | Madagascar                       | Algeria               | Uzbekistan       |
| Mali                  |                                  | Kenya                 | Papua New Guinea |
|                       |                                  |                       | Venezuela        |
|                       |                                  |                       | Paraguay         |



# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1190

Exploit Public-Facing Application

### T1090

Proxy

### T1566

Phishing

### T1068

Exploitation for Privilege Escalation

### T1204

User Execution

### T1078

Valid Accounts

### T1572

Protocol Tunneling

### T1588.002

Tool

### T1027

Obfuscated Files or Information

### T1204.001

Malicious Link

### T1588

Obtain Capabilities

### T1036

Masquerading

### T1203

Exploitation for Client Execution

### T1566.001

Spearphishing Attachment

### T1588.005

Exploits

### T1588.006

Vulnerabilities

### T1105

Ingress Tool Transfer

### T1041

Exfiltration Over C2 Channel

### T1133

External Remote Services



# Attacks Executed

| NAME                   | OVERVIEW   | DELIVERY METHOD                  | TARGETED CVEs     |
|------------------------|--|----------------------------------|-------------------|
| <u>BERT Ransomware</u> | BERT ransomware, active since March 2025, has rapidly evolved into a multi-platform threat targeting systems across critical sectors. Leveraging REvil's code and demanding Bitcoin via the Session messenger, the campaign’s growing operational footprint and double-extortion tactics signal a persistent and escalating threat landscape for global enterprises. | Phishing                         | -                 |
| TYPE                   |  | IMPACT                           | AFFECTED PRODUCTS |
| Ransomware             |  |                                  | Windows, Linux    |
| ASSOCIATED ACTOR       |  |                                  | PATCH LINK        |
| -                      |  | Data theft and Data exfiltration | -                 |
| IOC TYPE               | VALUE  |                                  |                   |
| SHA256                 | 6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02, ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be, f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799, 78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c, 8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311                             |                                  |                   |

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>Prometei</u>  | By early 2023, the Prometei v3 botnet, an upgraded version of the Prometei botnet malware, had compromised over 10,000 systems mining the Monero cryptocurrency. In its latest iteration, identified in March 2025, Prometei stepped up with new Linux-specific variants.  | Exploiting vulnerabilities         | CVE-2021-27065<br>CVE-2021-26858<br>CVE-2017-0144<br>CVE-2019-0708   |
| TYPE             |  | IMPACT                             | AFFECTED PRODUCTS  |
| Botnet           |  | Network compromise,<br>Data mining | Windows, Linux   |
| ASSOCIATED ACTOR |  |                                    | PATCH LINK   |
| -                |  |                                    | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a> ;<br><a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a> ;<br><a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708</a> ;<br><a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144</a> |
| IOC TYPE         | VALUE  |                                    |  |
| SHA256           | 46cf75d7440c30cbfd101dd396bb18dc3ea0b9fe475eb80c4545868aab5c578c, cc7ab872ed9c25d4346b4c58c5ef8ea48c2d7b256f20fe2f0912572208df5c1a, 205c2a562bb393a13265c8300f5f7e46d3a1aabe057cb0b53d8df92958500867, 656fa59c4acf841dcc3db2e91c1088daa72f99b468d035ff79d31a8f47d320ef, 67279be56080b958b04a0f220c6244ea4725f34aa58cf46e5161cfa0af0a3fb0 |                                    |  |

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>BeardShell</u> | BEARDSHELL is a custom backdoor developed by APT28, written in C++, and designed for stealthy remote access. It executes decrypted PowerShell scripts directly in memory and communicates with command-and-control servers via the Icedrive cloud API. The malware uses ChaCha20-Poly1305 encryption and system-specific directories to evade detection and blend in with normal traffic. | Phishing        | -                 |
| TYPE              |   | IMPACT          | AFFECTED PRODUCTS |
| Backdoor          |   |                 | Windows           |
| ASSOCIATED ACTOR  |   |                 | PATCH LINK        |
| APT28             |   |                 | -                 |
| IOC TYPE          | VALUE   |                 |                   |
| SHA256            | d1deeaf0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a, 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1  |                 |                   |

| NAME             | OVERVIEW   | DELIVERY METHOD   | TARGETED CVE     |
|------------------|--|-------------------|------------------|
| <u>Covenant</u>  | Covenant is an open-source .NET-based command-and-control (C2) framework often used by both red teams and threat actors like APT28. In this campaign, it was loaded in memory to enable fileless execution and stealthy communication. It connected to attacker-controlled Koofr cloud storage for payload delivery and command execution. | Phishing          | -                |
| TYPE             |  | IMPACT            | AFFECTED PRODUCT |
| Framework        |  | Data exfiltration | Windows          |
| ASSOCIATED ACTOR |  |                   | PATCH LINK       |
| APT28            |  |                   | -                |
| IOC TYPE         | VALUE  |                   |                  |
| SHA256           | 84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460   |                   |                  |

| NAME             | OVERVIEW  | DELIVERY METHOD                  | TARGETED CVE     |
|------------------|---|----------------------------------|------------------|
| <u>SlimAgent</u> | SLIMAGENT is a C++-based malicious tool used by APT28 to capture screenshots from infected systems. It leverages Windows GDI functions to take screenshots, encrypts them using AES and RSA, and stores them locally with timestamps. | Dropped via Covenant             | -                |
| TYPE             |   | IMPACT                           | AFFECTED PRODUCT |
| Tool             |   | Data theft and Data exfiltration | Windows          |
| ASSOCIATED ACTOR |   |                                  | PATCH LINK       |
| APT28            |   |                                  | -                |
| IOC TYPE         | VALUE   |                                  |                  |
| SHA256           | 9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c  |                                  |                  |
| MD5              | 889b83d375a0fb00670af5276816080e  |                                  |                  |

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="#">PoshC2</a> | PoshC2 is an open-source post-exploitation and command-and-control (C2) framework used by attackers to control compromised systems. Written in PowerShell and Python, it enables remote execution, credential harvesting, and lateral movement. Though originally developed for legitimate penetration testing, it is often abused by threat actors. | Phishing        | -                |
| TYPE                   |  | IMPACT          | AFFECTED PRODUCT |
| Tool                   |  |                 | -                |
| ASSOCIATED ACTOR       |  |                 | PATCH LINK       |
| -                      |  |                 | -                |
| IOC TYPE               | VALUE  |                 |                  |
| SHA256                 | e14b07b67f1a54b02fc6b65fdbba3c9e41130f283bfea459afa6bee763d3756f8  |                 |                  |

| NAME                   | OVERVIEW   | DELIVERY METHOD | TARGETED CVE     |
|------------------------|--|-----------------|------------------|
| <a href="#">Chisel</a> | Chisel is a fast TCP/UDP tunnel, used to bypass firewalls and enable covert communication between systems. It acts as a reverse proxy, commonly used in red team operations and by threat actors. Though designed for legitimate network debugging, it's often misused for data exfiltration and C2 communication. | -               | -                |
| TYPE                   |  | IMPACT          | AFFECTED PRODUCT |
| Tool                   |  |                 | -                |
| ASSOCIATED ACTOR       |  |                 | PATCH LINK       |
| -                      |  |                 | -                |
| IOC TYPE               | VALUE  |                 |                  |
| SHA256                 | e788f829b1a0141a488afb5f82b94f13035623609ca3b83f0c6985919cd9e83b   |                 |                  |

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="#">Classroom Spy</a> | Classroom Spy is a remote monitoring software designed for educators to oversee student computer activity in classrooms. It allows viewing screens, controlling systems, and managing student behavior during lessons. However, it is misused as spyware by malicious actors for unauthorized surveillance. | -   | -                |
| TYPE                          |   | IMPACT                                    | AFFECTED PRODUCT |
| Tool                          |   | Unauthorized monitoring, privacy invasion | -                |
| ASSOCIATED ACTOR              |   |   | PATCH LINK       |
| -                             |   |   | -                |
| IOC TYPE                      | VALUE   |   |                  |
| SHA256                        | 831d98404ce5e3e5499b558bb653510c0e9407e4cb2f54157503a0842317a363  |   |                  |



| NAME                    | OVERVIEW   | DELIVERY METHOD | TARGETED CVE     |
|-------------------------|--|-----------------|------------------|
| <a href="#">Trinper</a> | Trinper is a credential-stealing malware designed to extract sensitive information such as login credentials and system details from infected machines. It typically targets Windows systems and uses obfuscation techniques to evade detection. | Phishing        | -                |
| TYPE                    |  | IMPACT          | AFFECTED PRODUCT |
| Backdoor                |  |                 | Windows          |
| ASSOCIATED ACTOR        |  |                 | PATCH LINK       |
| -                       |  |                 | -                |
| IOC TYPE                | VALUE  |                 |                  |
| SHA256                  | f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666, d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2, 99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96   |                 |                  |



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-2021-27065</u>   | ProxyLogon              | Microsoft Exchange Server  | -   |
|   | ZERO-DAY                |  |   |
|   |                         | AFFECTED CPE   | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME  | CISA KEY                | cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*                                    | Prometei botnet   |
| Microsoft Exchange Server Remote Code Execution Vulnerability |                         |  |   |
|   | CWE ID                  | ASSOCIATED TTPs  | PATCH LINK  |
|   | CWE-22                  | T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a> |




| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|---|---|--|---|
| <u><b>CVE-2021-26858</b></u>                                  | ProxyLogon  | Microsoft Exchange Server  | -   |
|   | <b>ZERO-DAY</b>   |  |   |
|   |  | <b>AFFECTED CPE</b>  | <b>ASSOCIATED ATTACKS/RANSOMWARE</b>  |
| <b>NAME</b>   | <b>CISA KEY</b>   | cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*                                      | Prometei botnet   |
| Microsoft Exchange Server Remote Code Execution Vulnerability |  |  |   |
|   | <b>CWE ID</b>   | <b>ASSOCIATED TTPs</b>   | <b>PATCH LINK</b>   |
|   | CWE-20  | T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a> |

| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS  | ASSOCIATED ACTOR  |
|---|---|--|---|
| <u><b>CVE-2017-0144</b></u>                         | EternalBlue   | Microsoft SMBv1  | -   |
|   | <b>ZERO-DAY</b>   |  |   |
|   |  | <b>AFFECTED CPE</b>  | <b>ASSOCIATED ATTACKS/RANSOMWARE</b>  |
| <b>NAME</b>   | <b>CISA KEY</b>   | cpe:2.3:a:microsoft:server_message_block:1.0:*:*:*:*:*                             | Prometei botnet   |
| Microsoft SMBv1 Remote Code Execution Vulnerability |  |  |   |
|   | <b>CWE ID</b>   | <b>ASSOCIATED TTPs</b>   | <b>PATCH LINK</b>   |
|   | CWE-94  | T1059 : Command and Scripting Interpreter, T1210 : Exploitation of Remote Services | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144</a> |




| CVE ID  | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|---|---|---|---|
| <b><u>CVE-2019-0708</u></b>   | BlueKeep  | Windows: 10 - 11 23H2<br>Windows Server: 2019 - 2022 23H2   | -   |
|   | <b>ZERO-DAY</b>   |   |   |
|   |  | <b>AFFECTED CPE</b>   | <b>ASSOCIATED ATTACKS/RANSOM WARE</b>   |
| <b>NAME</b>   | <b>CISA KEY</b>   | cpe:2.3:o:microsoft:windows:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*                       | Prometei botnet   |
| Microsoft Remote Desktop Services Remote Code Execution Vulnerability |  |   |   |
|   | <b>CWE ID</b>   | <b>ASSOCIATED TTPs</b>  | <b>PATCH LINK</b>   |
|   | CWE-416   | T1021.001: Remote Desktop Protocol, T1068 : Exploitation for Privilege Escalation, T1059: Command and Scripting | <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708</a> |




| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|--|---|---|---|
| <u>CVE-2025-6543</u>   |  | NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46, 13.1 BEFORE 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP  | -   |
|  | ZERO-DAY  |   |   |
|  |  | AFFECTED CPE  | ASSOCIATED ATTACKS/RANSOMWARE   |
| NAME   | CISA KEY  | cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:*<br>cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:* | -   |
| Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability |  |   |   |
|  | CWE ID  | ASSOCIATED TTPs   | PATCH LINK  |
|  | CWE-119   | T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation  | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788</a> |

| CVE ID   | CELEBRITY VULNERABILITY   | AFFECTED PRODUCTS   | ASSOCIATED ACTOR  |
|--|---|---|---|
| <u><b>CVE-2025-5777</b></u>  | CitrixBleed 2   | NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS  | -   |
|  | <b>ZERO-DAY</b>   |   |   |
|  |    | <b>AFFECTED CPE</b>   | <b>ASSOCIATED ATTACKS/RANSOMWARE</b>  |
| <b>NAME</b>  | <b>CISA KEY</b>   | cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*fips:*:*:*<br>cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*ndcpp:*:*:* | -   |
| Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability |  |   |   |
|  | <b>CWE ID</b>   | <b>ASSOCIATED TTPs</b>  | <b>PATCH LINK</b>   |
|  | CWE-125   | T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation  | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420</a> |

# Adversaries in Action

| NAME   | ORIGIN                          | TARGETED INDUSTRIES                 | TARGETED REGIONS |
|--|---------------------------------|-------------------------------------|------------------|
| <br><br><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>   | Russia                          | Government                          | Ukraine          |
|  | MOTIVE                          |                                     |                  |
|  | Information theft and espionage |                                     |                  |
|  | TARGETED CVE                    | ASSOCIATED ATTACKS/RANSOM WARE      | AFFECTED PRODUCT |
|  | -                               | BeardShell, Covenant, and SlimAgent | Windows          |
| TTPs   |                                 |                                     |                  |
| TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; T1567.002; TA0001: Initial Access; TA0010: Exfiltration; T1546: Event Triggered Execution; TA0002: Execution; TA0011; TA0004: Privilege Escalation; TA0040: Command and Control; T1564: Hide Artifacts; T1567: Exfiltration to Cloud Storage: Exfiltration Over Web Service; T1041: Exfiltration Over C2 Channel: Impact; T1059.005: Visual Basic; T1546.015: Component Object Model HijackingT1566.003; T1566: Spearphishing via Service Phishing; T1059: Command and Scripting Interpreter; T1053.005: Scheduled Task; T1071.001: Web Protocols; T1021: Remote Services; T1082; T1574.001: DLL; T1218: System Binary Proxy Execution; T1071: Application Layer Protocol; T1204: User Execution; T1204.002: Malicious File; T1562; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1053: Impair Defenses; T1573: Encrypted Channel; T1003: OS Credential Dumping; T1113: System Information Discovery: Screen Capture; T1036: Masquerading: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1102: Web Service |                                 |                                     |                  |

| NAME   | ORIGIN                          | TARGETED INDUSTRIES  | TARGETED COUNTRIES       |
|--|---------------------------------|--|--------------------------|
| <br><b>TaxOff</b> | -                               | Media Outlets, Educational Institutions and Government Organizations | Russia                   |
|  | <b>MOTIVE</b>                   |  |                          |
|  | Information theft and espionage |  |                          |
|  | <b>TARGETED CVEs</b>            | <b>ASSOCIATED ATTACKS/RANSOM WARE</b>                                | <b>AFFECTED PRODUCTS</b> |
|  | -                               | Trinper  | -                        |

### TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1106: Native API; T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1041: Exfiltration Over C2 Channel; T1572: Protocol Tunneling; T1070: Indicator Removal; T1070.004: File Deletion; T1070.009: Clear Persistence; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1056: Input Capture; T1056.001: Keylogging; T1057: Process Discovery; T1083: File and Directory Discovery; T1115: Clipboard Data; T1071: Application Layer Protocol; T1090: Proxy; T1090.004: Domain Fronting; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actors **APT28, TaxOff**, and malware **BERT Ransomware, Prometei, PoshC2, Chisel, Classroom Spy, BeardShell, Covenant, SlimAgent, Trinper**.

## 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

- Running a Scan to discover the assets impacted by the **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT28, TaxOff**, and malware **BERT Ransomware, Prometei, PoshC2, Chisel, Classroom Spy, BeardShell, SlimAgent**, in Breach and Attack Simulation(BAS).



# Threat Advisories

[BERT Ransomware Quietly Gains Global Ground](#)

[Prometei Botnet's Persistent Playbook](#)

[APT28 Targets Government Agencies with BEARDSHELL and COVENANT](#)

[Cybercrime Surge Targets Africa's Financial Hubs](#)

[Chrome Zero-Day Exploited in the Wild](#)

[CVE-2025-49144: A Silent Shortcut to SYSTEM Privileges in Notepad++](#)

[Multiple Flaws in Citrix NetScaler ADC and Gateway Pose Immediate Threat](#)

# 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>BERT Ransomware</u></b> | SHA256 | 6182df9c60f9069094fb353c4b3294d13130a71f3e677566267d4419f281ef02,<br>ced4ed5e5ef7505dd008ed7dd28b8aff38df7febe073d990d6d74837408ea4be,<br>f2dc218ea8e2caa8668e54bae6561afd9fbf035a40b80ce9e847664ff0809799,<br>78eb838238dad971dcbc46b86491d95e297f3d47dc770de5c43af3163990d31c,<br>8478d5f5a33850457abc89a99718fc871b80a8fb0f5b509ac1102f441189a311   |
| <b><u>Prometei</u></b>        | SHA256 | 46cf75d7440c30cbfd101dd396bb18dc3ea0b9fe475eb80c4545868aab5c578c,<br>cc7ab872ed9c25d4346b4c58c5ef8ea48c2d7b256f20fe2f0912572208df5c1a,<br>205c2a562bb393a13265c8300f5f7e46d3a1aabe057cb0b53d8df92958500867,<br>656fa59c4acf841dcc3db2e91c1088daa72f99b468d035ff79d31a8f47d320ef,<br>67279be56080b958b04a0f220c6244ea4725f34aa58cf46e5161cfa0af0a3fb0,<br>7a027fae1d7460fc5fccaf8bed95e9b28167023efcbb410f638c5416c6af53ff,<br>87f5e41cbc5a7b3f2862fed3f9458cd083979dfce45877643ef68f4c2c48777e,<br>b1d893c8a65094349f9033773a845137e9a1b4fa9b1f57bdb57755a2a2dcb708, |

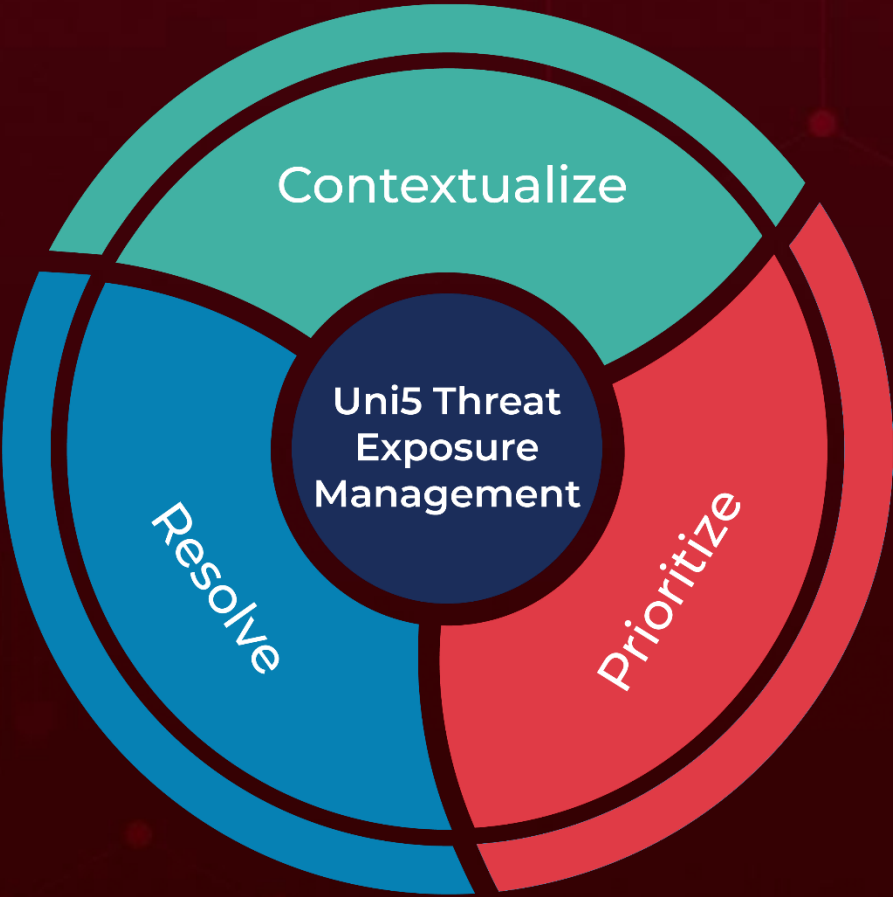
| Attack Name          | TYPE   | VALUE  |
|----------------------|--------|--|
| <u>Prometei</u>      | SHA256 | d21c878dcc169961bebd6e7712b46adf5ec3818cc9469debf1534ffa8d74fb7,<br>d4566c778c2c35e6162a8e65bb297c3522dd481946b81baffc15bb7d7a4fe531,<br>00ad8a3aba502de1235773e96d3674e15b6f72187545c09ccfd8e6b3c91300bc  |
| <u>BeardShell</u>    | SHA256 | d1deef0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a,<br>2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1   |
| <u>Covenant</u>      | SHA256 | 84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460   |
| <u>SlimAgent</u>     | SHA256 | 9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c   |
|                      | MD5    | 889b83d375a0fb00670af5276816080e   |
| <u>PoshC2</u>        | SHA256 | e14b07b67f1a54b02fc6b65fdb63c9e41130f283bfea459afa6bee763d3756f8   |
| <u>Chisel</u>        | SHA256 | e788f829b1a0141a488afb5f82b94f13035623609ca3b83f0c6985919cd9e83b   |
| <u>Classroom Spy</u> | SHA256 | 831d98404ce5e3e5499b558bb653510c0e9407e4cb2f54157503a0842317a363   |
| <u>Trinper</u>       | SHA256 | f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666,<br>d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2,<br>99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96 |

| Attack Name    | TYPE | VALUE  |
|----------------|------|--|
| <u>Trinper</u> | SHA1 | 20943541522cd3937b275c42016ad3e1e64e3f38,<br>d9fa06025ecd08fc417c9948148e7827280365f2,<br>39ecc624bd2d52db083424fbb3a47b0c60f5ae4e |
|                | MD5  | 16f6227f760487a70a3168cf9a497ac3,<br>dba17d2faa311f28e68477ea5cc1a300,<br>1b7b4608f2c9e0a4863a00edd60c3b78                         |

# 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  
**June 30, 2025 • 10:30 PM**

© 2025 All Rights are Reserved by Hive Pro



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