Date of Publication
April 21, 2025

Hive Pro

HiveForce Labs

# WEEKLY
# THREAT DIGEST

## Attacks, Vulnerabilities and Actors

14 to 20 APRIL 2025

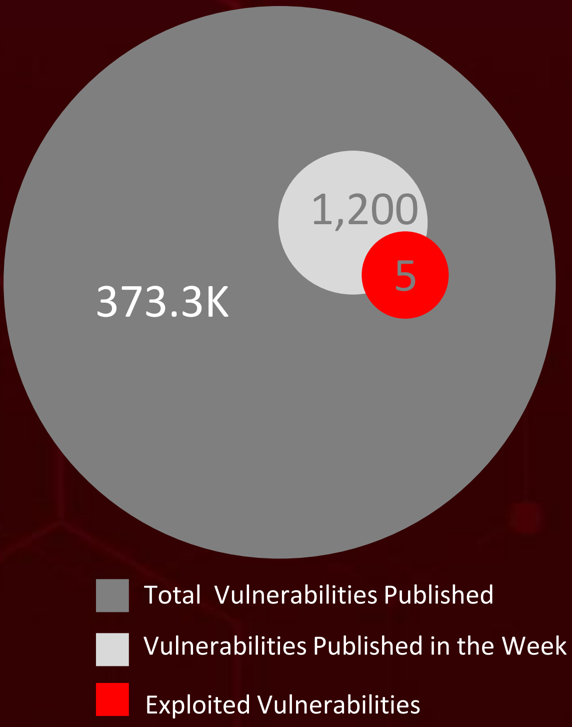
# Table Of Contents

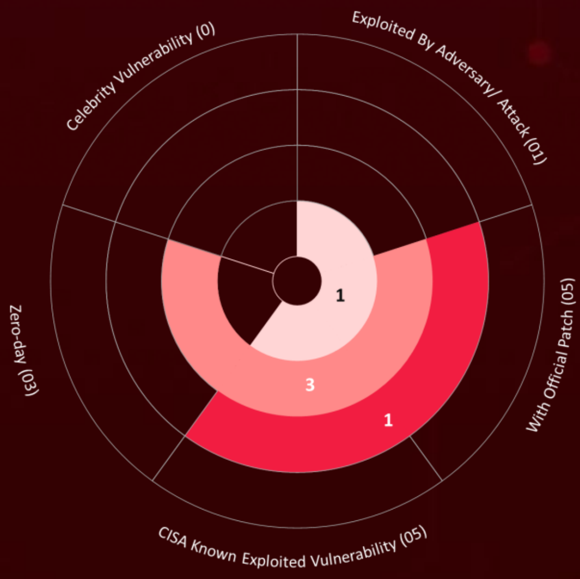
# Summary

HiveForce Labs has identified a surge in cyber threats, with **nine** attacks executed, **five** vulnerability uncovered, and **two** active adversaries exposed in the past week alone highlighting the relentless nature of cyberattacks.

HiveForce Labs has uncovered a fresh wave of cyber threats, headlined by two actively exploited zero-day vulnerabilities in Apple products **CVE-2025-31200** and **CVE-2025-31201** used in a highly targeted and sophisticated attack. Simultaneously, **CVE-2025-24054**, a Windows flaw that leaks NTLMv2-SSP hashes through malicious .library-ms files, has seen rapid exploitation despite a patch issued on March 11, with threat actors targeting entities in Poland and Romania.

Adding to the growing list of concerns, **APT29** has launched a deceptive phishing campaign leading to the deployment of a new malware loader, **GRAPELOADER**, using DLL side-loading to gain persistence and contact C2 servers. Meanwhile, a new ransomware strain dubbed "**DOGE BIG BALLS**" a bizarre rebrand of Fog ransomware has emerged, delivered via finance-themed ZIP files. It leverages PowerShell scripting, geolocation, and the old Intel driver bug **CVE-2015-2291**, and comes with an outrageous ransom note. These fast-evolving threats underscore the critical need for swift patching, vigilant defenses, and cybersecurity awareness.





# High Level Statistics

**9**
Attacks Executed

**5**
Vulnerabilities Exploited

**2**
Adversaries in Action

- PlayBoy Locker
- ResolverRAT
- DOGE BIG BALLS
- GammaSteel
- GRAPELOADER
- WINELOADER
- Interlock
- BerserkStealer
- LummaStealer

- CVE-2015-2291
- CVE-2025-31200
- CVE-2025-31201
- CVE-2025-24054
- CVE-2024-43451

- Shuckworm
- APT29

# Insights

**DOGE BIG BALLS** is turning heads, blending finance-themed lures, geolocation, and an old Intel driver bug into one wild and weaponized package.

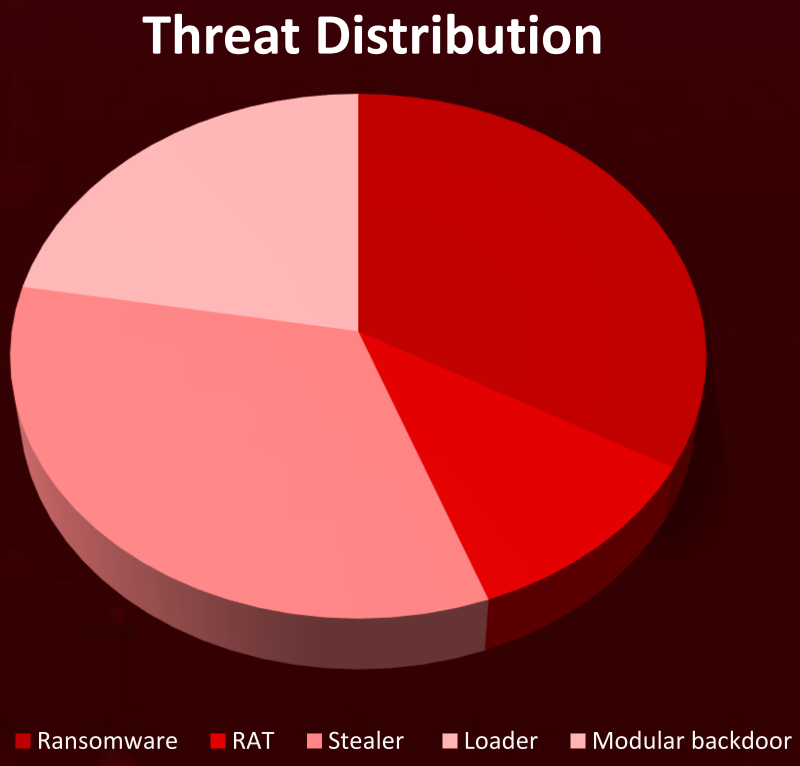
**CoreAudio cracked, RPAC breached:** Apple patches twin zero-days (**CVE-2025-31200 & CVE-2025-31201**) exploited in a precision-driven cyber assault.

**CVE-2025-24054** lets attackers leak hashes via malicious .library-ms files; exploitation kicked off just days after the patch.

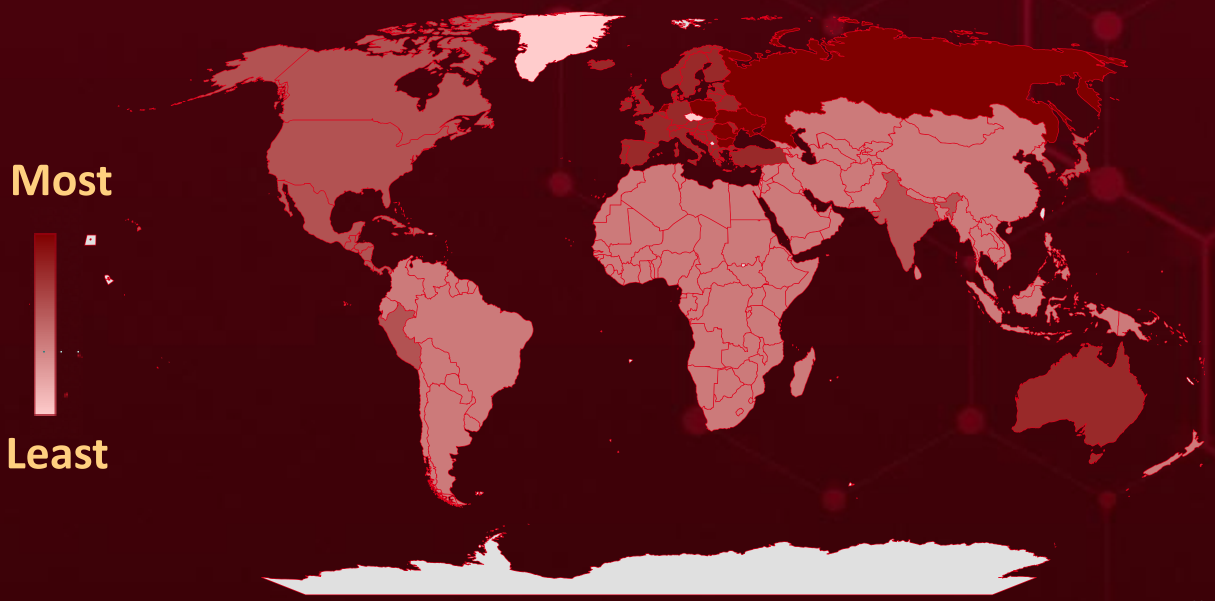
**APT29's classy bait:** Masquerading as a wine-tasting invite from a European ministry, the group used **GRAPELOADER** via DLL side-loading to plant the stealthy **WINELOADER** backdoor and establish long-term access.

**Shuckworm hits Ukraine:** Russia-linked APT resurfaces with a cyber-espionage campaign targeting a Western military mission, using USB-planted LNK files to deploy an upgraded GammaSteel malware variant.

**INTERLOCK Ransomware:** A growing threat with a rare focus on FreeBSD systems and sophisticated double-extortion tactics.



# Targeted Countries



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

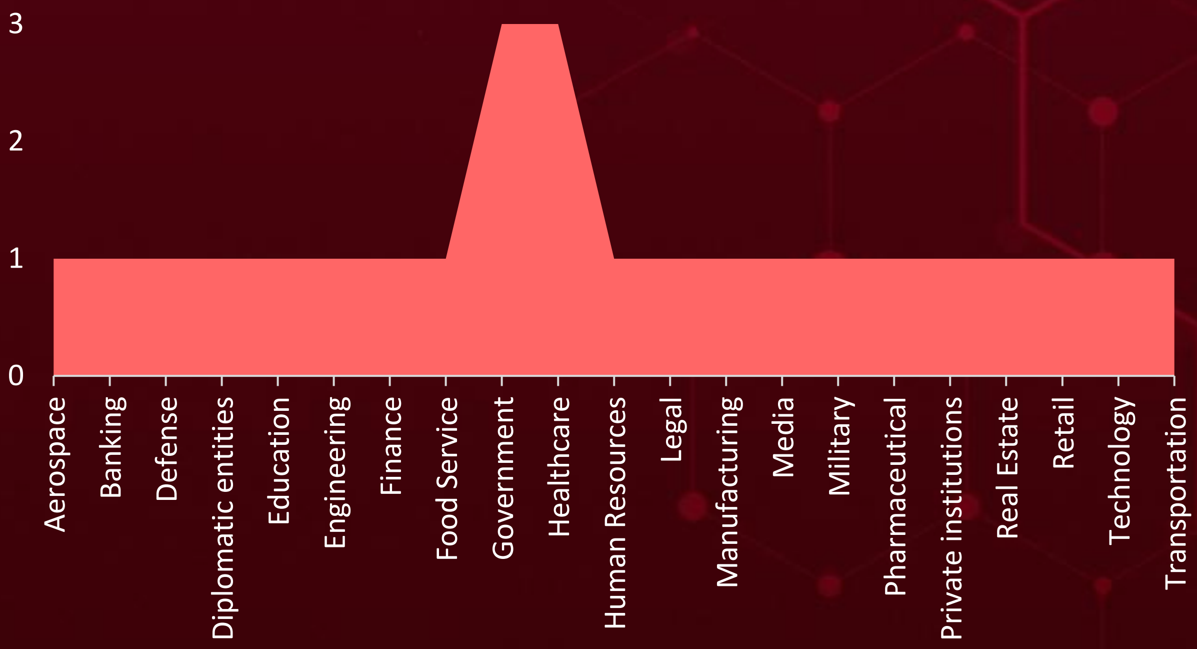
| | Countries |
|---|---|
| 🟥 | Poland |
| 🟥 | Russia |
| 🟥 | Romania |
| 🟥 | Bulgaria |
| 🟥 | Netherlands |
| 🟥 | Ukraine |
| 🟥 | Slovenia |
| 🟥 | Norway |
| 🟥 | Monaco |
| 🟥 | Bosnia and Herzegovina |
| 🟥 | Belarus |
| 🟥 | Albania |
| 🟥 | Belgium |
| 🟥 | Croatia |
| 🟥 | Andorra |
| 🟥 | Denmark |
| 🟥 | Portugal |
| 🟥 | Estonia |
| 🟥 | Serbia |
| 🟥 | Finland |
| 🟥 | Sweden |

| | Countries |
|---|---|
| 🟥 | France |
| 🟥 | Moldova |
| 🟥 | Germany |
| 🟥 | Montenegro |
| 🟥 | Greece |
| 🟥 | North Macedonia |
| 🟥 | Hungary |
| 🟥 | Australia |
| 🟥 | Iceland |
| 🟥 | Austria |
| 🟥 | Ireland |
| 🟥 | San Marino |
| 🟥 | Italy |
| 🟥 | Slovakia |
| 🟥 | Turkey |
| 🟥 | Spain |
| 🟥 | United Kingdom |
| 🟥 | Switzerland |
| 🟥 | Luxembourg |
| 🟥 | Malta |
| 🟥 | Latvia |

| | Countries |
|---|---|
| 🟥 | Lithuania |
| 🟥 | Liechtenstein |
| 🟥 | Antigua and Barbuda |
| 🟥 | Saint Lucia |
| 🟥 | United States |
| 🟥 | Costa Rica |
| 🟥 | Barbados |
| 🟥 | Cuba |
| 🟥 | Jamaica |
| 🟥 | Cyprus |
| 🟥 | Panama |
| 🟥 | Czech Republic (Czechia) |
| 🟥 | South Korea |
| 🟥 | Dominica |
| 🟥 | India |
| 🟥 | Dominican Republic |
| 🟥 | Belize |
| 🟥 | El Salvador |
| 🟥 | Japan |
| 🟥 | Grenada |
| 🟥 | Nicaragua |
| 🟥 | Guatemala |

| | Countries |
|---|---|
| 🟥 | Peru |
| 🟥 | Haiti |
| 🟥 | Canada |
| 🟥 | Holy See |
| 🟥 | Trinidad and Tobago |
| 🟥 | Honduras |
| 🟥 | Mexico |
| 🟥 | Pakistan |
| 🟥 | State of Palestine |
| 🟥 | Cameroon |
| 🟥 | Bangladesh |
| 🟥 | Tuvalu |
| 🟥 | Djibouti |
| 🟥 | Burundi |
| 🟥 | Côte d'Ivoire |
| 🟥 | Solomon Islands |
| 🟥 | Guinea |
| 🟥 | Thailand |
| 🟥 | Guinea-Bissau |
| 🟥 | North Korea |
| 🟥 | Guyana |
| 🟥 | Paraguay |

# Targeted Industries



# TOP MITRE ATT&CK TTPs

**T1566**
Phishing

**T1027**
Obfuscated Files or Information

**T1059**
Command and Scripting Interpreter

**T1547**
Boot or Logon Autostart Execution

**T1059.001**
PowerShell

**T1218**
System Binary Proxy Execution

**T1547.001**
Registry Run Keys / Startup Folder

**T1041**
Exfiltration Over C2 Channel

**T1070**
Indicator Removal

**T1486**
Data Encrypted for Impact

**T1070.004**
File Deletion

**T1005**
Data from Local System

**T1204**
User Execution

**T1082**
System Information Discovery

**T1016**
System Network Configuration Discovery

**T1105**
Ingress Tool Transfer

**T1543**
Create or Modify System Process

**T1566.001**
Spearphishing Attachment

**T1574.002**
DLL Side-Loading

**T1036**
Masquerading

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| PlayBoy Locker | PlayBoy Locker is a sophisticated ransomware strain operated by a group active since September 2024. Offered as a service, it provides threat actors with customizable ransomware payloads, a web-based management dashboard, and dark web-based customer support. Written in C++, the malware employs a hybrid encryption scheme that combines the HC-128 stream cipher with the Curve25519 elliptic curve algorithm to lock files. Once inside a network, it performs LDAP scans to discover other machines, attempts lateral movement by replicating itself, and terminates active processes to maximize impact. Infected files are appended with the ".PLBOY" extension, and victims receive a ransom note titled INSTRUCTIONS.txt containing payment and communication details. | phishing emails or vulnerable Remote Desktop Protocol (RDP) services | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | System Compromise, Encrypt Data | Windows, NAS, and ESXi |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | 3030a048f05146b85c458bcabe97968e5efdd81b224b96c30c83b74365839e7b,<br>a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556,<br>a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556 |
| TOR Address | vlofmq2u3f5amxmnblvxaghy73aedwta74fyceywr6eeguw3cn6h6uad[.]onion |

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 |
|---|---|---|---|
| ResolverRAT | ResolverRAT is a stealthy remote access trojan recently uncovered, notable for its sophisticated use of in-memory execution and runtime resolution techniques. ResolverRAT is built to evade both static and behavioral detection mechanisms. It operates entirely in memory, using strong encryption and compression to remain hidden from traditional security tools. Its capabilities include chunked data exfiltration where large files are broken into smaller pieces to mimic normal network activity and parallel command processing, allowing it to execute multiple tasks simultaneously without system instability. | Phishing | - |
| TYPE | | IMPACT | AFFECTED PRODUCTS |
| RAT | | Data Theft | Windows |
| ASSOCIATED ACTOR | | | PATCH LINK |
| - | | | - |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | 80625a787c04188be1992cfa457b11a166e19ff27e5ab499b58e8a7b7d44f2b9 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| DOGE BIG BALLS | DOGE BIG BALLS is a customized and rebranded variant of the Fog ransomware. Designed to do more than just encrypt files, this strain aims to confuse, intimidate, and mislead its victims. A single click initiates a stealthy PowerShell script that checks for administrative privileges before downloading and executing multiple malicious payloads. It encrypts files with a ".flocked" extension, deletes shadow copies, logs its activity, and drops a ransom note that leads victims to a Tor site. There, they're asked to pay $1,000 in Monero and, oddly, to list their top five work achievements. The malware also gathers detailed system information and adds a disturbing twist by including real personal details of an individual. | Phishing, Exploiting Vulnerability | CVE-2015-2291 |
| TYPE | | IMPACT | AFFECTED PRODUCTS |
| Ransomware | | Encrypt Data, System Compromise | iQVW32.SYS, iQVW64.SYS |
| ASSOCIATED ACTOR | | | PATCH LINK |
| - | | | https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | 3d2cbef9be0c48c61a18f0e1dc78501ddabfd7a7663b21c4fcc9c39d48708e91,<br>f08b5316f6bc009d0cb41d4ce0086e615bf130b667cb2cdceecad07fda24fc49 |

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 |
|---|---|---|---|
| GammaSteel | GammaSteel is an information-stealing malware designed to exfiltrate sensitive data from compromised networks. It is delivered via a stealthy PowerShell-based attack chain, allowing it to operate with minimal visibility and evade traditional detection methods. Once deployed, GammaSteel silently harvests data, targeting system information, credentials, and other valuable assets, before transmitting them to attacker-controlled servers. | Using a malicious LNK file on a USB drive | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Stealer | | Data Theft | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Shuckworm | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| GRAPELOADER | GRAPELOADER is a recently identified initial-stage tool designed for host fingerprinting, establishing persistence, and delivering follow-on payloads. GRAPELOADER consistently features a shared code structure, obfuscation techniques, and string decryption methods. Upon execution, it gathers basic system information such as the host name and username and transmits this data to a Command and Control (C2) server. The tool then remains active, awaiting instructions or the delivery of next-stage shellcode, positioning it as a versatile component in multi-stage attack chains. | Phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Loader | | Loads WINELOADER | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| APT29 | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | d931078b63d94726d4be5dc1a00324275b53b935b77d3eed1712461f0c180164,<br>24c079b24851a5cc8f61565176bbf1157b9d5559c642e31139ab8d76bbb320f8 | | |

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 |
|---|---|---|---|
| WINELOADER | A newer variant of the WINELOADER backdoor has emerged, embedded within a 64-bit trojanized DLL named vmtools.dll. While the file claims to export 964 functions, only one of them is used as the true entry point for malicious activity. Notably, the Export Directory reveals RVA duplicity each pair of exported functions shares the same Relative Virtual Address indicating that the DLL actually contains just 482 unique exports. This deceptive export structure, paired with the backdoor’s stealthy execution, suggests a deliberate effort to evade static analysis and blend in with legitimate system components. | Phishing | - |
| TYPE | | IMPACT | AFFECTED PRODUCTS |
| Backdoor | | Data Theft | - |
| ASSOCIATED ACTOR | | | PATCH LINK |
| APT29 | | | - |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | adfe0ef4ef181c4b19437100153e9fe7aed119f5049e5489a36692757460b9f8 |

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 CVEs</th></tr>
<tr><td>Interlock</td><td rowspan="5">INTERLOCK is a rising ransomware group gaining attention for its technical sophistication, including malware compiled in C/C++ for both Windows and Linux systems. While the Windows variant is most commonly observed, what truly sets INTERLOCK apart is its rare and deliberate focus on FreeBSD environments an unusual target in the ransomware ecosystem. The group employs polished double-extortion tactics and operates a data leak site called “Worldwide Secrets Blog,” where stolen data is published and victims are invited to negotiate ransom terms. Once launched, these fake installers execute a PowerShell backdoor, enabling the deployment of additional tools and ultimately delivering the ransomware payload.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Ransomware</td><td rowspan="3">System Compromise, Encrypt Data, Data Theft</td><td>Microsoft Windows, Linux</td></tr>
<tr><td><b>ASSOCIATE D  ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f,<br>4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>BerserkStealer</td><td rowspan="5">BerserkStealer is a credential-stealing malware designed to harvest sensitive information that can be used to facilitate lateral movement across compromised networks. It has been observed packed with the Interlock group’s custom packer, a technique also used to obfuscate other malware families linked to the group.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Stealer</td><td rowspan="3">Data Theft</td><td>Microsoft Windows, Linux</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692</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 CVEs |
|---|---|---|---|
| LummaStealer | Lumma Stealer, also known as LummaC2 Stealer, is an information-stealing malware written in C that has been available as Malware-as-a-Service (MaaS) on Russian-speaking forums since at least August 2022. It primarily targets cryptocurrency wallets and two-factor authentication (2FA) browser extensions, stealing sensitive data from the victim's machine. | Phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Stealer | | Data Theft | Microsoft Windows, Linux |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

| IOC TYPE | VALUE |
|---|---|
| SHA256 | 4672fe8b37b71be834825a2477d956e0f76f7d2016c194f1538139d21703fd6e |

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 |
|---|---|---|---|
| CVE-2015-2291 | ✗ | iQVW32.SYS: Before 1.3.1.0;<br>iQVW64.SYS: Before 1.3.1.0 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw32.sys:1.03.0.7:*:*:*:*:*:*:*<br>cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw64.sys:1.03.0.7:*:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* | DOGE BIG BALLS Ransomware |
| Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-20 | T1059: Command and Scripting Interpreter;<br>T1068: Exploitation for Privilege Escalation;<br>T1499: Endpoint Denial of Service | https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2025-31200 | ✗ | macOS Prior to Version 15.4.1, iOS and iPadOS Prior to Version 18.4.1, tvOS Prior to Version 18.4.1, visionOS Prior to Version 2.4.1 | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:*<br>cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*<br>cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:*<br>cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:* | - |
| Apple Multiple Products Memory Corruption Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-787 | T1059: Command and Scripting Interpreter;<br>T1566: Phishing | https://support.apple.com/en-us/108382 ,<br>https://support.apple.com/en-us/118575 ,<br>https://support.apple.com/en-us/108414 ,<br>https://support.apple.com/en-us/118481 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2025-31201 | ☒ | macOS Prior to Version 15.4.1, iOS and iPadOS Prior to Version 18.4.1, tvOS Prior to Version 18.4.1, visionOS Prior to Version 2.4.1 | - |
|  | ZERO-DAY |  |  |
|  | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:*<br>cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*<br>cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:*<br>cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:* | - |
| Apple Multiple Products Arbitrary Read and Write Vulnerability | ✓ |  |  |
|  | CWE ID | ASSOCIATED TTPs | PATCH LINK |
|  | CWE-287 | T1068: Exploitation for Privilege Escalation;<br>T1203: Exploitation for Client Execution | https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108414 , https://support.apple.com/en-us/118481 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2025-24054 | ✗ | Windows Server 2008 – 2025<br>Windows 10 – 11 24H2 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* | - |
| Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-73 | T1566: Phishing;<br>T1204: User Execution | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2024-43451 | ✗ | Windows Server 2008 – 2025<br>Windows 10 -11 24H2 | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* | - |
| Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-73 | T1566: Phishing;<br>T1204: User Execution | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451 |

# Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">Shuckworm (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Gamaredon, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)</td><td>Russia</td><td rowspan="3">Military</td><td rowspan="3">Ukraine</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>-</td><td>GammaSteel</td><td>-</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; T1091: Replication Through Removable Media; T1567: Exfiltration Over Web Service; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1132: Data Encoding; T1132.001: Standard Encoding; T1001: Data Obfuscation; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1547.009: Shortcut Modification; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1027: Obfuscated Files or Information; T1033: System Owner/User Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">APT29 (aka Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, Blue Kitsune, G0016, Midnight Blizzard, SeaDuke, TA421, UAC-0029, UNC3524, Cranefly , TEMP.Monkeys, Blue Dev 5, NobleBaron, Solar Phoenix, Earth Koshchei)</td><td>Russia</td><td rowspan="3">Embassies, Government, and Diplomatic entities</td><td rowspan="3">Europe</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>GRAPELOADER, WINELOADER</td><td>Windows</td></tr>
<tr></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0007: Discovery; TA0005: Defense Evasion; TA0010: Exfiltration; TA0002: Execution; TA0003: Persistence; TA0001: Initial Access; TA0009: Collection; TA0011: Command and Control; T1566: Phishing; T1204: User Execution; T1204.001: Malicious Link; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1005: Data from Local System; T1566.002: Spearphishing Link; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1016: System Network Configuration Discovery; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1041: Exfiltration Over C2 Channel; T1027.009: Embedded Payloads; T1070.001: Clear Windows Event Logs; T1070: Indicator Removal; T1573.001: Symmetric Cryptography; T1573: Encrypted Channel; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1082: System Information Discovery; T1656: Impersonation</td></tr>
</table>

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **Shuckworm, APT29** and malware **PlayBoy Locker, ResolverRAT, DOGE BIG BALLS, GammaSteel, GRAPELOADER, WINELOADER, Interlock, BerserkStealer, LummaStealer.**

**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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Shuckworm, APT29** and malware **PlayBoy Locker, ResolverRAT, DOGE BIG BALLS, GRAPELOADER, WINELOADER, Interlock** and **BerserkStealer** in Breach and Attack Simulation(BAS).

# Threat Advisories

# 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 |
|---|---|---|
| PlayBoy Locker | SHA256 | 3030a048f05146b85c458bcabe97968e5efdd81b224b96c30c83b74365839e7b,<br>a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556,<br>a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556 |
| | File Name | INSTRUCTIONS.txt |
| | TOR Address | vlofmq2u3f5amxmnblvxaghy73aedwta74fyceywr6eeguw3cn6h6uad[.]onion |
| ResolverRAT | SHA256 | 80625a787c04188be1992cfa457b11a166e19ff27e5ab499b58e8a7b7d44f2b9 |
| DOGE BIG BALLS | SHA256 | 3d2cbef9be0c48c61a18f0e1dc78501ddabfd7a7663b21c4fcc9c39d48708e91,<br>f08b5316f6bc009d0cb41d4ce0086e615bf130b667cb2cdceecad07fda24fc49,<br>8e209e4f7f10ca6def27eabf31ecc0dbb809643feaecb8e52c2f194daa0511aa,<br>805b2f5cab2a4ba6088e6b6f91d6f1f0671c61092b571358969d69ff8c184c30,<br>30a6688899c22a3ce4c1b977fae762e3f7342d776e1aa2c90835e785d42f60c1,<br>ecfed78315f942fe0e6762acd73ef7f30c34620615ef5e71f899e1d069dabd9e,<br>2c38a56beec1f7c8b919a1a2d9f9497358e763a1c8d9d71aa8a0e4ef062d3ec2,<br>4ad9216a0a6ac84a7b0b5593b0fc97e27de9cdfeb84ab7e5339ae5a4102100c0,<br>8d843c757aea85087a95794f93071bfacb7c4db06f33520308f39b97cf88cabb |

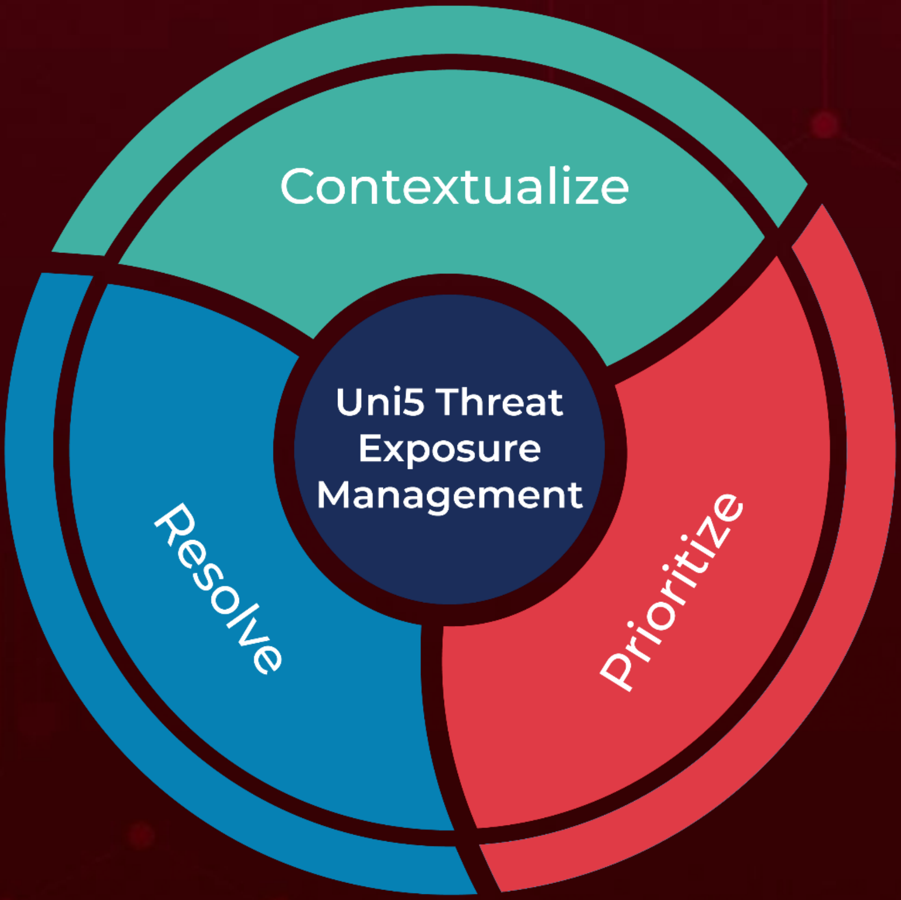
| Attack Name | TYPE | VALUE |
|---|---|---|
| GRAPELOADER | SHA256 | d931078b63d94726d4be5dc1a00324275b53b935b77d3eed1712461f0c180164,<br>24c079b24851a5cc8f61565176bbf1157b9d5559c642e31139ab8d76bbb320f8 |
| WINELOADER | SHA256 | adfe0ef4ef181c4b19437100153e9fe7aed119f5049e5489a36692757460b9f8 |
| Interlock | SHA256 | 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f,<br>4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9,<br>33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9,<br>b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039,<br>a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642,<br>0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea,<br>e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1,<br>f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e |
| BerserkStealer | SHA256 | eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692,<br>a5623b6a6f289bb328e4007385bdb1659407a9e825990a0faaef3625a2e782cf |
| LummaStealer | SHA256 | 4672fe8b37b71be834825a2477d956e0f76f7d2016c194f1538139d21703fd6e |

*A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.*

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

**April 21, 2025 • 6:10 AM**

More at www.hivepro.com