Date of Publication
November 20, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

# THREAT DIGEST

## Attacks, Vulnerabilities and Actors

13 to 19 NOVEMBER 2023

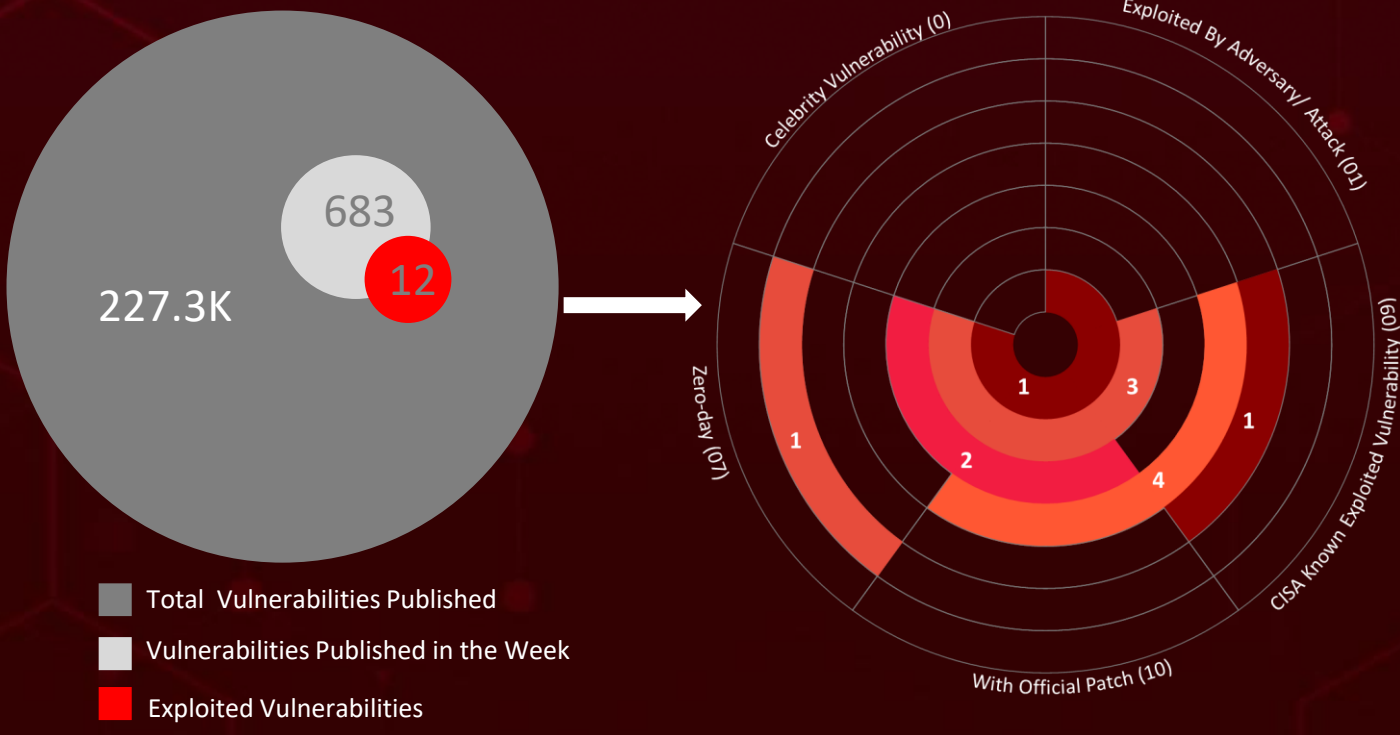
# Table Of Contents

# Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **nine** attacks were executed, **twelve** vulnerabilities were uncovered, and **four** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs revealed that among the **seven zero-day** vulnerabilities, **one** exploit targeting **Zimbra Collaboration** email software has been utilized by **four** distinct groups in attacks. Additionally, **one** vulnerability was identified in **VMware Cloud Director Appliance**, and **five zero-days** were discovered in Microsoft's November 2023 Patch Tuesday.

**TA402** initiated sophisticated phishing campaigns, specifically targeting government entities in the Middle East. The **NoEscape ransomware**, suspected to be a rebrand of Avaddon, is strategically employed in multi-extortion attacks. These attacks are on the rise, posing a significant threat to users worldwide.



# High Level Statistics

**9**
Attacks Executed

**12**
Vulnerabilities Exploited

**4**
Adversaries in Action

- Ducktail
- IronWind
- SharpSploit
- NoEscape
- GhostLocker
- BlackCat
- AveMaria
- Raccoon
- VIDAR

- CVE-2023-36844
- CVE-2023-36845
- CVE-2023-36846
- CVE-2023-36847
- CVE-2023-36851
- CVE-2023-36033
- CVE-2023-36025
- CVE-2023-36036
- CVE-2023-36038
- CVE-2023-36413
- CVE-2023-34060
- CVE-2023-37580

- TA402
- Winter Vivern
- GhostSec
- Scattered Spider

# Insights

**Beyond the Web: Scattered Spider**'s Symphony of Social Engineering in Cyber Espionage

**The Great Exploit:** Decoding the Exploits of **Zimbra's Zero-Day** by **Four** Cunning Groups

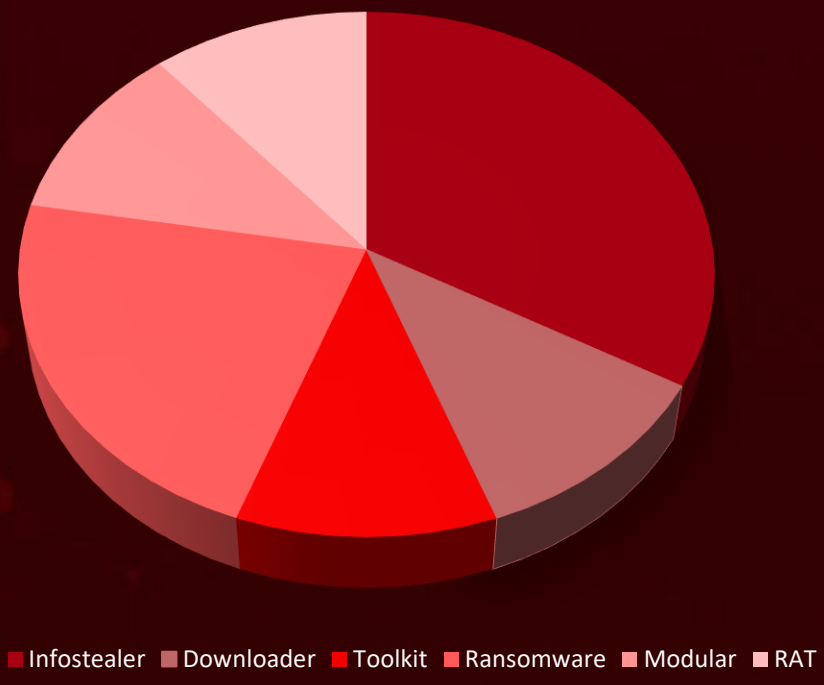
**The Hacktivist Arsenal:** **GhostLocker** RaaS by **GhostSec** Raises Cybersecurity Stakes

**Zero-Day Blitz:** Microsoft's November 2023 Patch Tuesday Unveils **60** Important Flaws Alongside **5** Zero-Days

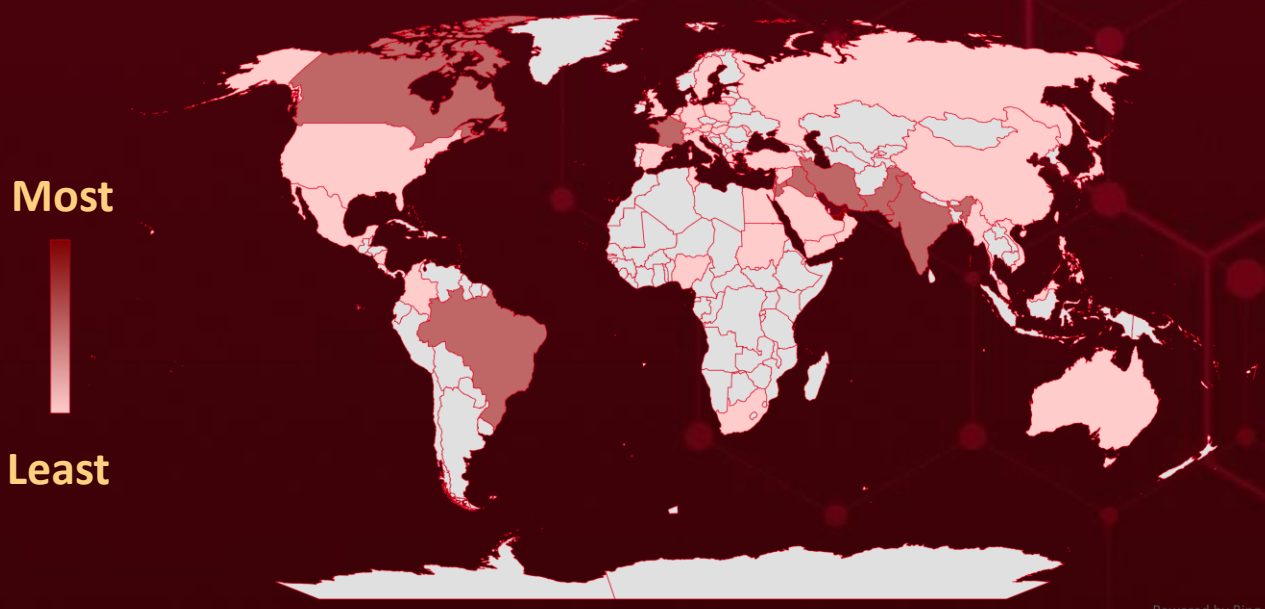
**Middle East Under Siege: TA402**'s Economic-themed Phishing Heist with **IronWind**

**Avaddon's Shadow:** **NoEscape** Ransomware Rises as a Global Financial Threat

## Threat Distribution

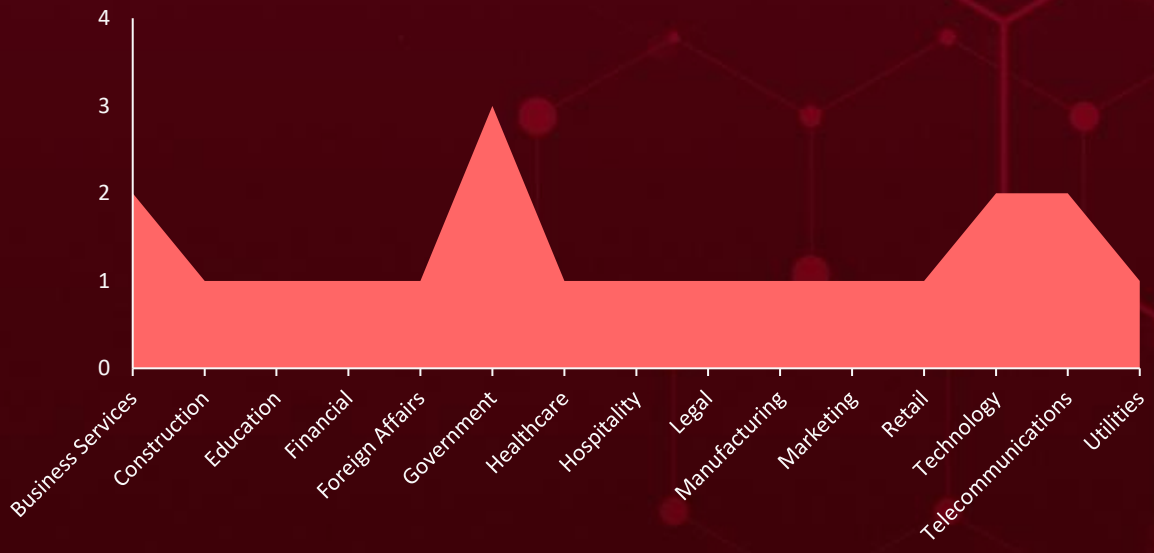


# Targeted Countries




| | Countries | | Countries | | Countries |
|---|---|---|---|---|---|
| | United Arab Emirates | | China | | Turkey |
| | Israel | | Sweden | | Malaysia |
| | Iran | | Colombia | | United States |
| | Pakistan | | Netherlands | | Mauritius |
| | Brazil | | Italy | | Yemen |
| | Iraq | | Nigeria | | Mexico |
| | Canada | | Japan | | Moldova |
| | Jordan | | Cyprus | | |
| | France | | Columbia | | |
| | India | | Philippines | | |
| | Lebanon | | Kuwait | | |
| | Russia | | Puerto Rico | | |
| | Oman | | Switzerland | | |
| | Myanmar | | Republic of Korea | | |
| | Belgium | | Syria | | |
| | Poland | | Saudi Arabia | | |
| | Germany | | Tunisia | | |
| | Spain | | South Korea | | |
| | Greece | | United Kingdom | | |
| | Nicaragua | | Sudan | | |
| | Hungary | | Vietnam | | |
| | Palestine | | Egypt | | |
| | Austria | | Akrotiri and Dhekelia | | |
| | Qatar | | Taiwan | | |
| | Bahrain | | Lithuania | | |
| | South Africa | | Australia | | |

# Targeted Industries




# TOP MITRE ATT&CK TTPs

| | | | | |
|---|---|---|---|---|
| **T1059** Command and Scripting Interpreter | **T1204** User Execution | **T1588** Obtain Capabilities | **T1588.006** Vulnerabilities | **T1543** Create or Modify System Process |
| **T1566** Phishing | **T1560** Archive Collected Data | **T1071.001** Web Protocols | **T1078** Valid Accounts | **T1588.005** Exploits |
| **T1027** Obfuscated Files or Information | **T1486** Data Encrypted for Impact | **T1204.002** Malicious File | **T1055** Process Injection | **T1556** Modify Authentication Process |
| **T1539** Steal Web Session Cookie | **T1071** Application Layer Protocol | **T1567** Exfiltration Over Web Service | **T1082** System Information Discovery | **T1021** Remote Services |

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Ducktail | Ducktail info stealer propagated by masquerading as documents related to projects and products of well-known companies and brands. A distinctive feature of this campaign was the use of Delphi as the programming language, deviating from the previous approach that relied on .NET applications. | Spear-phishing emails | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Infostealer | | Extortion of data | - |
| **ASSOCIATED ACTOR** | | | **PATH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 8eafccab8c6a80356c84c9ae3bd3603262069748be59a8d5aee4dfa3cf4a00a3, 9cf88cfd198e0070bb24868ce56f260f55a4b227e266ebcb37fdb83183299ae5, c2e8bc6389ba6ba32a350312f4fdda33628c806587ade0836f3886e2ffcaf9b2 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| IronWind | TA402 orchestrated a phishing campaign, deploying a file named PPAM. Within this file were three distinct components, facilitating the deployment of a novel initial access downloader known as IronWind. The infiltration of IronWind occurred through the use of timeout.exe. Subsequently, IronWind initiated communication with a C2 domain via an HTTP GET request. | Social Engineering | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Downloader | | Denial of Service, Data Theft, and compromised systems | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| TA402 | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47, 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115, e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c | | |

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 |
|---|---|---|---|
| SharpSploit | The IronWind downloader is designed to establish a connection with a server controlled by the attacker for the retrieval of additional payloads. Among these payloads is a post-exploitation toolkit called SharpSploit, a .NET post-exploitation library written in C#. This process unfolds in a multi-stage sequence | Spear phishing and IronWind | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Toolkit | | Denial of Service, Data Theft, and compromised systems | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| TA402 | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47, ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f, 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| NoEscape | The NoEscape ransomware, suspected to be a rebrand of Avaddon, targets enterprises globally through multi-extortion attacks. Operating as Ransomware-as-a-Service, it encrypts files, changes wallpapers, and demands ransom, emphasizing financial motives via a TOR negotiation site. | Phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Data Theft and Espionage | Windows, Linux, and ESXi |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a, 2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5, 4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e | | |
| SHA1 | ea1f7940271fc80d06b2f222506020b650ad41bc, 30f71a24c15dd81965b12996a79d914acf4f169e, 12dc0a2de3ad30201107bfcb679de5acacf31e5c | | |
| MD5 | 204f028c983f654be32b97e849edeaab, 47ae17d89c2d9b6acdc7458f5df1c6f7, 5779cec690b5bbc61687381ae8a8d518 | | |

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 |
|---|---|---|---|
| GhostLocker | GhostSec, a hacktivist group, has introduced GhostLocker, an advanced Ransomware-as-a-Service (RaaS) framework. GhostSec used Python to develop their encryptor, utilizing PyInstaller to package Python code into standalone executable applications compatible with various operating systems. Recent versions of GhostLocker are compiled using Nuitka, a tool that translates Python programs into C binaries. | Phishing, Affiliate Programs, Darkweb Marketplace | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Modular | | Data Theft and Espionage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| GhostSec | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778, ee227cdOef308287bc536a3955fd8138&16a0228ac42140e9M308ae6343a3f, Oe484560a909fc06b9987db73346eaoca6750d523f2334913c23e061695f5cc | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| BlackCat (aka AlphaV, AlphaVM, ALPHV-ng, Noberus) | The BlackCat ransomware gained attention for its utilization of the Rust programming language and its adoption of a Ransomware-as-a-Service (RaaS) business model. BlackCat is highly customizable, allowing it to be tailored for the creation of targeted executables. | Social engineering expertise, phishing, and SIM swap attacks, | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Data Theft, compromised systems and Espionage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Scattered Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 17fd1b0bda42ee4fd6c0444e22ee566c582efb51d72f7382dc089cfbfb705042, 82efdfd29b22cad8e80ef90940086986410d00ec4c42c547069612c7b0f33eb1, a9c37c4caedf09aebcad23be27b6db636d54e94e0f9b86c1bb61da0784269936 | | |

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 |
|---|---|---|---|
| AveMaria (aka AVE_MARIA, AveMariaRAT, Warzone RAT, WarzoneRAT) | The AveMaria RAT is a remote access trojan written in C++, offered as malware-as-a-service. It possesses a diverse set of capabilities, ranging from stealing victims' files and passwords to capturing desktop activities. The RAT receives regular updates from its command and control (C2) server. | Social engineering expertise, phishing, and SIM swap attacks, | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| RAT | | Data Theft, compromised systems and Espionage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Scattered Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 33b1fec8b20ebd775dbe037a652b5002124a317b434208c400d5cf933b0e68ef, fd770dfea61dde4dde009e95f4a4ea966ff588ee181a8afb1bb730803912dd73, c4f2e2bf5071a42ee6ca811a253e55adf09b1982bacf5f9b90149ff0393950e0 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Raccoon (aka Mohazo, Racealer) | Raccoon is an information-stealing malware available as a Malware-as-a-Service (MaaS). It can be acquired through a subscription, costing $200 per month. The Raccoon malware has already infected over 100,000 devices, making it one of the most discussed viruses on underground forums in 2019. | Social engineering expertise, phishing, and SIM swap attacks, | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Infostealer | | Data Theft, compromised systems and Espionage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Scattered Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 33b1fec8b20ebd775dbe037a652b5002124a317b434208c400d5cf933b0e68ef, fd770dfea61dde4dde009e95f4a4ea966ff588ee181a8afb1bb730803912dd73, c4f2e2bf5071a42ee6ca811a253e55adf09b1982bacf5f9b90149ff0393950e0, | | |
| IPv4 | 193.222.96[.]7, 185.193.125[.]199, 194.87.31[.]58, 5.78.80[.]43, 5.78.81[.]39 | | |

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 |
|---|---|---|---|
| VIDAR | Vidar is a dangerous malware that steals information and cryptocurrency from infected users. It derives its name from the ancient Scandinavian god of Vengeance. This stealer has been terrorizing the internet since 2018 | Social engineering expertise, phishing, and SIM swap attacks, | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Infostealer | | Data Theft, compromised systems and Espionage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Scattered Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 3dae32e22775721f2f9de5fec79dbcd8d62adaeb057b47c4524e02d130a43b25, ffaed8dcf0282df833b74faf419729dc20951ee7edbb58103fa5c582e93d5f3a, 9a58dd63b51866541d91a5bae6260c27aeec7a4135cd67a6fb686f549d3646a6 | | |
| URLs | hxxp://5.75.246[.]163/, hxxp://5.75.246.163/vcruntime140[.]dll, hxxp://5.75.246.163/softokn3[.]dll, hxxp://5.75.246.163/nss3[.]dll | | |

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-2023-36844 |  | Juniper Junos OS: 20.4 - 22.4R2 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:* | - |
| Juniper Junos OS EX Series PHP External Variable Modification Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-473 | T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion | https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36845</td><td>  </td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-473</td><td>T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36846 |  | Juniper Junos OS: 20.4 - 22.4R2 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:* | - |
| Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-306 | T1190: Exploit Public-Facing Application, T1040: Network Sniffing | https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36847</td><td>✗</td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36851</td><td>✗</td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>WORKAROUND</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36033 | ✗ | Windows: 10 - 11 23H2, Windows Server: 2019 - 2022 23H2 | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:* | - |
| Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-119 | T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link | https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36033 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36025 | ✗ | Windows: 10 - 11 23H2, Windows Server: 2008 - 2022 23H2 | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:* | - |
| Microsoft Windows SmartScreen Security Feature Bypass Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-254 | T1190: Exploit Public-Facing Application, T1040: Network Sniffing | https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36036 |  | Windows: 10 - 11 23H2, Windows Server: 2008 - 2022 23H2 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:* | - |
| Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-119 | T1190: Exploit Public-Facing Application, T1040: Network Sniffing | https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36036 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36038 |  | Visual Studio: 2022 version 17.2 – 2022, version 17.7, ASP.NET Core: 8.0 .NET: 8.0.0 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:microsoft:visual_studio:2022:version17.7:*:*:*:*:*:*:* | - |
| ASP.NET Core Denial of Service Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-20 | T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1574: Hijack Execution Flow | https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36038 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-36413 | ✗ | Microsoft Office: 2016 – 2019, Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions, Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems | - |
| | ZERO-DAY | | |
| | ✓ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:* | - |
| Microsoft Office Security Feature Bypass Vulnerability | ✗ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-254 | T1190: Exploit Public-Facing Application, T1040: Network Sniffing | https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36413 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-34060 | ✗ | VMware Cloud Director: 10.5.0 | - |
| | ZERO-DAY | | |
| | ✓ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:vmware:vCloud_Director:10.5.0:*:*:*:*:*:*:* | - |
| VMware Cloud Director Authentication Bypass Vulnerability | ✗ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **WORKAROUND** |
| | CWE-287 | T1190: Exploit Public-Facing Application, T1040: Network Sniffing | https://kb.vmware.com/s/article/95534 |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-37580</td><td>  </td><td rowspan="2">Zimbra Collaboration (ZCS): 8.8.15 - 8.8.15</td><td rowspan="2">Winter Vivern</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:zimbra:zimbra:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-79</td><td>T1189: Drive-by Compromise, T1204: User Execution, T1059.007: JavaScript</td><td>https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41 https://wiki.zimbra.com/wiki/Security_Center</td></tr>
</table>

# Adversaries in Action

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  <br>TA402 (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5) | Palestine | Government, Foreign Affairs | Middle East |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | IronWind, SharpSploit | - |
| **TTPs** | | | |
| TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and: Control; T1059: Command and: Scripting Interpreter; T1072: Software Deployment: Tools; T1083: File and Directory: Discovery; T1082: System Information: Discovery; T1047: Windows Management Instrumentation; T1560: Archive Collected Data; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1543: Create or Modify System Process; T1204: User Execution | | | |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  <br>Winter Vivern (aka UAC-0114, TA473) | Unknown | Government | Greece, Moldova, Tunisia, Vietnam, Pakistan |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | CVE-2023-37580 | - | Zimbra Collaboration (ZCS) |
| **TTPs** | | | |
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1588.005: Exploits; T1566: Phishing; T1059: Command and Scripting Interpreter; T1134: Access Token Manipulation; T1190: Exploit Public-Facing Application | | | |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  <br>GhostSec (aka Ghost Security) | Unknown | Telecommunications Companies, Surveillance Systems, and Internet Of Things (IoT) Devices. | Russia, Israel, Columbia, Iran, South Africa, Nigeria, Pakistan, Iraq, United Arab Emirates, Lebanon, France, Brazil, Sudan, Myanmar, Nicaragua, Philippines, Canada |
| | **MOTIVE** | | |
| | Information theft, espionage and Financial crime | | |
| | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | GhostLocker | - |
| **TTPs** | | | |
| TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1087.001: Local Account; T1659: Content Injection; T1543: Create or Modify System Process; T1560: Archive Collected Data; T1574: Hijack Execution Flow; T1057: Process Discovery; T1211: Exploitation for Defense Evasion; T1071.001: Web Protocols; T1059.006: Python; T1486: Data Encrypted for Impact | | | |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  Scattered Spider (aka Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, and Muddled Libra) | Unknown | Commercial facilities, Telecommunications, Technology, and Business-Process Outsourcing (BPO) | Worldwide |
| | **MOTIVE** | | |
| | Financial gain | | |
| | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, and VIDAR Stealer | - |

| TTPs |
|---|
| TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1585.001: Social Media Accounts; T1585: Establish Accounts; T1566: Phishing; T1660: Phishing; T1566.004: Spearphishing Voice; T1199: Trusted Relationship; T1078.002: Domain Accounts; T1078: Valid Accounts; T1648: Serverless Execution; T1204: User Execution; T1136: Create Account; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1484.002: Domain Trust Modification; T1484: Domain Policy Modification; T1578.002: Create Cloud Instance; T1578: Modify Cloud Compute Infrastructure; T1656: Impersonation; T1606: Forge Web Credentials; T1621: Multi-Factor Authentication Request Generation; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552: Unsecured Credentials; T1217: Browser Bookmark Discovery; T1538: Cloud Service Dashboard; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1539: Steal Web Session Cookie; T1021: Remote Services; T1021.007: Cloud Services; T1213.003: Code Repositories; T1213.002: Sharepoint; T1213: Data from Information Repositories; T1074: Data Staged; T1114:Email Collection; T1530: Data from Cloud Storage; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1567.002: Exfiltration to Cloud Storage |

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **twelve exploited vulnerabilities** and block the indicators related to the threat actors **TA402, Winter Vivern, GhostSec, Scattered Spider,** and malware **Ducktail, IronWind, SharpSploit, NoEscape, GhostLocker, BlackCat, AveMaria, Raccoon, VIDAR**.

**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 **twelve exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TA402, Winter Vivern, GhostSec, Scattered Spider,** and malware **Ducktail, IronWind, SharpSploit, NoEscape, GhostLocker, BlackCat, AveMaria, Raccoon, VIDAR** in Breach and Attack Simulation(BAS).

# Threat Advisories

Multiple Critical Vulnerabilities in Juniper Exploited in the Wild

Hackers Employ Updated Ducktail to Target Indian Marketers

Microsoft’s November 2023 Patch Tuesday Addresses Five Zero-day Vulnerabilities

TA402's Covert Operation Takes Aim at the Middle East

VMware Unveils Critical Authentication Bypass Vulnerability in VCD Appliance

In-Depth Analysis of NoEscape Ransomware

Four Threat Actors Capitalized on Zimbra Zero Day to Infiltrate Government Organizations

GhostSec Pioneering the Hacktivist Front with GhostLocker

Scattered Spider Cyber Threat Key Findings and Security Measures

# 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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

## Indicators of Compromise (IOCs)

| Attack Name | TYPE | VALUE |
|---|---|---|
| Ducktail | SHA256 | 8eafccab8c6a80356c84c9ae3bd3603262069748be59a8d5aee4dfa3cf4a00a3, 9cf88cfd198e0070bb24868ce56f260f55a4b227e266ebcb37fdb83183299ae5, c2e8bc6389ba6ba32a350312f4fdda33628c806587ade0836f3886e2ffcaf9b2, 3097d80d4aa3abf2599058bf58d85aa8cec6ca6894c13c6d360dce162a5dd626, 1663d092935809dd5f3f0049463f4367ded67f2253b039d9b0c05510b2e4c94e |
| IronWind | SHA256 | 9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47, 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115, e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c |
| SharpSploit | SHA256 | 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47, ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f, 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368, 81fc4a5b1d22efba961baa695aa53201397505e2a6024743ed58da7bf0b4a97f, 3b2a6c7a39f49e790286185f2d078e17844df1349b713f278ecef1defb4d6b04, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| SharpSploit | SHA256 | 7bddde9708118f709b063da526640a4132718d3d638505aafce5a20d404b2761 |
| NoEscape | SHA256 | 0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a,<br>2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5,<br>4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e,<br>4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e,<br>5300d7456183c470a40267da9cd1771d6147445b203d8eb02437348bf3169e0d,<br>53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128,<br>62205bf0a23e56524f2f1c44897f809457ad26bc70810008ec5486e17c7e64e2,<br>68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0,<br>68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8,<br>73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e,<br>831a2409d45d0c7f15b7f31eddbbdfe7d58414499e81b3da7d9fdee28fafe646,<br>8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31,<br>91c515d55fae6d21b106c8c55067ce53d42bef256bd5a385cadd104cf68f64ff,<br>9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c,<br>10d2b5f7d8966d5baeb06971dd154dc378496f4e5faf6d33e4861cd7a26c91d7,<br>21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da,<br>46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561,<br>c34c5dd4a58048d7fd164e500c014d16befa956c0bce7cae559081d57f63a243 |
| | SHA1 | ea1f7940271fc80d06b2f222506020b650ad41bc,<br>30f71a24c15dd81965b12996a79d914acf4f169e,<br>12dc0a2de3ad30201107bfcb679de5acacf31e5c,<br>30c60f18279ed5fd36e3ac2d3ba5ddbdc5d1f624,<br>9cbc7417fa5ce2f6d87026337fc7892e4f485819,<br>d38c613020cb4616783c8535380e28404f7eaebf,<br>b17403e7dcb992ba8d2b56dd843406264d3910e5,<br>317f296131b37a73c9a5d253015821dfdc8b1190 |
| | MD5 | 204f028c983f654be32b97e849edeaab,<br>47ae17d89c2d9b6acdc7458f5df1c6f7,<br>5779cec690b5bbc61687381ae8a8d518, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| NoEscape | MD5 | 58b4a4eed74fbfbf104d0ffd92207018, a106c1236357c315722ddbd985c5613c, c850f6816459e3364b2a54239642101b |
| GhostLocker | SHA256 | 7e14d88f60fe80f8fa27076566fd77e51c7d04674973a564202b4a7cbfaf2778, ee227cdOef308287bc536a3955fd8138&16a0228ac42140e9M308ae6343a3f, Oe484560a909fc06b9987db73346eaoca6750d523f2334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653oee898a7a338424bd3e9b15d792972, 663ac2d887df18e6da97dd358ebd2bca55404fd4a1C8ClC51215834fc6d11b33, 9b6be74c2c144f8bcb92c8350855d35C14bb7f2b727551C3dd5C8054c4136e3f, ee227cdOef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 0e484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, abac31b5527803a89c941cf24280a9653cdee898a7a338424bd3e9b15d792972, 663ac2d887df18e6da97dd358ebd2bca55404fd4a1c8c1c51215834fc6d11b33, Oe484560a909fc06b9987db73346efaOca6750d5232334913c23e061695f5cc, 15d874e24caf162bc58597ac5f22716694b5d43cf433bee6a78a0314280f2c80, 0e484560a909fc06b9987db73346efa0ca6750d523f2334913c23e061695f5cc, 4844f44c9de364377f574e4d6a8a77dc0b4d6a67f21ccbf693ac366e52eaa8cb, 65d3a922754af96d8d722859ac31f3de96522d50659c67607021f2ac728f9630, a98f8468d70426ba255469a92d983d653f937d954e936e0ff5d9a0f44f1bdf70, ee227cd0ef308287bc536a3955fd81388a16a0228ac42140e9cf308ae6343a3f, 7d37eddf0b101ff2b633b2ffe33580bdb993a97fecc06874d7b5b07119b9ec99, 4c09a012efff318b01a72199051815c5a7b920634fb6c76082673681f54f2ec3 |
| BlackCat | SHA256 | 17fd1b0bda42ee4fd6c0444e22ee566c582efb51d72f7382dc089cfbfb705042, 82efdfd29b22cad8e80ef90940086986410d00ec4c42c547069612c7b0f33eb1, a9c37c4caedf09aebcad23be27b6db636d54e94e0f9b86c1bb61da0784269936, 1124a6eea74d6e128ac275ce462f2807cd900d49c87382db81f901e60c8e7758, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| BlackCat | SHA256 | 76f99fbf8f91556c98848cabfb3fd85892939e410903e03da67e517102745102, 76f99fbf8f91556c98848cabfb3fd85892939e410903e03da67e517102745102 |
| AveMaria | SHA256 | 33b1fec8b20ebd775dbe037a652b5002124a317b434208c400d5cf933b0e68ef, fd770dfea61dde4dde009e95f4a4ea966ff588ee181a8afb1bb730803912dd73, c4f2e2bf5071a42ee6ca811a253e55adf09b1982bacf5f9b90149ff0393950e0, 62de5582c8c8dad5e6ae1e6008e3883c72b59de0b17cec54be78a888d4097dc2, 40052b060229a0b036bdf73aa09ea1ecc6e73555f448dc092340ccb342ec1669, c925c6fb78be7a4b617be38e6cf80e94cf30198a48689c94d78d42cef12f8223, 568e609adc8d405cb059b471c7f99a2dbc2969642721cc4ce51e869a6af35dca, f0b92472c6a95a379f7235c22460fdb3602d625a662141e7baecc48c049ad715, a230a63b3011b2ebe1fb667cb661835fe34fb93bb6a1cbd4f132996b437e947c, 7bcdc2e607abc65ef93afd009c3048970d9e8d1c2a18fc571562396b13ebb301, 4fd7411cc681154e27eede4332a010641db743700099c602f5ac1e61968c3264, e6df4f343401f5c3c79228940acc0dcadcd655e1e0e8010f9f67eb946d67e94a, 3c4d55297278d1e2d4393d4b65f6ed5a4d88ebf590677521e95f084bab83b6bb, 2a11c5bca51d510efec348abaa05617f21e5b4ab08b67e6261d9830b4729e649 |
| Raccoon | SHA256 | 184e98107496e5859dd0f09c42deffffaf0cc9362cc192f0e89bf2c4b20d82fd, fd3f9ee2a7b4e35be97140818562dc4470f90705cbd959e87c07ed983692e33d, abcbbdb2a2eb219a82c3f446f74ac6ef93a3deb11e4c277dee8c106792d7b783, 5ff52ab9349cd6d7a7fc0d2596c3423cdfb5df668b363fb93bd686f9ab198910, 1e5c7dcfbe4a1e9da06229b4512229c463b0268832b9cb6cdb35a1153963be37, 43f48b33734f2b7ab20e3798845f8411723f643a15c9833b86942ab6beb9d4fe, 5566d651067c35b90b47039ec1384432ec89fcdc946188274fb5127a8874b194, 35efa67d11c826f739cedc44c759bf9f12b12deab0af24bd8a402eccb7157d97, 334f1cfbe30bc002491e179ac48e228e142e78f13a2fa5eaeb44bcf4cf2bf946, |

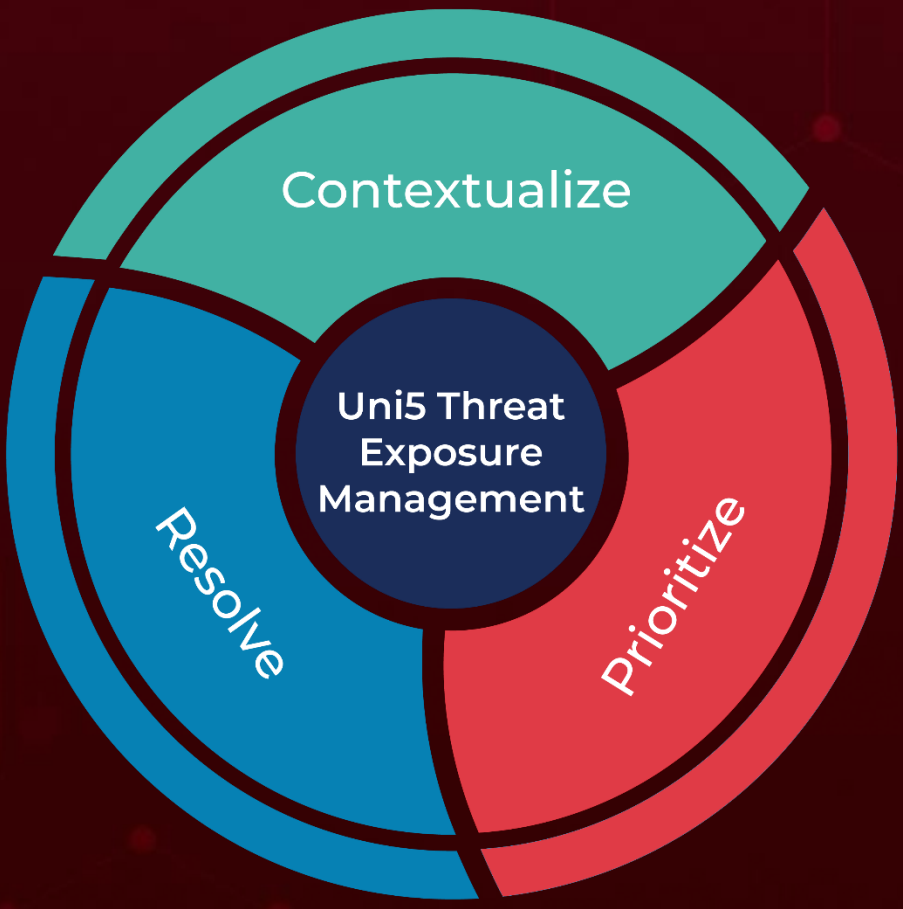
| Attack Name | TYPE | VALUE |
|---|---|---|
| Raccoon | SHA256 | 61431a0d94e6995e43fa174b18ca64052374c5d2ff1743631e13154ca1cf0fab, 89b8c862587864fe60e46ee4f4e8cbba2d8c32081a04ad5df072c6f99f06f4e2, 529c26f60ac5ebc31836486d9fa29f3b139437f06b160ca7f2887d13126c937e, 0ea39ba88fb2afb12f328a24d8b0441c6c6d2220c8ceac1a1c0640c7d6b43ae4, 8352d5041c2baf4613361108ef86b62ce3814bfa543a52662d40ddfc5dbf045a, 1e5b1cee1779ab2659fbaf465da3dfda327fdc83e78b73c4cebc241356ff00d9, 302886dba2ea9783a67247110cfabea3f94d1f78343b55f66edd58fc4be926f1, eeb5ee631e4e3dea3a6faf8fc70bf52d1814db8f5c6a6ebe729ae23df71879e5, 5320425988b0670455042dbd99d0c30b96ddf4710932dbe61b95711b185536b6, 0c1226d05d81a2f2f9ed910fff598bd00a0cb7ae43b3793735d45de1f35b838f, 31b6fba02c5c0d97a7ae7436a7e30793fe86f36ddf289e8eb53702dcd0ef06b9 |
| | IPv4 | 193.222.96[.]7, 185.193.125[.]199, 194.87.31[.]58, 5.78.80[.]43, 5.78.81[.]39, 94.142.138[.]147, 157.90.161[.]111, 89.23.107[.]183 |
| | URLs | hxxp://51.195.166.184/, hxxp://31.192.237.23:80/, hxxp://45.61.138.198:80/, hxxp://91.92.246.197:80/, hxxp://91.103.252.11 |
| VIDAR | SHA256 | 3dae32e22775721f2f9de5fec79dbcd8d62adaeb057b47c4524e02d130a43b25, ffaed8dcf0282df833b74faf419729dc20951ee7edbb58103fa5c582e93d5f3a, 9a58dd63b51866541d91a5bae6260c27aeec7a4135cd67a6fb686f549d3646a6, 13e384c54054a094b8045928c8ec9d3697372e551e4887b4ea9e18e319f0f40b, 48b7d39b9c19b0e6131928830add88e9c43e01e8218db17877abca9a65d14a5d, 1eda38c94d7896c350c73e5ac87cf2cd65e96ba7d03cddc7f1302c5d1b65ca88, c1f234ee29062e05c71fbb29d43b75e4a73aeccc95201dea7956fc6e6a5949cf, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| VIDAR | SHA256 | 726855dc870ed0224d91891b898e542393149b0eaef7817aa332b71c13b22ae0, 6ecf9fda65dc1a4a9c7610510ac9f78a6663e75d736a8444c72e11a0cc8d8d46, fc5336b039a9cc8e14d515f338c90a5a404249adab200032324c65f055904255, 0e9783330259b925379f44dfdc9e8f86b545ad43e8b747a8214a7d7e7617940e |
| | URLs | hxxp://5.75.246[.]163/, hxxp://5.75.246.163/vcruntime140[.]dll, hxxp://5.75.246.163/softokn3[.]dll, hxxp://5.75.246.163/nss3[.]dll, hxxp://5.75.246.163/msvcp140[.]dll, hxxp://5.75.246.163/mozglue[.]dll, hxxp://5.75.246.163/freebl3[.]dll, hxxp://5.75.246.163/sqlite3[.]dll, hxxp://168.119.173.77[:]2087/, hxxp://168.119.173.77:2087/vcruntime140[.]dll, hxxp://168.119.173.77:2087/softokn3[.]dll |

# 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

**November 20, 2023 . 4:00 AM**



More at www.hivepro.com