Date of Publication
December 4, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

# THREAT DIGEST

## Attacks, Vulnerabilities and Actors

27 NOVEMBER to 3 DECEMBER 2023

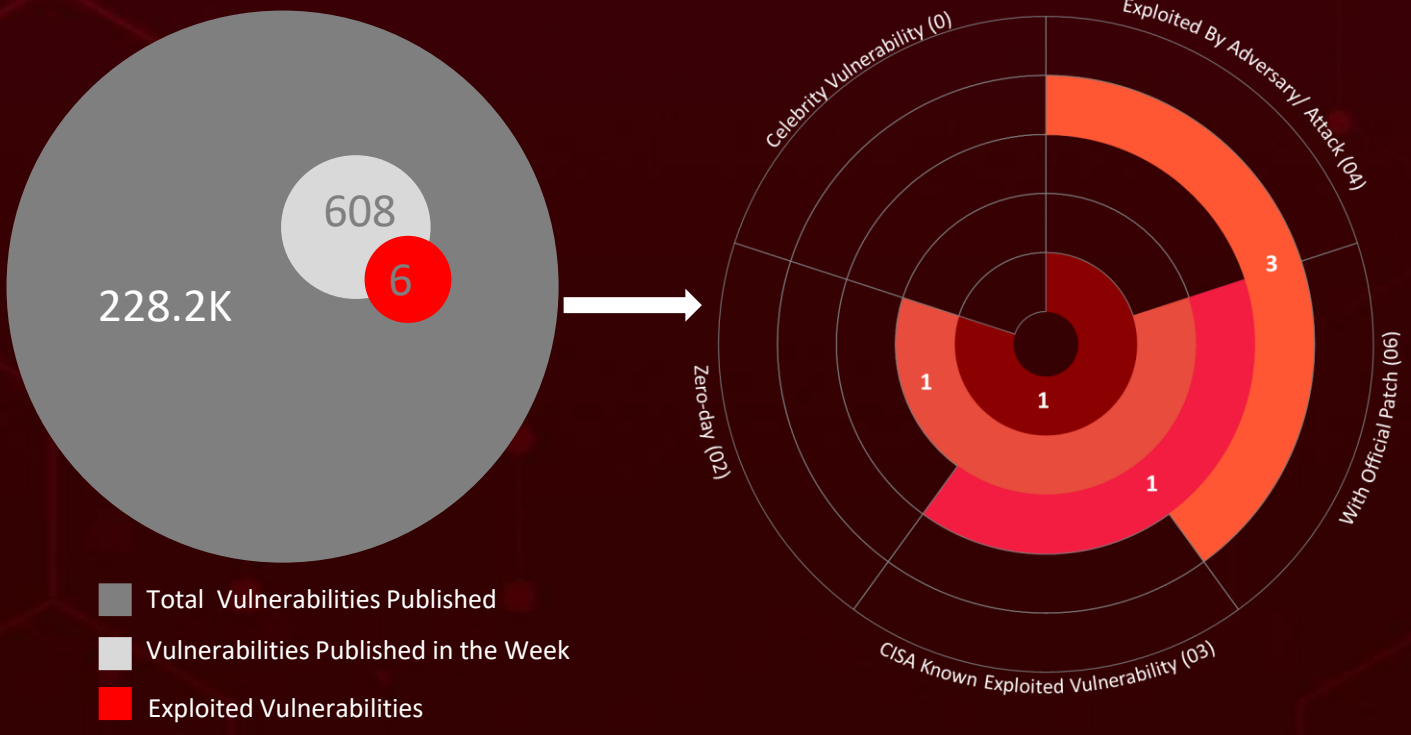
# Table Of Contents

# Summary

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

Furthermore, HiveForce Labs revealed that among the **two zero-day** vulnerabilities, one in WinRAR was exploited by **DarkCasino**, an APT group with economic motivations. Additionally, a vulnerability was identified in **Google**, marking the sixth zero-day flaw exploited by attackers widely. Hackers are actively exploiting a critical vulnerability in **ownCloud**.

The **Cactus ransomware** is actively exploiting critical **Qlik Sense vulnerabilities** with the ultimate goal of establishing persistence and enabling remote control, infiltrating corporate networks stealthily. These attacks are on the rise, posing a significant threat to users worldwide.



# High Level Statistics

**8**
Attacks Executed

**6**
Vulnerabilities Exploited

**2**
Adversaries in Action

- RustBucket
- SwiftLoader
- ObjCShellz
- KandyKorn
- ParaSiteSnatcher
- Djvu
- PrivateLoader
- Cactus

- CVE-2023-38831
- CVE-2023-6345
- CVE-2023-49103
- CVE-2023-41266
- CVE-2023-41265
- CVE-2023-48365

- DarkCasino
- Lazarus Group

# Insights

**Code Red for Chrome:** Act Now to Patch **Zero-Day** Vulnerability Threatening Remote Execution

**Economic Espionage:** **DarkCasino**'s utilization of the **WinRAR Zero-day**, with a specific focus on online trading platforms, underscores its intent to compromise financial systems.

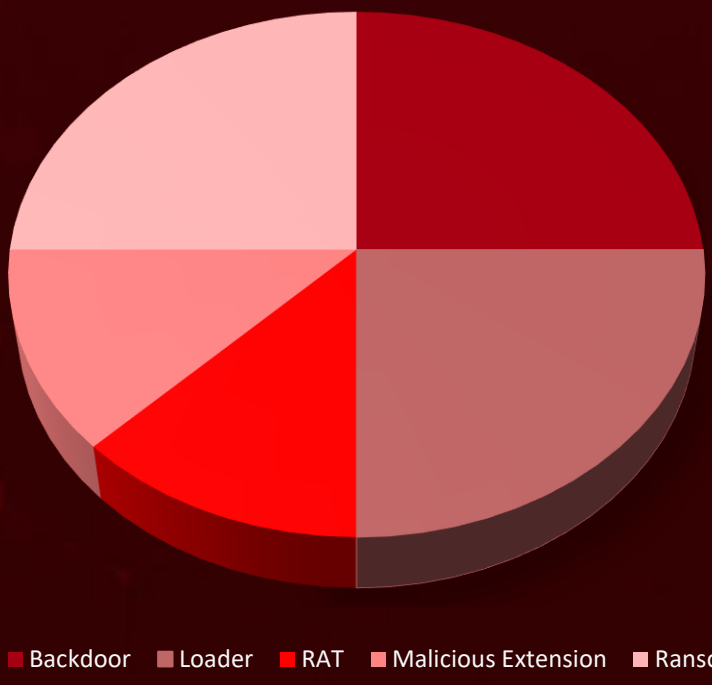
**Guard Your Mac!** North Korean Threat Actors Unleash **RustBucket** and **KandyKorn** in Cryptocurrency Heist

**Patched or Preyed Upon:** **Cactus Ransomware**'s Hunt for Unpatched **Qlik Sense** Systems

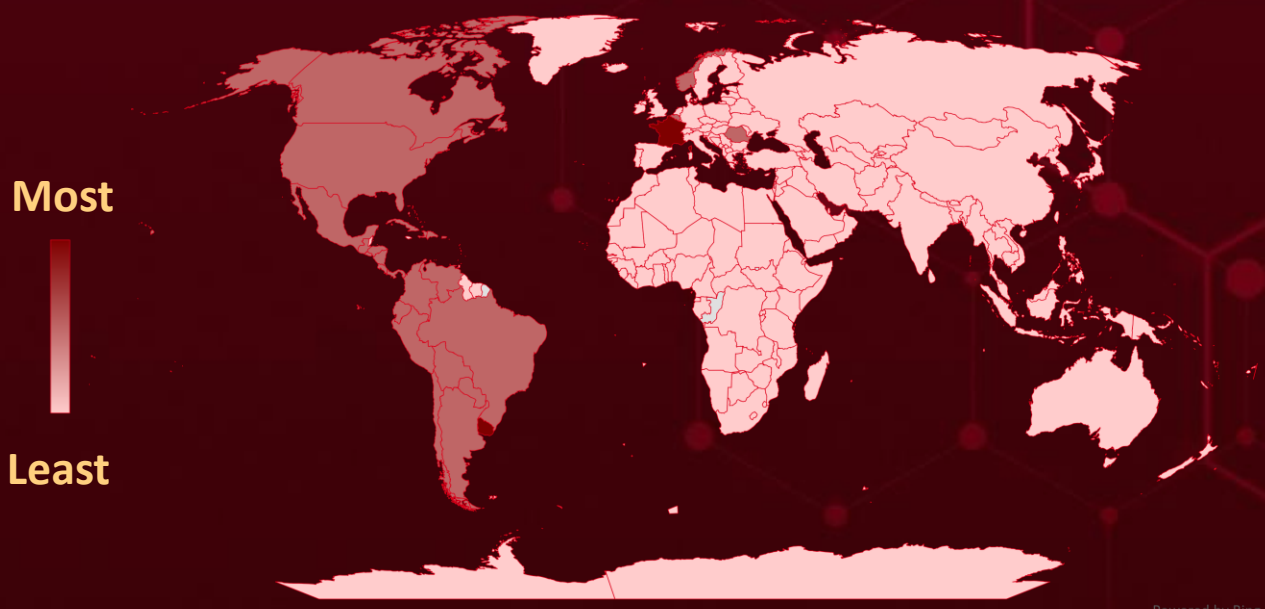
**Cracked and Trapped:** The Deceptive **DJVU** Variant Disguised as Cracked Software Holds Systems Hostage for **$980**

**Breaking Chains:** The **Lazarus** Group's Sneak Attack Through **MagicLine4NX** Vulnerability

## Threat Distribution

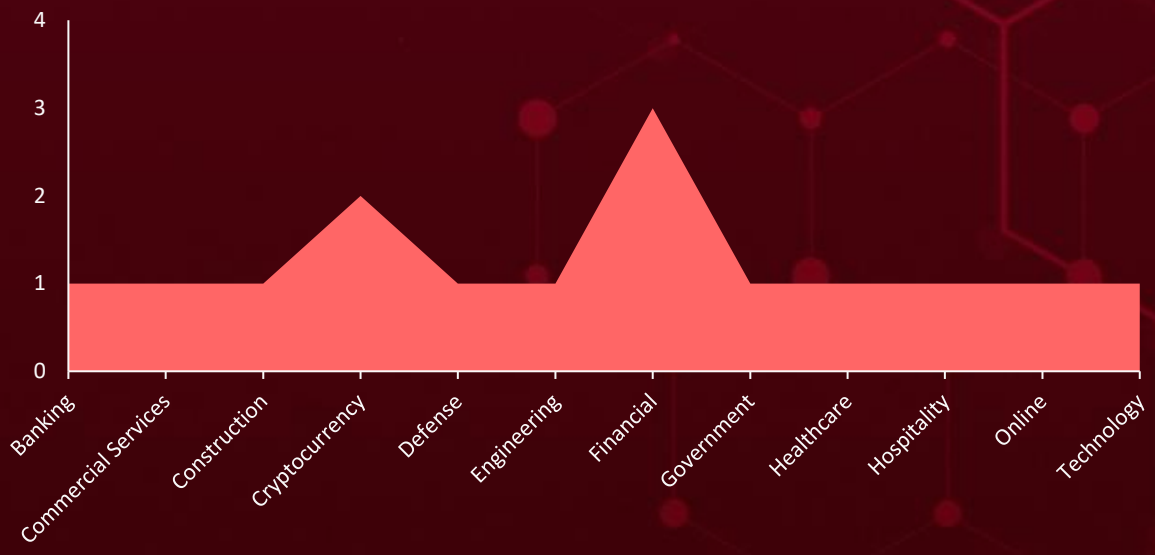


# Targeted Countries




| Countries | Countries | Countries |
|---|---|---|
| France | Mongolia | Cyprus |
| Uruguay | Poland | Philippines |
| Mexico | Bermuda | Denmark |
| Belgium | United Kingdom | Saudi Arabia |
| Paraguay | Bhutan | DR Congo |
| Bolivia | Thailand | Sierra Leone |
| Haiti | Nepal | Earth |
| Brazil | Turkmenistan | Slovakia |
| Norway | Bulgaria | East Timor |
| Canada | Australia | Somaliland |
| Puerto Rico | Austria | Easter Island |
| Chile | Cambodia | South Ossetia |
| Guatemala | Bahrain | Antigua and Barbuda |
| Colombia | Algeria | |
| Honduras | Belarus | Sri Lanka |
| Costa Rica | Serbia | Egypt |
| Nicaragua | Central African Republic | Sweden |
| Cuba | | Afghanistan |
| Panama | Spain | Tajikistan |
| Dominican Republic | Syria | Equatorial Guinea |
| Peru | China | Tokelau |
| Ecuador | Maldives | Eritrea |
| Romania | Andorra | Tunisia |
| United States | Angola | Ukraine |
| Argentina | Nigeria | Ethiopia |
| El Salvador | Croatia | Malaysia |
| Venezuela | Oman | Finland |

# Targeted Industries




# TOP MITRE ATT&CK TTPs

| | | | | |
|---|---|---|---|---|
| **T1059** Command and Scripting Interpreter | **T1588.006** Vulnerabilities | **T1083** File and Directory Discovery | **T1018** Remote System Discovery | **T1055** Process Injection |
| **T1659** Content Injection | **T1566** Phishing | **T1588** Obtain Capabilities | **T1071** Application Layer Protocol | **T1082** System Information Discovery |
| **T1059.001** PowerShell | **T1204.002** Malicious File | **T1203** Exploitation for Client Execution | **T1053** Scheduled Task/Job | **T1490** Inhibit System Recovery |
| **T1071.001** Web Protocols | **T1070.001** Clear Windows Event Logs | **T1053.005** Scheduled Task | **T1204** User Execution | **T1027** Obfuscated Files or Information |

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| RustBucket | RustBucket is a new malware family that targets macOS systems. RustBucket is a multi-stage malware that uses a variety of techniques to infect its victims, including phishing emails, malicious websites, and drive-by downloads. | Unknown | - |
| | | **IMPACT** | **AFFECTED PRODUCTS** |
| **TYPE** | | Steal sensitive information and install other malware | macOS |
| Backdoor | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 812c795908f38bdb5cc20487569e53e04dfda8ad87ebe7156f3fb2fed1ab0b9b, 9fb57fca174506e96e2eda8db31a193b7476ce076557ff10617cdcae4d5716aa, a43c3097adb0d82eceb867957b54cc29e863d983daa547102361c59c0ac2a804, 070b2723a925d0788ddc3e5e4a214b7c64c61d44e5d01ca5bbe589f45256aa56, aa109f4fe27ed1f69e78a5aeba5356618ba24d8188077f0361c25a2e0d88874c | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| SwiftLoader | SwiftLoader is a backdoored PDF reader app, it secretly retrieves and executes secondary malware. | Unknown | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Loader | | steal cryptocurrency | macOS |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1 | | |

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 |
|---|---|---|---|
| ObjCShellz | The malware, written in Objective-C, operates as a remote shell, enabling attackers to execute commands on compromised systems. It communicates with its C2 server using a POST request, providing information about the victim's macOS version. | Unknown | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Backdoor | | Executes custom commands | macOS |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | ca6d8b8a84e40adb8949f37eef65315d1d25283583c0a65921414611e615b27d, cde067b700e5f39e276a104497bc3ae0a5677977376a1b4c87de3d03730000bf, 462f4ccc290b3cc87cdce2a82aa3f0cb48140a88b590ee175ef9c24180b545c7, fe31f8cba8fc3832da136778aa28c406bf8ef04b448cba076ff7f5f3b8be7683, 1219c2c14afd2db469b0ae479236ab45abd20f6092592b539e04ba7aceec25e2 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| KandyKorn | KandyKorn primarily targets macOS and is a Remote Access Trojan written in C++. | - | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| RAT | | steal cryptocurrency | macOS |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA1 | 62267b88fa6393bc1f1eeb778e4da6b564b7011e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, ac336c5082c2606ab8c3fb023949dfc0db2064d5, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3 | | |

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 |
|---|---|---|---|
| ParaSiteSnatcher | ParaSiteSnatcher is a malicious browser extension with ability to intercept HTTP requests enabling Threat Actors to manipulate and exfiltrate HTTP data. | Through a VBScript downloader | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Malicious Extension | | Extract highly sensitive information | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4, e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807, 96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f, b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250, 6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| PrivateLoader | PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server. | Phishing, exploit kits, malvertising, trojanized executables | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Loader | | Download and execute payloads | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| MD5 | 6cc7d9664c1a89c58549e57b5959bb38 | | |
| SHA1 | 85b665c501b9ab38710050e9a5c1b6d2e96acccc | | |
| SHA256 | 27c1ed01c767f504642801a7e7a7de8d87dbc87dee88fbc5f6adb99f069afde4 | | |

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 |
|---|---|---|---|
| Djvu | Djvu is a ransomware family initially identified in 2018 and linked to the STOP ransomware, utilizes various file extensions for naming encrypted files. | Disguise of cracked software | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Data exfiltration and information theft | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 61cbdd06eb0034a51074b1bcaeed4d2d7aff85f7e1fe61903481b1fb63508db4, ce00b1cb3ac152e4c3d6688e595146c2382616cb83139bac6ee798f0e2e99c19, 864f2a472db2e654cd2f2925be768a442d167c6d15c2a678ec81f713ff897b1d, c18b111c047ba4e0aa30ca19634ffd9f131aecb5dec7645c78a666e85e469b03, d0644b5e3e7dcad31d5918e4688e31d6fc691ce2e709e6033263774baf37c50e | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Cactus | CACTUS ransomware targets large commercial entities, gains initial access to networks through Qlik Sense vulnerabilities, exfiltrates sensitive data, and communicates with victims through Tox. It employs a variety of tools and tactics to distribute the ransomware binary and maintain persistence within the environment, while also attempting to obtain credentials and escalate privileges through lateral movement. | Exploiting critical Qlik Sense vulnerabilities, | CVE-2023-41266 CVE-2023-41265 CVE-2023-48365 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Data Theft, Compromised systems, and Espionage | Qlik Sense Enterprise for Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8, 09e7e3f23bac60ce7a4024ed7972981865f030c3edba9cda760d055f0a46e448, 0a8088e2ba539541f476836c6f4e5812c4ae5c52133801faa1bc3806a4ade683, 1ea49714b2ff515922e3b606da7a9f01732b207a877bcdd1908f733eb3c98af3 | | |

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-2023-38831 |  | WinRAR version 6.22 and older versions | DarkCasino |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:* | - |
| RARLAB WinRAR Code Execution Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH DETAILS |
| | CWE-20 | T1059: Command and Scripting Interpreter | Update WinRAR version to 6.23 or later versions https://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-6345 | ✗ | Google Chrome 100.0.4896.60 – 119.0.6045.160 | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* | - |
| Google Chrome Skia Integer Overflow Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-190 | T1059: Command and Scripting Interpreter | https://www.google.com/intl/en/chrome/?standalone=1 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-49103 | ✗ | ownCloud graphapi 0.2.0 – 0.3.0 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:owncloud:graphapi:*:*:*:*:*:*:*:* | - |
| ownCloud graphapi app Information Disclosure Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-200 | T1598: Phishing for Information | https://marketplace.owncloud.com/apps/graphapi , https://marketplace.owncloud.com/apps/oauth2 , https://owncloud.com/download-server |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-41266 | ✗ | Qlik Sense Enterprise for Windows | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:* | Cactus ransomware |
| Qlik Sense Enterprise path traversal vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-20 | T1202: Indirect Command Execution, T1059: Command and Scripting Interpreter, | https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCTS | ASSOCIATED ACTOR |
|---|---|---|---|
| CVE-2023-41265 | ✗ | Qlik Sense Enterprise for Windows | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:* | Cactus ransomware |
| Qlik Sense Enterprise Privilege escalation vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-444 | T1068: Exploitation for Privilege Escalation | https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-48365</td><td>  </td><td rowspan="2">Qlik Sense Enterprise for Windows</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*</td><td rowspan="2">Cactus ransomware</td></tr>
<tr><td rowspan="3">Qlik Sense Enterprise remote code execution vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-444</td><td>T1059: Command and Scripting Interpreter</td><td>https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads</td></tr>
</table>

# Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4">  <br><br>DarkCasino</td><td>Unknown</td><td rowspan="3">Cryptocurrency trading platforms, online casinos and network banks worldwide</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Economic benefits</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2023-38831</td><td>-</td><td>RARLAB WinRAR</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0011:Command and Control; T1027: Obfuscated Files or Information; T1055: Process Injection; T1566: Phishing; T1140: Deobfuscate/Decode Files or Information; T1056: Input Capture; T1059: Command and Scripting Interpreter; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1105: Ingress Tool Transfer; T1204: User Execution; T1204.002: Malicious File; T1203: Exploitation for Client Execution</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3">  <br><br>Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</td><td>North Korea<br>MOTIVE<br>Information theft and espionage, Sabotage and destruction, Financial crime</td><td>Government Organizations, Financial Institutions and Defense</td><td>Worldwide</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>-</td><td>MagicLine4NX</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1129: Shared Modules; T1027: Obfuscated Files or Information; T1036: Masquerading; T1563: Remote Service: Session Hijacking; T1112: Modify Registry; T1056: Input Capture; T1012: Query Registry; T1018: Remote System Discovery; T1082: System Information Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1588.006: Vulnerabilities; T1573: Encrypted Channel; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actors **DarkCasino, Lazarus Group,** and malware **RustBucket, SwiftLoader, ObjCShellz, KandyKorn, ParaSiteSnatcher, Djvu, PrivateLoader, Cactus**.

**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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **DarkCasino, Lazarus Group,** and malware **RustBucket, SwiftLoader, ObjCShellz, KandyKorn, ParaSiteSnatcher, Djvu, PrivateLoader, Cactus** in Breach and Attack Simulation(BAS).

# Threat Advisories

The Rise of DarkCasino APT Group Exploiting WinRAR 0-Day

North Korean APT's Covert Supply-Chain Ambush

North Korean Hackers Target Crypto Users with RustBucket and KandyKorn

Google Addresses Sixth Zero-Day Flaw Exploited by Attackers Wildly

ParaSiteSnatcher A Silent Threat to Latin America

ownCloud Critical Vulnerability is under active exploitation

DJVU Ransomware's Variant Emerges Disguised as Cracked Software

Cactus Ransomware Exploits Vulnerabilities in Qlik Sense

# 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 malicious 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 |
|---|---|---|
| RustBucket | SHA256 | 812c795908f38bdb5cc20487569e53e04dfda8ad87ebe7156f3fb2fed1ab0b9b, 9fb57fca174506e96e2eda8db31a193b7476ce076557ff10617cdcae4d5716aa, a43c3097adb0d82eceb867957b54cc29e863d983daa547102361c59c0ac2a804, 070b2723a925d0788ddc3e5e4a214b7c64c61d44e5d01ca5bbe589f45256aa56, aa109f4fe27ed1f69e78a5aeba5356618ba24d8188077f0361c25a2e0d88874c |
| SwiftLoader | SHA256 | 47b8b4d55d75505d617e53afcb6c32dd817024be209116f98cbbc3d88e57b4d1 |
| ObjCShellz | SHA256 | ca6d8b8a84e40adb8949f37eef65315d1d25283583c0a65921414611e615b27d, cde067b700e5f39e276a104497bc3ae0a5677977376a1b4c87de3d03730000bf, 462f4ccc290b3cc87cdce2a82aa3f0cb48140a88b590ee175ef9c24180b545c7, fe31f8cba8fc3832da136778aa28c406bf8ef04b448cba076ff7f5f3b8be7683, 1219c2c14afd2db469b0ae479236ab45abd20f6092592b539e04ba7aceec25e2 |
| KandyKorn | SHA1 | 62267b88fa6393bc1f1eeb778e4da6b564b7011e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, ac336c5082c2606ab8c3fb023949dfc0db2064d5, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| KandyKorn | SHA1 | 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3, 8d5d214c490eae8f61325839fcc17277e514301e, 9f97edbc1454ef66d6095f979502d17067215a9d, c45f514a252632cb3851fe45bed34b175370d594, ce3705baf097cd95f8f696f330372dd00996d29a, e244ff1d8e66558a443610200476f98f653b8519, e77270ac0ea05496dd5a2fbccba3e24eb9b863d9, e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3, 62267b88fa6393bc1f1eeb778e4da6b564b7011e, 8d5d214c490eae8f61325839fcc17277e514301e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, 9f97edbc1454ef66d6095f979502d17067215a9d, ac336c5082c2606ab8c3fb023949dfc0db2064d5, c45f514a252632cb3851fe45bed34b175370d594, ce3705baf097cd95f8f696f330372dd00996d29a, e244ff1d8e66558a443610200476f98f653b8519, e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f, e77270ac0ea05496dd5a2fbccba3e24eb9b863d9 |
| ParaSiteSnatcher | SHA256 | 0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4, e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807, 96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f, b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250, 6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4, 9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba, 1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa, 8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc, 8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6, bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7, ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2, 1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b, 3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b, 71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8, 21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240, |

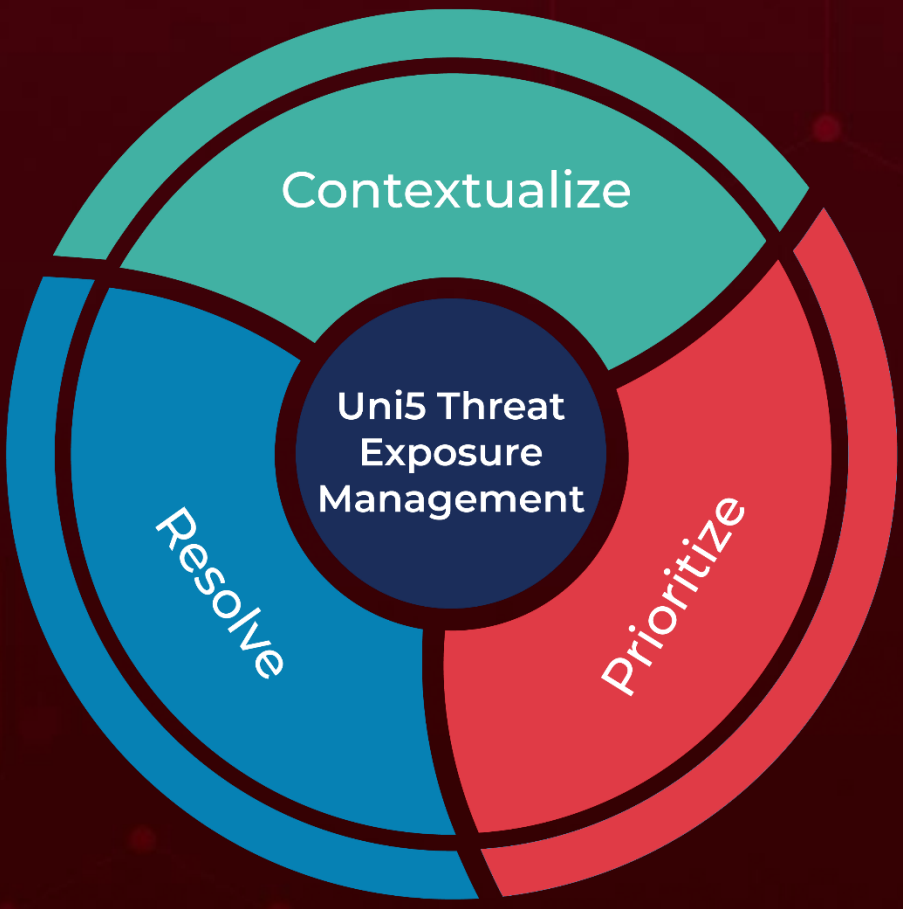
| Attack Name | TYPE | VALUE |
|---|---|---|
| ParaSiteSnatcher | SHA256 | c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f,<br>5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6,<br>049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c,<br>b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4,<br>e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123,<br>a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0,<br>260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627,<br>e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3,<br>77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315,<br>72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df |
| Djvu | SHA256 | 61cbdd06eb0034a51074b1bcaeed4d2d7aff85f7e1fe61903481b1fb63508db4,<br>ce00b1cb3ac152e4c3d6688e595146c2382616cb83139bac6ee798f0e2e99c19,<br>864f2a472db2e654cd2f2925be768a442d167c6d15c2a678ec81f713ff897b1d,<br>c18b111c047ba4e0aa30ca19634ffd9f131aecb5dec7645c78a666e85e469b03,<br>d0644b5e3e7dcad31d5918e4688e31d6fc691ce2e709e6033263774baf37c50e,<br>f6f2310f44da2c4c97832cff60fb3f60719491f5971cf7fe22062d4ada705e32,<br>0c8969456b94f05ca3ee3f6b0518bd151fe0547150086980282f4ad1fc8a7bd6,<br>84161c7097bc5a675ed250ed222f1f4d0aea4c2dc48d623aecd9f7fc44a7119c,<br>23c672f232c10ed80e8a361da94c54d07ecb2673d21bf663f75ab5dba43b2ae0,<br>91c21cadd1249480ace996ae3d3e1a0370976d9c4bd17bdade97b1bb92fc59e0,<br>895593614cf395846b5cdd2c8c4bc7adb87de14cc849e28632f1ab6ff49b43fb,<br>72a9bb670dc192dae57c0238afdb706bea501f8e0bf06b4fa4b8669741c93547,<br>40fff8c4d316ae5de858fdd429d684a96426ce701582d133718be7bea7ea5ac5,<br>f9b5765e9f494c0c485774a401904ed83092fbd6e19184a4ff48c74f6aed02e6 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| PrivateLoader | MD5 | 6cc7d9664c1a89c58549e57b5959bb38 |
| | SHA1 | 85b665c501b9ab38710050e9a5c1b6d2e96acccc |
| | SHA256 | 27c1ed01c767f504642801a7e7a7de8d87dbc87dee88fbc5f6adb99f069afde4 |
| Cactus | SHA256 | 0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8,<br>09e7e3f23bac60ce7a4024ed7972981865f030c3edba9cda760d055f0a46e448,<br>0a8088e2ba539541f476836c6f4e5812c4ae5c52133801faa1bc3806a4ade683,<br>1ea49714b2ff515922e3b606da7a9f01732b207a877bcdd1908f733eb3c98af3,<br>21d7ad955dbc5732be90f3d6dbb4e161ef9cf511a7989e72c4ea1c5e44744167,<br>4b0a5d6a176317437978211a423a7c1cdf832baa7984bba09aeeb5a1e4d07aa3,<br>509a533ade43406eb50fa9cb8984b2e10d008ad0ea8c22d0652f3ee101125bb7,<br>6642d79f4d1044b756e2c3221ace37a71b4a671e18847f2940e2ea349dc6cb67,<br>69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc,<br>70a580e734c2331098fa3ecf3f1c928e17ddb92f99f75956c3f805b065222685,<br>729f0ff446c0aa04fdae3529ef02cf552e63782e841c24f3c4cb481b4b947859,<br>78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17,<br>7a8c7166ebdae96e7adceaf50c064bf1cf85d3c360a6ff513414dc3078a6aa54,<br>9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a,<br>a5296d07dabb3d7b53fce4cf803190bfa57e062abeb11a6d801250acb7005c5f,<br>c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd,<br>d1db583aad156dc4edd093a64aade4180a77477cb247347e3fc97cae401d061f,<br>d455264bbb253a659149ba186f872920d83e3c6a0cab13965aa52a6b49406019,<br>d7429c7ecea552403d8e9b420578f954f5bf5407996afaa36db723a0c070c4de,<br>e9ac9436b5d61dd85e87e0fcd11b729a91466fe2f55f1f32501202d9ed98d562 |

# 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

**December 4, 2023 . 9:00 PM**



More at www.hivepro.com