Date of Publication
April 2, 2026

Hive Pro

Hiveforce Labs

MONTHLY

# THREAT DIGEST

## Vulnerabilities, Attacks, and Actors

MARCH 2026

# Table Of Contents


Summary..... 03

Insights..... 04

Threat Landscape..... 05

Vulnerabilities Summary..... 06

Attacks Summary..... 09

Adversaries Summary..... 13

Targeted Products..... 15

Targeted Countries..... 17

Targeted Industries..... 18

Top MITRE ATT&CK TTPs..... 19

Top Indicators of Compromise (IOCs)..... 20

Vulnerabilities Exploited..... 24

Attacks Executed..... 38

Adversaries in Action..... 63

MITRE ATT&CK TTPS..... 80

Top 5 Takeaways..... 86

Recommendations..... 87

Appendix..... 88

Indicators of Compromise (IoCs)..... 89

What Next?..... 95

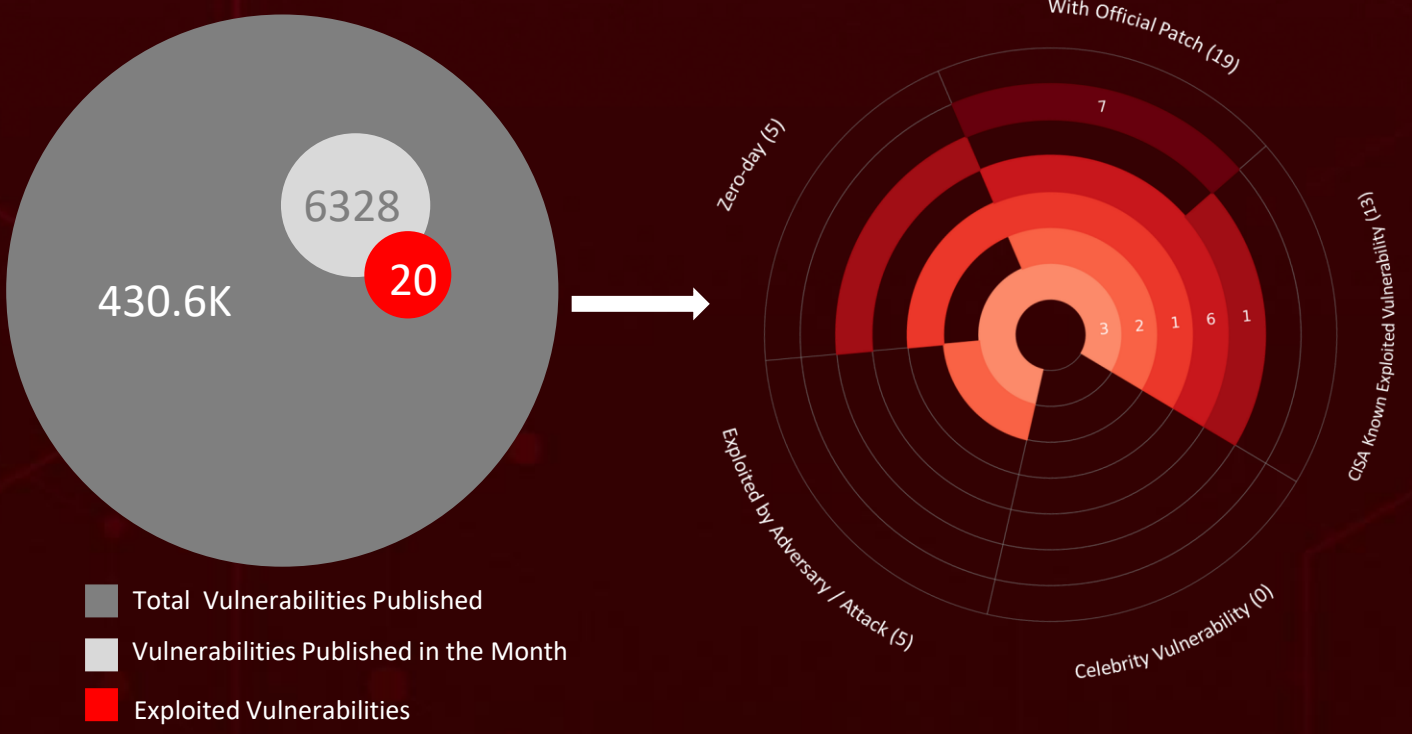
# Summary

**March** marked a turning point in the threat landscape, with five actively exploited zero-days reshaping the pace and urgency of cyber defense. Among the most concerning developments is the continued activity of **Void Manticore**, an Iranian state-backed group linked to MOIS. The group has intensified its hybrid warfare playbook, blending destructive wiper malware with coordinated data leaks and psychological operations to amplify disruption beyond the technical domain.

At the same time, the Russia-linked **APT28** has escalated its targeting of Ukrainian government entities, leveraging the Microsoft Office vulnerability **CVE-2026-21509** to gain footholds within critical systems. This activity underscores a persistent trend of state-sponsored actors rapidly operationalizing newly discovered flaws to support strategic intelligence objectives and destabilization efforts.

On the vulnerability front, vendors are racing to contain active exploitation. VMware pushed urgent patches for multiple flaws in VMware Aria Operations, including **CVE-2026-22719**, while Google Chrome users faced immediate risk from **CVE-2026-3909** and **CVE-2026-3910**. These vulnerabilities, affecting components like Skia and the V8 engine, highlight how browser-level flaws remain prime entry points for attackers.

Compounding the threat environment, rising geopolitical tensions have fueled a surge in cyber-enabled influence and intrusion campaigns. Threat actors are capitalizing on this climate through **phishing lures**, credential harvesting, and multi-stage malware delivery. Simultaneously, the **TeamPCP** supply chain campaign signals a shift toward ecosystem-level compromise, targeting widely used developer tools. As these risks converge, proactive patching, supply chain scrutiny, and layered defenses are no longer optional; they are operational imperatives.



# Insights

In March 2026, a geopolitical cybersecurity landscape unfolds, revealing the **United States, Kuwait, Bahrain, Qatar, Israel,** and **the United Arab Emirates** are the top-targeted countries

Highlighted in **March 2026** is a cyber battleground encompassing the **Government, Healthcare, Defense, Financial, Education,** and **NGOs** sectors, designating them as the top industries

**Void Manticore** is blending wiper-driven destruction, data leaks, and psychological ops into a coordinated playbook of modern hybrid cyber warfare.

Active exploitation of Cisco Catalyst SD-WAN Manager flaws (**CVE-2026-20122** and **CVE-2026-20128**) is turning enterprise networks into immediate, real-world attack surfaces.

Iran-linked actors are turning everyday **IP cameras** into battlefield sensors, enabling real-time reconnaissance and precision-driven battle damage assessment for missile operations.

**Interlock** ransomware weaponized Cisco FMC's **CVE-2026-20131** as a zero-day, enabling unauthenticated root-level Java RCE through deserialization flaws.

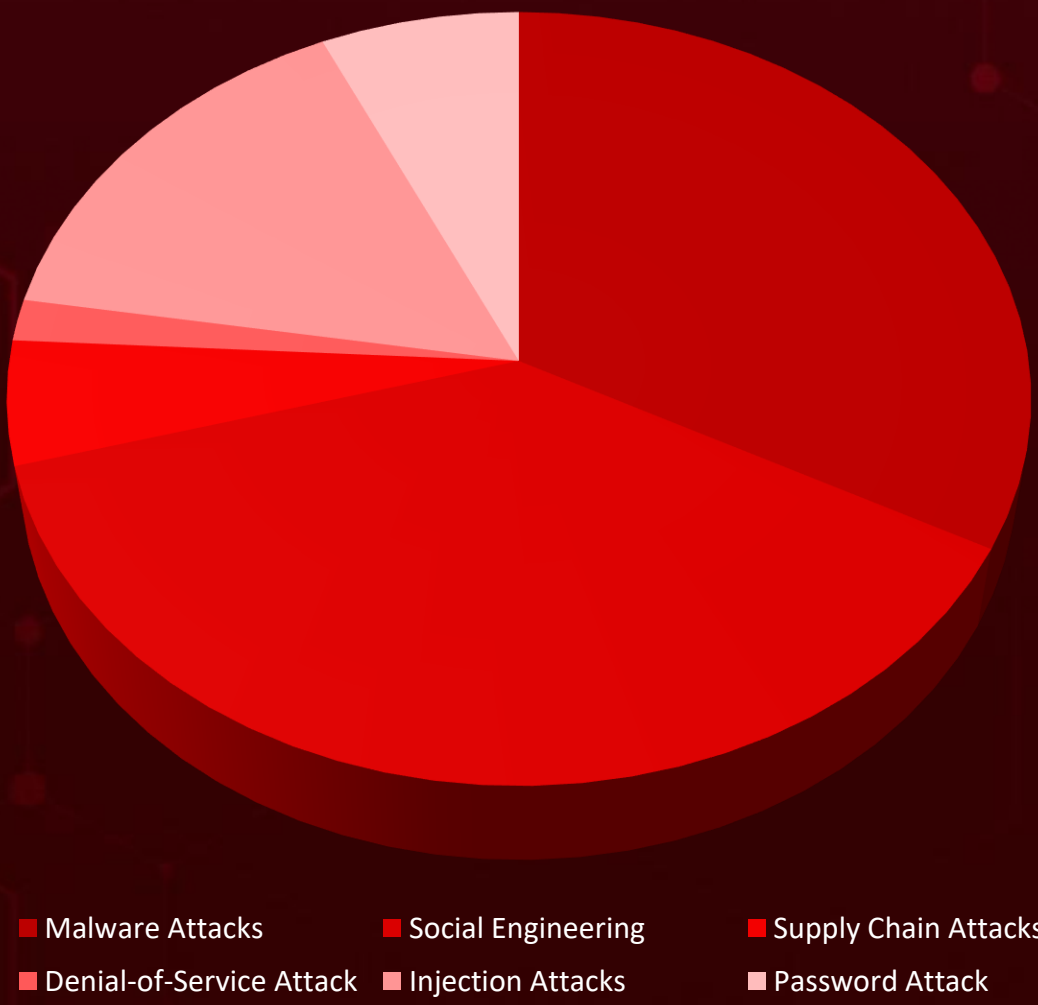
**TeamPCP** is weaponizing the software supply chain, backdooring tools like Trivy and LiteLLM to siphon credentials across npm, PyPI, and GitHub CI/CD pipelines.

**MuddyWater** is blending spear-phishing with Dindoor and Fakeset backdoors, leveraging cloud exfiltration and Telegram-based C2 to quietly sustain espionage operations.

**Dust Specter** is exploiting trust in government channels, using MFA impersonation and ClickFix-style lures to stealthily deliver advanced .NET malware to high-value officials.

**APT37's** Ruby Jumper turns a simple LNK into a stealthy, cloud-driven espionage chain.

# Threat Landscape

# Vulnerabilities Summary

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-22719 | Broadcom VMware Aria Operations Command Injection Vulnerability | Broadcom VMware Aria Operations | ✗ | ✓ | ✓ |
| CVE-2026-20122 | Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability | Cisco Catalyst SD-WAN Manager | ✗ | ✗ | ✓ |
| CVE-2026-20128 | Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability | Cisco Catalyst SD-WAN Manager | ✗ | ✗ | ✓ |
| CVE-2019-0604 | Microsoft SharePoint Remote Code Execution Vulnerability | Microsoft SharePoint | ✗ | ✓ | ✓ |
| CVE-2026-26127 | .NET Denial of Service Vulnerability | Microsoft.Bcl.Memory | ✗ | ✗ | ✓ |
| CVE-2026-21262 | SQL Server Elevation of Privilege Vulnerability | Microsoft SQL Server | ✗ | ✗ | ✓ |
| CVE-2026-21509 | Microsoft Office Security Feature Bypass Vulnerability | Microsoft Office | ✗ | ✗ | ✓ |
| CVE-2026-3909 | Google Skia Out-of-Bounds Write Vulnerability | Google Chrome | ✓ | ✓ | ✗ |
| CVE-2026-3910 | Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability | Google Chrome | ✓ | ✓ | ✓ |
| CVE-2017-7921 | Hikvision Multiple Products Improper Authentication Vulnerability | Hikvision | ✓ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2021-36260 | Hikvision Multiple Products Improper Input Validation Vulnerability | Hikvision | ✗ | ✓ | ✓ |
| CVE-2023-6895 | Hikvision Intercom Broadcasting System Command Injection Vulnerability | Hikvision | ✗ | ✗ | ✓ |
| CVE-2025-34067 | HIKVISION Integrated Security Management Platform Remote Command Execution Vulnerability | Hikvision | ✗ | ✗ | ✓ |
| CVE-2021-33044 | Authentication Bypass Vulnerability | | ✗ | ✓ | ✓ |
| CVE-2025-66376 | Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability | Zimbra Collaboration (ZCS) | ✗ | ✓ | ✓ |
| CVE-2026-20131 | Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability | Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management | ✓ | ✓ | ✓ |
| CVE-2026-20079 | Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability | Cisco Secure Firewall Management Center Software | ✗ | ✗ | ✓ |
| CVE-2026-33017 | Langflow Code Injection Vulnerability | Langflow Langflow | ✗ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-1731 | BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability | BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) | ✗ | ✓ | ✓ |
| CVE-2026-1281 | Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability | Ivanti Endpoint Manager Mobile (EPMM) | ✓ | ✓ | ✓ |

# Attacks Summary

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| Dohdoor | Backdoor | - | - | - | Phishing |
| RESTLEAF | Downloader | - | - | - | Phishing |
| SNAKEDROPPER | Loader | - | - | - | RESTLEAF malware |
| THUMBSBD | Backdoor | - | - | - | SNAKEDROPPER |
| VIRUSTASK | Tool | - | - | - | SNAKEDROPPER |
| FOOTWINE | Backdoor | - | - | - | VIRUSTASK |
| BLUELIGHT | Backdoor | - | - | - | VIRUSTASK |
| SPLITDROP | Dropper | - | - | - | Phishing |
| TWINTASK | Backdoor | - | - | - | SPLITDROP |
| TWINTALK | Backdoor | - | - | - | SPLITDROP |
| GHOSTFORM | RAT | - | - | - | Phishing |
| ClipXDaemon | Clipper | - | Linux (X11 Desktop Environments) | - | - |
| A0Backdoor | Backdoor | - | - | - | Social Engineering |
| LOTUSLITE | Backdoor | - | - | - | Phishing |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| BiBi Wiper | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Cl Wiper | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| No-Justice Wiper | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| SlimAgent | Spying tool | CVE-2026-21509 | Microsoft Office | ✓ | Exploiting The Microsoft Office Vulnerability |
| BeardShell | Backdoor | CVE-2026-21509 | Microsoft Office | ✓ | Exploiting The Microsoft Office Vulnerability |
| Covenant | Framework | CVE-2026-21509 | Microsoft Office | ✓ | Exploiting The Microsoft Office Vulnerability |
| VENON | RAT | - | - | - | Phishing |
| Slopoly | Framework | - | - | - | Social Engineering |
| NodeSnake | RAT | - | - | - | Social Engineering |
| Interlock | Ransomware | CVE-2026-20131 | Cisco Secure Firewall Management Center (FMC) Software, Cisco Security Cloud Control (SCC) Firewall Management | ✓ | Social Engineering, Exploiting Vulnerability |
| InterlockRAT | RAT | - | - | - | Social Engineering |
| AppleChris | Backdoor | - | - | - | Phishing |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| MemFun | Backdoor | - | - | - | Phishing |
| Getpass | Credential Harvester | - | - | - | Phishing |
| LeakNet | Ransomware | - | - | - | Social Engineering |
| Deno | Loader | - | - | - | Social Engineering |
| EndRAT | RAT | - | - | - | Phishing |
| RftRAT | RAT | - | - | - | Phishing |
| RemcosRAT | RAT | - | - | - | Phishing |
| Vidar Stealer 2.0 | Stealer | - | - | - | Fake game cheat repositories |
| Rhadamanthys | Infostealer | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Hatef | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Hamsa | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Handala | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Handala PowerShell | Wiper | CVE-2019-0604 | Microsoft SharePoint | ✓ | Phishing |
| Dindoor | Backdoor | - | - | - | Spear-phishing |
| Fakeset | Backdoor | - | - | - | Cloud-hosted payload |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| Stagecomp | Downloader | - | - | - | Signed binary |
| Darkcomp | Backdoor | - | - | - | Dropped by Stagecomp |
| LampoRAT | RAT | - | - | - | Spear-phishing |
| UDPGangster | Backdoor | - | - | - | Macro-laced Office documents |
| BlackBeard | Backdoor | - | - | - | Macro documents, process hollowing |
| Nuso | Backdoor | - | - | - | Macro-laced Excel documents |
| Phoenix | Backdoor | - | - | - | Macro-laced Office documents |
| CanisterWorm | Worm | - | - | - | npm supply chain compromise |
| Beast Ransomware | Ransomware | - | - | - | Phishing, compromised RDP |

# Adversaries Summary

| ACTOR NAME | MOTIVE | ORIGIN | CVEs | ATTACK | PRODUCT |
|---|---|---|---|---|---|
| APT37 | Information theft and espionage | North Korea | - | - | - |
| Dust Specter | Information theft and espionage | Iran | - | SPLITDROP, TWINTASK, TWINTALK, GHOSTFORM | - |
| Mustang Panda | Information theft and espionage | China | - | LOTUSLITE | - |
| Void Manticore | Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated | Iran | CVE-2019-0604 | BiBi Wiper, Cl Wiper, No-Justice Wiper, Handala Wiper, Handala PowerShell Wiper, Rhadamanthys, Hatef Wiper, Hamsa Wiper | Windows Microsoft SharePoint and Linux |
| APT28 | Information theft and espionage | Russia | CVE-2026-21509 | SlimAgent, BeardShell, Covenant | Microsoft Office |
| Hive0163 | Information theft and espionage, Financial gains | - | - | Slopoly, NodeSnake, Interlock ransomware, InterlockRAT | - |
| UNK_InnerAmbush | Information theft and espionage | China | - | - | - |
| TA402 | Information theft and espionage | Gaza | - | - | - |

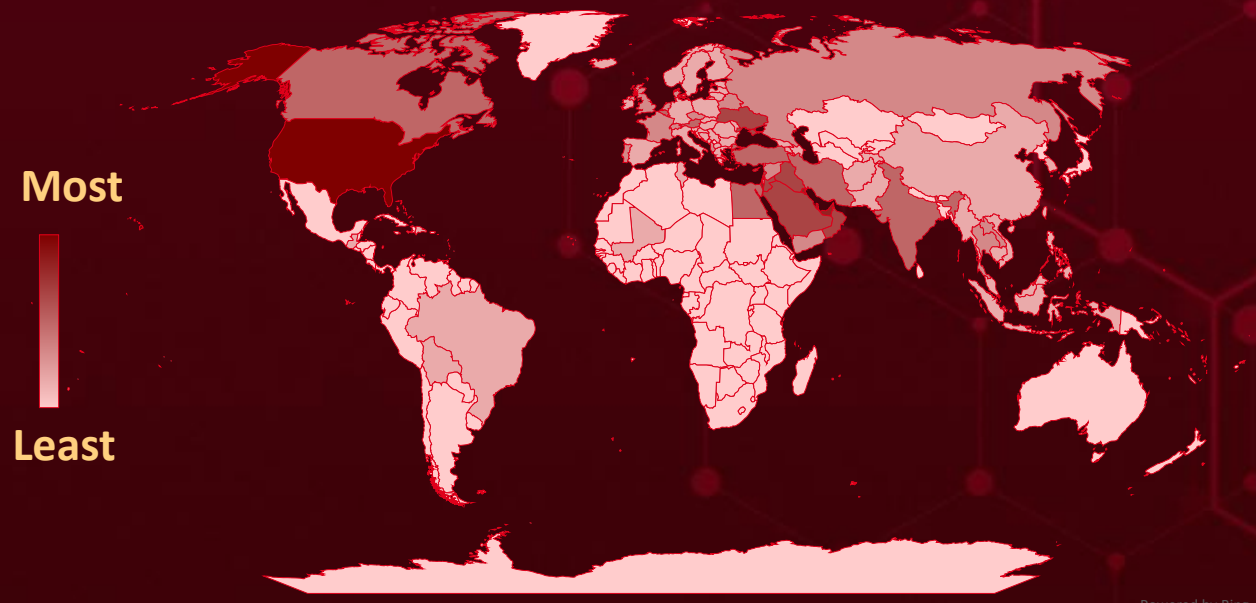
| ACTOR NAME | MOTIVE | ORIGIN | CVEs | ATTACK | PRODUCT |
|---|---|---|---|---|---|
| UNK_RobotDreams | Information theft and espionage | Pakistan | - | - | - |
| UNK_NightOwl | Information theft and espionage | - | - | - | - |
| TA473 | Information theft and espionage | - | - | - | - |
| TA453 | Information theft and espionage | Iran | - | - | - |
| CL-STA-1087 | Information theft and espionage | China | - | AppleChris, MemFun, Getpass | - |
| Konni | Information theft and espionage | North Korea | - | EndRAT, RftRAT, RemcosRAT | KakaoTalk PC Application |
| MuddyWater | Cyber Espionage, Intelligence Collection, Pre-positioning for Potential Destructive Operations | Iran | CVE-2026-1731 CVE-2026-1281 | Dindoor, Fakeset, Stagecomp, Darkcomp, LampoRAT, UDPGangster, BlackBeard, Nuso, Phoenix | Windows, Linux |
| Prince of Persia | Information theft and Espionage | Iran | - | - | - |
| TeamPCP | Espionage, Sabotage, Disruption, Financial Gains | - | - | CanisterWorm | Docker APIs, Kubernetes clusters, and CI/CD pipelines |

# Targeted Products

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| vmware by Broadcom | Hybrid Cloud Infrastructure Platform, Virtualization Platform | Broadcom Vmware Cloud Foundation, Broadcom Vmware vSphere Foundation Version Before 9.0.2.0 Broadcom Vmware Aria Operations (Before 8.18.6 / Before 9.0.2.0), VMware Telco Cloud Platform, Vmware Telco Cloud Infrastructure |
| cisco | Network Infrastructure Management | Cisco Catalyst SD- WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1) |
| | Security Management Platform, Cloud-Based Security Management Platform | Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management |
| Microsoft | On-premises server application | Microsoft SharePoint Server 2019, 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Foundation 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Enterprise Server 2016 |
| | Software Library | Microsoft.Bcl.Memory 9.0, 10.0; .NET 9.0 installed on Windows, Mac OS, Linux; .NET 10.0 installed on Linux, Mac OS, Windows |
| | Database Management System (DBMS) / Server Software | Microsoft SQL Server 2025, 2022, 2019, 2017, 2016 |
| | Software | Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems) |
| | Browser | Google Chrome (before 146.0.7680.75) |
| alhua TECHNOLOGY | Network-Connected Hardware Device | |
| zimbra A SYNACOR PRODUCT | Enterprise Collaboration & Messaging Server (Server Software) | Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13 |

| VENDOR | PRODUCT TYPE | PRODUCT ALONG WITH VERSION |
|---|---|---|
| HIKVISION | IoT / Surveillance Hardware | Hikvision DS-2CD2xx2F-I Series V5.2.0 build 140721 to V5.4.0 build 160530, DS-2CD2xx0F-I Series V5.2.0 build 140721 to V5.4.0 Build 160401, DS-2CD2xx2FWD Series V5.3.1 build 150410 to V5.4.4 Build 161125, DS-2CD4x2xFWD Series V5.2.0 build 140721 to V5.4.0 Build 160414, DS-2CD4xx5 Series V5.2.0 build 140721 to V5.4.0 Build 160421, DS-2DFx Series V5.2.0 build 140805 to V5.4.5 Build 160928, and DS-2CD63xx Series V5.0.9 build 140305 to V5.3.5 Build 160106 devices. |
| | IoT Communication & Broadcasting System | Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) |
| | Physical Security Management Platform | HIKVISION Integrated Security Management Platform |
| Langflow | AI Application Development Platform | Langflow Langflow version before 1.9.0 |
| BeyondTrust | Privileged Remote Access & Support Platform | BeyondTrust Remote Support: Before 25.3.2 BeyondTrust Privileged Remote Access: Before 25.1.1 |
| ivanti | Unified Endpoint Management (UEM) / Mobile Device Management Platform | Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior |

# Targeted Countries




| Color | Countries |
|---|---|
| | United States |
| | Kuwait |
| | Bahrain |
| | Qatar |
| | Israel |
| | United Arab Emirates |
| | Saudi Arabia |
| | Cyprus |
| | Ukraine |
| | Oman |
| | Iraq |
| | Jordan |
| | Lebanon |
| | Egypt |
| | Austria |
| | Iran |
| | Belgium |
| | Turkey |
| | Canada |
| | India |
| | Denmark |
| | Switzerland |

| Color | Countries |
|---|---|
| | Portugal |
| | Akrotiri and Dhekelia |
| | Thailand |
| | France |
| | Palestine |
| | United Kingdom |
| | Russia |
| | Belarus |
| | Syria |
| | Laos |
| | Czech Republic |
| | Albania |
| | Netherlands |
| | Yemen |
| | Poland |
| | Tajikistan |
| | Slovakia |
| | Greece |
| | Norway |

| Color | Countries |
|---|---|
| | Sweden |
| | Hungary |
| | Bulgaria |
| | Iceland |
| | Bosnia and Herzegovina |
| | Cambodia |
| | Republic of Ireland |
| | Indonesia |
| | Serbia |
| | Azerbaijan |
| | South Korea |
| | Italy |
| | Estonia |
| | Andorra |
| | Timor-Leste |
| | China |
| | Georgia |
| | Latvia |
| | Pakistan |
| | Afghanistan |

| Color | Countries |
|---|---|
| | Philippines |
| | Liechtenstein |
| | Brazil |
| | Vietnam |
| | Romania |
| | Croatia |
| | San Marino |
| | Malaysia |
| | Singapore |
| | Mali |
| | Slovenia |
| | Malta |
| | Spain |
| | Mauritius |
| | Brunei |
| | Moldova |
| | Taiwan |
| | Monaco |
| | Finland |
| | Montenegro |
| | Tunisia |

| Color | Countries |
|---|---|
| | Guadeloupe |
| | Saint Lucia |
| | Barbados |
| | Tonga |
| | Algeria |
| | Antigua and Barbuda |
| | Isle of Man |
| | Ghana |
| | American Samoa |
| | Guinea |
| | Colombia |
| | Aruba |
| | Ivory Coast |
| | Fiji |
| | Jamaica |
| | Rwanda |
| | Japan |
| | Cameroon |
| | Jersey |
| | Bhutan |

# Targeted Industries

Most


Least

# TOP 25 MITRE ATT&CK TTPS

| | | | | |
|---|---|---|---|---|
| **T1059** Command and Scripting Interpreter | **T1204** User Execution | **T1071** Application Layer Protocol | **T1071.001** Web Protocols | **T1566** Phishing |
| **T1036** Masquerading | **T1082** System Information Discovery | **T1027** Obfuscated Files or Information | **T1204.002** Malicious File | **T1059.001** PowerShell |
| **T1102** Web Service | **T1041** Exfiltration Over C2 Channel | **T1190** Exploit Public-Facing Application | **T1053** Scheduled Task/Job | **T1574** Hijack Execution Flow |
| **T1583** Acquire Infrastructure | **T1070** Indicator Removal | **T1021** Remote Services | **T1005** Data from Local System | **T1547** Boot or Logon Autostart Execution |
| **T1036.005** Match Legitimate Resource Name or Location | **T1140** Deobfuscate/Decode Files or Information | **T1588** Obtain Capabilities | **T1598.002** Spearphishing Attachment | **T1105** Ingress Tool Transfer |

# Top Indicators of Compromise (IOCs)

| Attack Name | TYPE | VALUE |
|---|---|---|
| LOTUSLITE | MD5 | 10fb1122079b5ae8e4147253a937f40f |
| | SHA1 | 7d4e31c8b11be7c970860c4fbc8fe85c70724cb1 |
| | SHA256 | 856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216 |
| BiBi Wiper | SHA256 | 74d8d60e900f931526a911b7157511377c0a298af986d42d373f51aac4f362f6 |
| Cl Wiper | SHA256 | e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0 |
| No-Justice Wiper | SHA256 | 36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f |
| SlimAgent | SHA1 | 5603e99151f8803c13d48d83b8a64d071542f01b |
| | SHA256 | 9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c |
| BeardShell | SHA1 | 6d39f49aa11ce0574d581f10db0f9bae423ce3d5 |
| | SHA256 | 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1 |
| Covenant | SHA256 | 27a331384cfca9a4d2aa45afdc12c7156cfb4da775f1380d4870f06fbb77ccf2,<br>62d3b82ac3688b1c00adce7cd241de2a50c24caac4ed6b8e46b16da1266457eb,<br>1b2b83d462493eb63d6655103cf968d396ee7bdf7dd317f8cb5a5eadee6b560f |
| VENON | IPv4 | 206[.]0[.]29[.]58,<br>51[.]222[.]75[.]250,<br>51[.]222[.]75[.]248,<br>192[.]99[.]226[.]117,<br>212[.]69[.]5[.]84,<br>34[.]227[.]229[.]85 |
| | SHA256 | c482286a7fdfb64d308c197a4deabcd773b8b62d9e74d1d08fcfd02568d75d72,<br>d61be2b21e135726c547a388ecb47552559e5221894f5005ce35bdb24efc0c26 |
| AppleChris | SHA256 | 9e44a460196cc92fa6c6c8a12d74fb73a55955045733719e3966a7b8ced6c500,<br>5a6ba08efcef32f5f38df544c319d1983adc35f3db64f77fa5b51b44d0e5052c,<br>0e255b4b04f5064ff97da214050da81a823b3d99bce60cdd9ee90d913cc4a952, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| AppleChris | SHA256 | 413daa580db74a38397d09979090b291f916f0bb26a68e7e0b03b4390c1b472f, 2ee667c0ddd4aa341adf8d85b54fbb2fce8cc14aa88967a5cb99babb08a10fae |
| MemFun | SHA256 | ad25b40315dad0bda5916854e1925c1514f8f8b94e4ee09a43375cc1e77422ad |
| Getpass | SHA256 | ee4d4b7340b3fa70387050cd139b43ecc65d0cfd9e3c7dcb94562f5c9c91f58f |
| Deno | Domains | okobojirent[.]com, mshealthmetrics[.]com, verify-safeguard[.]top, neremedysoft[.]com, ndibstersoft[.]com, windowallclean[.]com, cnoocim[.]com, delhedghogeggs[.]com, serialmenot[.]com, crahdhduf[.]com, weaplink[.]com |
| | IPv4 | 194[.]31[.]223[.]42, 144[.]31[.]2[.]161, 87[.]121[.]79[.]6, 87[.]121[.]79[.]25, 144[.]31[.]54[.]243, 144[.]31[.]224[.]98 |
| Interlock Ransomware Group | SHA256 | e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f |
| Rhadamanthys | SHA256 | aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f |
| Hatef | SHA256 | e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35 |
| Hamsa | URL | hxxp[:]//sjc1[.]vultrobjects[.]com/f5update/update[.]sh |
| | SHA256 | 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad |
| Handala | MD5 | 5986ab04dd6b3d259935249741d3eff2 |
| | SHA256 | 454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| Handala PowerShell | MD5 | 3cb9dea916432ffb8784ac36d1f2d3cd |
| Dindoor | SHA256 | 0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542, 1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1, 2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043, 2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5, 42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f, 7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4, 7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef, b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0, bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a, c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e |
| Fakeset | SHA256 | 077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de, 15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84, |
| UDPGangster | PDB Path | C:\Users\piper\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb, C:\Users\gangster\source\repos\udp_3.0 - Copy - Copy\x64\release_86\udp_3.0.pdb, C:\Users\SURGE\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb |
| BlackBeard | IPv4 | 159[.]198[.]68[.]25, 159[.]198[.]66[.]153 |
| | SHA256 | 156b325231742a73ded4104fbde1c55ad3913d2eaf09b5194ef74c81ee3ba393, cc2ec568f978f328b6de112670a1b35ca1f9db377ff32cb9d313a5b2ac3c127b, 7523e53c979692f9eecff6ec760ac3df5b47f172114286e570b6bba3b2133f58, 0be499354dc498248d27f6d186eb3bb75a607ae4a2c0a6734c76f1a1b7b1d316, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79, 1bcd8d7dc7bed5873bbdd2822e84e19773a33d659b16587ca9dc6db204447a86 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| Nuso | SHA256 | 1b9e6fe4b03285b2e768c57e320d84323ac9167598395918d56a12e568b0009a, 9c207c51c448f96eaae91241a39c8bb85e2307f2d2a99244763a53176cf4c02f, c91413ad7c94c0e2694862b9d671d1204873bf65576ba2cb91fbd562a4ccf79b |
| | PDB Path | C:\Users\nuso\source\repos\http_vip\http_vip\f*ckAnalyzor.pdb, C:\Users\nuso\source\repos\http_last_ver\http_last_ver\f*ckAnalyser.pdb |
| Phoenix | IPv4 | 46[.]101[.]36[.]39 |
| | SHA256 | 668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839 |
| | PDB Path | C:\Users\win10\Desktop\phonix\phoenix\x64\Release\phoenix.pdb, D:\phonix\phoenixV3\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Debug\phoenix.pdb |
| CanisterWorm | SHA256 | c37c0ae9641d2e5329fcdee847a756bf1140fdb7f0b7c78a40fdc39055e7d926 |
| Beast Ransomware | SHA256 | 6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0, 479d0947816467d562bf6d24b295bf50512176a2d3d955b8f4d932aea2378227, cc0680de960f3e1b727b61a42e59f9c282bd8e41fe20146ed191c7f4bf9283a7, cf5c45be416d1b18dd67ffa95c6434691f1f9ba9c30754fa6fc9978c1f975750, 2ce62601491549ab91c9517e0accf3286ed29976f6ec359d31ddc060a8d99eb3, 812df0efea089b956d08352ff0a7e8789d43862dc3764f4441d4e1c1d1fb7957, 5bd8f9cbd108abc53fb1c44b8d10239a2a0a9dd20c698fd2fb5dc1938ae7ba96 |
| | IPv4 | 5[.]78[.]84[.]144 |

# Vulnerabilities Exploited

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-22719 | ✗ | Broadcom VMware Cloud Foundation, Broadcom VMware vSphere Foundation Version Before 9.0.2.0 Broadcom VMware Aria Operations (Before 8.18.6 / Before 9.0.2.0), VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure | - |
| | ZERO-DAY | | |
| | ✗ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:vmware:aria_operations:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:* | - |
| Broadcom VMware Aria Operations Command Injection Vulnerability | ✓ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-20122 | ✗ | Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1) | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:* | - |
| Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-648 | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-20128 | ✗ | Cisco Catalyst SD-WAN Manager (Before 20.18) | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:* | - |
| Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-257 | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="6">CVE-2019-0604</td><td>  </td><td rowspan="3">Microsoft SharePoint Server 2019, 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Foundation 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Enterprise Server 2016</td><td rowspan="3">Void Manticore</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="3">cpe:2.3:a:microsoft:sharepoint_enterprise_server:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*</td><td rowspan="3">BiBi Wiper, Cl Wiper, No-Justice Wiper, Handala Wiper, Handala PowerShell Wiper, Rhadamanthys, Hatef Wiper, Hamsa Wiper</td></tr>
<tr><td rowspan="3">Microsoft SharePoint 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-20</td><td>T1190: Exploit Public-Facing Application, T1505: Server Software Component, T1505.003: Web Server, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1608: Stage Capabilities, T1608.001: Upload Malware</td><td>https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-26127 | ✗ | Microsoft.Bcl.Memory 9.0, 10.0; .NET 9.0 installed on Windows, Mac OS, Linux; .NET 10.0 installed on Linux, Mac OS, Windows | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:microsoft:.net_core:*:*:*:*:*:*:*:* | - |
| .NET Denial of Service Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-125 | T1498: Network Denial of Service, T1499: Endpoint Denial of Service, T1499.001: OS Exhaustion Flood | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26127 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-21262 | ✗ | Microsoft SQL Server 2025, 2022, 2019, 2017, 2016 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:microsoft:sql_server_*:*:*:*:*:*:*:*:* | - |
| SQL Server Elevation of Privilege Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-284 | T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts, T1078.002: Domain Accounts | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21262 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-21509 | ✗ | Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems) | APT28 |
| | ZERO-DAY | | |
| | ✓ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:enterprise:*:*:* | SlimAgent, BeardShell, Covenant |
| Microsoft Office Security Feature Bypass Vulnerability | ✓ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-807 | T1566: Phishing, T1204: User Execution, T1204.002: Malicious File, T1055: Process Injection | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-3909 | ✗ | Google Chrome (before 146.0.7680.75) | - |
| | ZERO-DAY | | |
| | ✓ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* | - |
| Google Skia Out-of- Bounds Write Vulnerability | ✓ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-787 | T1189: Drive-By Compromise; T1203: Exploitation for Client Execution | ✗ |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-3910</td><td>  </td><td rowspan="2">Google Chrome (before 146.0.7680.75)</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:google:chrome:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94, CWE-119</td><td>T1189: Drive-By Compromise; T1059: Command and Scripting Interpreter</td><td>https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2017-7921</td><td>✗</td><td rowspan="2">Hikvision DS-2CD2xx2F-I Series V5.2.0 build 140721 to V5.4.0 build 160530, DS-2CD2xx0F-I Series V5.2.0 build 140721 to V5.4.0 Build 160401, DS-2CD2xx2FWD Series V5.3.1 build 150410 to V5.4.4 Build 161125, DS-2CD4x2xFWD Series V5.2.0 build 140721 to V5.4.0 Build 160414, DS-2CD4xx5 Series V5.2.0 build 140721 to V5.4.0 Build 160421, DS-2DFx Series V5.2.0 build 140805 to V5.4.5 Build 160928, and DS-2CD63xx Series V5.0.9 build 140305 to V5.3.5 Build 160106 devices.</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:hikvision:ds-2cd2032-i_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:hikvision:ds-2cd2112-i_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:hikvision:ds-2cd2212-i5_firmware:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Hikvision Multiple Products Improper Authentication Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-287</td><td>T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation</td><td>https://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2021-36260 | ✗ ZERO-DAY | Hikvision Multiple Products | - |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:hikvision:ds-2cd2026g2-iu\/sl_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:hikvision:ds-2cd2046g2-iu\/sl_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:hikvision:ds-2cd2066g2-i\(u\)_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:hikvision:ds-2cd2086g2-i\(u\)_firmware:-:*:*:*:*:*:*:* | - |
| Hikvision Multiple Products Improper Input Validation Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter | https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/ |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2023-6895 | ✗ ZERO-DAY | HikvHikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) | - |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:hikvision:intercom_broadcast_system:*:*:*:*:*:*:*:* | - |
| Hikvision Intercom Broadcasting System Command Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-78 | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter | https://www.hikvision.com/en/support/download/software/ |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2025-34067 | ✗ | HIKVISION Integrated Security Management Platform | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:hikvision:integrated_security_management_platform:*:*:*:*:*:*:*:* | - |
| HIKVISION Integrated Security Management Platform Remote Command Execution Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-502 | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter | https://www.hikvision.com/europe/support/cybersecurity/security-advisory/clarification-on-hikvision-software---fastjson-vulnerability--cv/ |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2021-33044 | ✗ | | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dahuasecurity:ipc_firmware:*:*:*:*:*:*:*:* | - |
| Authentication Bypass Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-287 | T1190: Exploit Public-Facing Application; T1556: Modify Authentication Process | https://www.dahuasecurity.com/download-center/firmware |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2025-66376 | ✗ | Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:* | - |
| Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-79 | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter | https://wiki.zimbra.com/wiki/Zimbra_Releases |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-20131 | ✗ | Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:security_cloud_control:*:*:*:*:*:*:*:* | Interlock Ransomware Group |
| Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-502 | T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-20079</td><td>✗</td><td rowspan="2">Cisco Secure Firewall Management Center (FMC) Software</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:cisco:secure_firewall_management_center:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-288</td><td>T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2</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-2026-33017</td><td>  </td><td rowspan="2">Langflow Langflow version before 1.9.0</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:langflow:langflow:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Langflow Code Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94, CWE-95, CWE-306</td><td>T1190: Exploit Public-Facing Application, T1059.006: Command and Scripting Interpreter: Python</td><td>https://github.com/langflow-ai/langflow/releases</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-2026-1731</td><td>  </td><td rowspan="2">BeyondTrust Remote Support: Before 25.3.2<br>BeyondTrust Privileged Remote Access: Before 25.1.1</td><td rowspan="2">MuddyWater</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:beyondtrust:remote_support:*:*:*:*:*:*:*:*<br>cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://www.beyondtrust.com/trust-center/security-advisories/bt26-02</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-1281</td><td>✗</td><td rowspan="2">Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior</td><td rowspan="2">MuddyWater</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:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*<br>cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*<br>cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*<br>cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*<br>cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</td></tr>
</table>

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Dohdoor | Dohdoor uses a method called DNS-over-HTTPS (DoH) to communicate with its control server. It can also download and run additional malicious files in memory without writing them to the disk. Once it infects a system, it creates a hidden backdoor, allowing the attacker to load and run further malicious payloads, like Cobalt Strike Beacon, directly in the system's memory through legitimate Windows processes. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Evades detection, Deploys other malware | Windows |
| Backdoor | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| RESTLEAF | RESTLEAF is an initial malware that uses Zoho WorkDrive to communicate with its control server and fetch more malicious files. It gets a valid access token by using embedded credentials, allowing it to perform further actions on Zoho WorkDrive. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Bypasses traditional communication channels, Fetches additional malware | Windows |
| Downloader | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| APT37 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| SNAKEDROPPER | SNAKEDROPPER is a loader that installs the Ruby runtime, ensures the malware stays active on the system, and drops additional malicious files like THUMBSBD and VIRUSTASK. It prepares for execution by replacing a key file, `operating_system.rb`, with a modified version that automatically loads when Ruby starts. | RESTLEAF malware | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Persistence, Drops additional malware | Windows |
| Loader | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| APT37 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| THUMBSBD | THUMBSBD is disguised as a Ruby file called `ascii.rb`. It uses removable media to connect separate network segments, allowing two-way communication and data theft across isolated networks. | SNAKEDROPPER | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Data Exfiltration | Windows |
| Backdoor | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| APT37 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| VIRUSTASK | VIRUSTASK is a tool that spreads through removable media by replacing files with malicious LNK shortcuts. It runs a multi-stage infection process that takes control of files. | SNAKEDROPPER | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Persistence | Windows |
| Tool | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| APT37 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| FOOTWINE | FOOTWINE is a backdoor delivered later in the attack. It's an encrypted payload with a shellcode launcher that includes surveillance features like keylogging and audio/video capturing. | VIRUSTASK | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Surveillance, Remote Access | Windows |
| Backdoor | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| APT37 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| BLUELIGHT | BLUELIGHT is a backdoor that uses cloud services like Google Drive, OneDrive, pCloud, and BackBlaze for communication. Its functions include executing commands, browsing files, downloading additional malware, uploading files, and removing itself. | VIRUSTASK | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Data theft, Downloads additional malware | Windows |
| Backdoor | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| APT37 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| SPLITDROP | SPLITDROP is a .NET-based dropper that uses a user-provided password to decrypt embedded malware and carry out its attack. | Phishing | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Facilitates attack, Bypasses detection | Windows |
| Dropper | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Dust Specter | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| TWINTASK | TWINTASK is a worker module that repeatedly checks a file for new commands every 15 seconds and runs them using PowerShell. It operates in an endless loop. | SPLITDROP | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Remote Control | Windows |
| Backdoor | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Dust Specter | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| TWINTALK | TWINTALK is a 32-bit .NET DLL that acts as a C2 orchestrator. It checks the C2 server for new commands, coordinates with the worker module, and sends back the results. It works alongside the worker module to execute commands using a file-based polling system. | SPLITDROP | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Data Exfiltration, Remote Control | Windows |
| Backdoor | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Dust Specter | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| GHOSTFORM | GHOSTFORM is a .NET-based RAT that combines all the functions of the initial attack into one file and runs PowerShell scripts in memory. It uses evasion techniques like invisible Windows forms and timers to delay its execution. | Phishing | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Defensive Evasion, Remote Control | Windows |
| RAT | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Dust Specter | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| ClipXDaemon | ClipXDaemon is an automated cryptocurrency clipboard hijacker. It uses the publicly available bincrypter framework to encrypt and hide shell payloads. | - | - |
| | | IMPACT | AFFECTED PLATFORM |
| TYPE | | Data Theft | Linux (X11 Desktop Environments) |
| Clipper | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| - | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| A0Backdoor | A0Backdoor uses runtime decryption to hide its core logic, making static analysis difficult. Upon execution, it allocates new memory and copies its code there. While this self-copying doesn't directly affect functionality, it's still significant. After decryption, the backdoor collects system-specific information to fingerprint the compromised machine. | Social Engineering | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | Obscured Behavior, Memory Manipulation, Information Theft | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| LOTUSLITE | LOTUSLITE is a C++ backdoor used for espionage, connecting to a hard-coded IP-based command-and-control server. It enables remote tasking, data theft, and ensures persistence, surviving system reboots. Its functionality is minimal but effective for covert operations. | Phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Backdoor | | Information Theft, Remote Control | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| Mustang Panda | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| BiBi Wiper | BiBi Wiper is a custom destructive malware designed to permanently damage files on compromised systems. It accepts command-line parameters such as target_path to specify which files or directories to wipe. The malware launches multiple threads based on the system's CPU cores to speed up the wiping process and uses a queue to coordinate tasks between them. It overwrites targeted files with random data and then renames them using random filenames with the ".BiBi" extension, rendering the files unusable. | Phishing | CVE-2019-0604 |
| | | **IMPACT** | **AFFECTED PRODUCT** |
| **TYPE** | | Information Theft, Operational disruption | Microsoft SharePoint |
| Wiper | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |
| Void Manticore | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Cl Wiper | Cl Wiper is a destructive malware that erases data by executing cl.exe with command-line arguments and abusing the legitimate rwdsk.sys driver from ElRawDisk to gain raw access to disks, files, and partitions. This allows the malware to overwrite critical data and render systems unusable. Notably, the license key embedded in the wiper matches one used in the ZeroCleare malware, which has previously been linked to actors associated with Iran's Ministry of Intelligence and Security (MOIS), suggesting possible tooling overlap. | Phishing | CVE-2019-0604 |
| | | **IMPACT** | **AFFECTED PRODUCT** |
| **TYPE** | | Information Theft, Operational disruption | Microsoft SharePoint |
| Wiper | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |
| Void Manticore | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| No-Justice Wiper | No-Justice wiper is a 220.34 KB binary that requires administrator privileges to erase the data on the computer. | Phishing | CVE-2019-0604 |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Information Theft, Operational disruption | Microsoft SharePoint |
| Wiper | | | PATCH LINK |
| ASSOCIATED ACTOR | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |
| Void Manticore | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| SlimAgent | SlimAgent is a lightweight espionage tool derived from XAgent, the primary backdoor used by the APT28 group. It is designed for stealthy surveillance and can log keystrokes, capture screenshots, and collect clipboard data, allowing attackers to monitor user activity and steal sensitive information. | Exploiting The Microsoft Office Vulnerability | CVE-2026-21509 |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Clipboard data theft | Microsoft Office |
| Spying tool | | | PATCH LINK |
| ASSOCIATED ACTOR | | | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509 |
| APT28 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| BeardShell | BeardShell is a sophisticated malware implant that executes PowerShell commands within a .NET runtime environment. It uses the legitimate cloud storage service Icedrive as its command-and-control (C2) channel, allowing attackers to issue commands and maintain remote access while blending malicious traffic with normal cloud activity. | Exploiting The Microsoft Office Vulnerability | CVE-2026-21509 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Backdoor | | Persistent unauthorized access | Microsoft Office |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| APT28 | | | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Covenant | Covenant is an open-source .NET post-exploitation framework that allows attackers to create and manage implants through a web-based dashboard. In espionage operations, it can be used for long-term system access and control, enabling attackers to manage compromised machines efficiently during extended campaigns. | Exploiting The Microsoft Office Vulnerability | CVE-2026-21509 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Framework | | Remote system control | Microsoft Office |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| APT28 | | | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509 |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| VENON | VENON is a Rust-based banking Remote Access Trojan (RAT) that targets financial platforms. It uses DLL sideloading through a legitimate NVIDIA executable, multiple anti-analysis evasion techniques, and advanced encryption to avoid detection. The malware also deploys credential-stealing banking overlays and uses VBScript-based shortcut hijacking to target banking applications. | Phishing | - |
| | | **IMPACT** | **AFFECTED PRODUCT** |
| **TYPE** | | Banking credential theft, Remote system control | Windows |
| RAT | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Slopoly | Slopoly a suspected AI-assisted PowerShell backdoor that was deployed in the later stages of the attack to maintain persistent access to the compromised server. Its use suggests the threat actor may have operated the C2 framework in a live, hands-on manner during the intrusion. | Social Engineering | - |
| | | **IMPACT** | **AFFECTED PRODUCT** |
| **TYPE** | | Persistent backdoor access | Windows, Linux |
| Framework | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| Hive0163 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| NodeSnake | NodeSnake, a NodeJS-based malware that acts as the first stage of a larger command-and-control (C2) framework. Once installed, NodeSnake communicates with its C2 server using HTTP POST requests, allowing attackers to establish initial control over the compromised system. | Social Engineering | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Persistent foothold | Windows, Linux |
| RAT | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Hive0163 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| InterlockRAT | InterlockRAT is a remote access trojan that allows attackers to remotely control infected systems, execute commands, steal credentials and files, and deploy additional payloads. It typically communicates with a command-and-control server to perform reconnaissance, exfiltrate system data, and maintain persistent access for follow-on attacks such as ransomware deployment. | Social Engineering | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote system control, Sensitive data exfiltration | Windows, Linux |
| RAT | | | PATCH LINK |
| ASSOCIATED ACTOR | | | - |
| Hive0163 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| AppleChris | AppleChris is a versatile malware strain designed for flexible deployment, delivered either as a standalone executable or as a DLL to better blend into compromised systems. In several cases, attackers have leveraged DLL hijacking by placing a malicious swprv32.sys component within the system32 directory, allowing it to be loaded by trusted processes. To maintain persistence, the malware registers itself as part of the Volume Shadow Copy Service, effectively gaining elevated privileges while masquerading as a legitimate Windows component, helping it stay under the radar and evade detection. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Privilege escalation, System Compromise | Windows |
| Backdoor | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| CL-STA-1087 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| MemFun | MemFun is a multi-stage, modular malware built for stealth and flexibility. It begins with an initial loader disguised as GoogleUpdate.exe, which operates entirely in memory to evade detection. This loader connects to a command-and-control (C2) server to fetch a secondary DLL payload containing the exported MemFun function, which is then executed to launch the main backdoor. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | System Compromise | Windows |
| Backdoor | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| CL-STA-1087 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Getpass | Getpass is a customized variant of Mimikatz, delivered as a standalone DLL and disguised as a legitimate Palo Alto Networks component within the Cyvera directory to avoid suspicion. Once executed, it invokes its vncpass function to escalate privileges by obtaining SeDebugPrivilege, enabling deep access to sensitive system processes. The malware then targets multiple Windows authentication packages, such as MSV, WDigest, Kerberos, and CloudAP, to extract plaintext credentials, NTLM hashes, and authentication data directly from the memory of lsass.exe, allowing attackers to harvest valuable credentials while remaining largely stealthy. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Steal data | Windows |
| Credential Harvester | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| CL-STA-1087 | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| LeakNet | LeakNet, a ransomware group identified in November 2024, has shifted to a scalable ClickFix social engineering technique, tricking users on compromised websites into executing malicious commands themselves. Once triggered, it deploys a second-stage loader using the legitimate Deno runtime, allowing the attack to blend in with normal activity. The payload runs as encoded, in-memory scripts rather than traditional files, making detection and analysis significantly more difficult. | Social Engineering | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Encrypt Data, Data theft | Windows |
| Ransomware | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Deno | The Deno runtime loader executes a Base64-encoded payload almost entirely in memory, minimizing disk artifacts while evading detection. It fingerprints the infected system and establishes communication with a command-and-control (C2) server to receive further instructions. By leveraging Deno, a legitimate JavaScript/TypeScript runtime like Node.js, the malware blends into normal activity while efficiently running its payload in memory. | Social Engineering | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Loads payloads | Windows |
| Loader | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| EndRAT | EndRAT is a lightweight remote access trojan developed in AutoIt that, despite its simplicity, delivers a full range of RAT capabilities. It enables attackers to manage files, execute commands through a remote shell, transfer data, and maintain persistence on infected systems, making it an effective tool for sustained unauthorized access. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | System Compromise | Windows |
| RAT | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| Konni | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| RftRAT | RftRAT is a Remote Access Trojan designed to give attackers full control over compromised systems, enabling data theft and covert surveillance. It is built using AutoIt, a Windows automation scripting language, which helps the malware blend in with legitimate activity and evade detection by security tools while maintaining persistent access. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | System Compromise | Windows |
| RAT | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| Konni | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| RemcosRAT | Remcos, is often employed by attackers to gain complete control over systems. It operates stealthily, elevates privileges, and persists through reboots. Common methods of delivery include phishing emails, exploit kits, and watering hole attacks. | Phishing | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Information Theft, Espionage | Windows |
| RAT | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| Konni | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Vidar Stealer 2.0 | Vidar 2.0 is a stealthy information stealer that extracts browser data, credentials, crypto wallets, and tokens, often monetized by attackers. Rewritten in C with polymorphic and multithreaded capabilities, it evades detection using obfuscation and anti-analysis techniques. Its C2 communication leverages Telegram bots and Steam profiles, allowing it to operate quickly and quietly, often exfiltrating data before detection. | Fake game cheat repositories | - |
| | | **IMPACT** | **AFFECTED PLATFORM** |
| **TYPE** | | Data theft, Steal Data | Windows |
| Stealer | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | - |
| - | | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Interlock Ransomware Group | INTERLOCK is a ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. The group employs refined double-extortion tactics and runs a leak site called “Worldwide Secrets Blog” to publish stolen data and pressure victims into negotiations. | Exploiting Vulnerability | CVE-2026-20131 |
| | | **IMPACT** | **AFFECTED PRODUCTS** |
| **TYPE** | | Information Theft, Financial Loss | Cisco Secure Firewall Management Center (FMC) Software, Cisco Security Cloud Control (SCC) Firewall Management |
| Ransomware | | | **PATCH LINK** |
| **ASSOCIATED ACTOR** | | | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh |
| Hive0163 | | | |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Rhadamanthys | Rhadamanthys is information-stealing malware distributed through large-scale phishing campaigns. It is designed to exfiltrate sensitive data from infected systems, including credentials and financial information. Targeting various sectors globally has been observed, often masquerading as legitimate communications to deceive victims. | Phishing | CVE-2019-0604 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Infostealer | | Data theft | Microsoft SharePoint |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Void Manticore | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Hatef | The Windows wiper, "Hatef," begins by identifying its own process and ensuring only a single instance is running through checks on process name, session ID, and execution path. It then verifies whether it has Administrator privileges; if not, it displays a deceptive prompt posing as a legitimate updater to trick the user into granting elevated access. This combination of execution control and social engineering helps the malware secure the permissions needed to carry out its destructive actions. | Phishing | CVE-2019-0604 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Wiper | | Wipes data | Microsoft SharePoint |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Void Manticore | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Hamsa | Hamsa is a destructive wiper designed to erase data while concealing its intent through layered obfuscation. The payload is embedded within a script that uses five successive Base64 encoding stages and is ultimately executed via the 'eval' command, allowing it to evade straightforward analysis. Once decoded, it reveals a Bash-based routine engineered to wipe system data. The name "Hamsa" reflects this technique, derived from the Arabic word for "five," referencing the multiple encoding layers used to hide its core functionality. | Phishing | CVE-2019-0604 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Wiper | | Wipes data | Microsoft SharePoint |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Void Manticore | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Handala | Handala Wiper is a custom destructive malware deployed via Group Policy logon scripts as handala.bat, enabling it to execute remotely from the Domain Controller without being written to disk on target systems. It is designed to overwrite files across the system and corrupt the Master Boot Record (MBR), leading to severe, low-level data destruction and system inoperability. The wiper also leverages the Telegram Bot API for command-and-control communication, helping operators manage attacks while maintaining a level of stealth. | Phishing | CVE-2019-0604 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Wiper | | Wipes data | Microsoft SharePoint |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Void Manticore | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Handala PowerShell | Handala PowerShell Wiper is an AI-assisted destructive script delivered alongside the main Handala Wiper via Group Policy logon scripts. It systematically enumerates and deletes files across user directories, ensuring widespread data loss. In its final stage, it floods all logical drives with a propaganda image named handala.gif, leaving a visible signature of the attack. The script's structured logic and detailed comments strongly suggest it was developed with AI assistance. | Phishing | CVE-2019-0604 |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Wiper | | Wipes data | Microsoft SharePoint |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| Void Manticore | | | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Dindoor | A novel backdoor by MuddyWater that leverages the Deno JavaScript runtime for execution. It communicates with C2 over HTTPS and blends into legitimate traffic for long-term persistent access. Signed with a certificate issued to "Amy Cherne". | Spear-phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Backdoor | | Remote access, Data exfiltration | Windows, Linux |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| MuddyWater | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Fakeset | A Python-based backdoor deployed by MuddyWater alongside Dindoor. Hosted on Backblaze cloud storage and signed with certificates linked to prior Seedworm operations, enabling remote access to compromised networks. | Cloud-hosted payload | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote access, Persistent foothold | Windows, Linux |
| Backdoor | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Stagecomp | A downloader/stager linked to MuddyWater that retrieves and deploys the Darkcomp backdoor onto victim systems. Shares digital certificates with other Seedworm malware families including Fakeset. | Signed binary | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Payload staging, Backdoor deployment | Windows, Linux |
| Downloader | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Darkcomp | A backdoor dropped by Stagecomp, attributed to MuddyWater by Google, Microsoft, and Kaspersky. Provides persistent remote access and command execution on compromised Windows hosts. | Dropped by Stagecomp | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote access, Command execution | Windows, Linux |
| Backdoor | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| LampoRAT | A Rust-based RAT by Boggy Serpens (MuddyWater) that uses the Telegram Bot API for C2 communication. Masquerades as Kaspersky's avp.exe and supports shell command execution. Shows indicators of AI-assisted development. | Spear-phishing | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote access, Reconnaissance | Windows, Linux |
| RAT | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| UDPGangster | A custom backdoor by Boggy Serpens using a UDP-based C2 protocol to execute commands and exfiltrate data. Employs multiple anti-analysis techniques and is delivered via VBA macro-embedded Office documents. | Macro-laced Office documents | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Backdoor | | Command execution, Data exfiltration | Windows, Linux |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| MuddyWater | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| BlackBeard | A Rust-based backdoor by Boggy Serpens delivered via a C++ injector using process hollowing. Communicates over HTTPS with AES-256-GCM encryption and uses HTTP status codes for commands. Achieves persistence via custom file association. | Macro documents, process hollowing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Backdoor | | Persistent access, Defense evasion | Windows, Linux |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| MuddyWater | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Nuso | A custom HTTP backdoor by Boggy Serpens that uses HTTP status codes as command triggers (e.g., 201 for shell, 418 for exit). Exfiltrates system info via bit-rotated custom HTTP headers for evasive C2 communication. | Macro-laced Excel documents | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote access, Reconnaissance | Windows, Linux |
| Backdoor | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Phoenix | An evolving backdoor family by Boggy Serpens with multiple versions (v3, v4/Mononoke). Delivered via a mature VBA builder pipeline featuring brute-force stalling, property-based payload encapsulation, and WMI-based lateral execution. | Macro-laced Office documents | - |
| | | IMPACT | AFFECTED PRODUCT |
| TYPE | | Remote access, Lateral movement | Windows, Linux |
| Backdoor | | | |
| ASSOCIATED ACTOR | | | PATCH LINK |
| MuddyWater | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| CanisterWorm | A self-propagating npm supply chain worm by TeamPCP that steals npm tokens to republish infected packages. Uses an ICP blockchain canister as a decentralized C2 dead drop. Deploys a Kamikaze wiper on Iranian Kubernetes targets. | npm supply chain compromise | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Worm | | Credential theft, Data destruction | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| TeamPCP | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Beast Ransomware | A RaaS platform evolved from Monster ransomware, targeting Windows, Linux, and ESXi. Uses hybrid ECC + ChaCha20 encryption and self-propagates via SMB scanning. Performs double extortion through its BEAST LEAKS site. | Phishing, compromised RDP | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCT** |
| Ransomware | | File encryption, Data exfiltration | Windows, Linux, VMware ESXi, Network Attached Storage (NAS) |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

# Adversaries in Action

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
| APT37 (aka ScarCruft, Reaper, TEMP.Reaper, Ricochet Chollima, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt) | North Korea | All | Worldwide |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | RESTLEAF, SNAKEDROPPER, THUMBSBD, VIRUSTASK, FOOTWINE, and BLUELIGHT | - |

**TTPs**

TA001: Initial Access; TA002: Execution; TA003: Persistence; TA005: Defense Evasion; TA007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA009: Collection: T1566: Phishing; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1055: Process Injection; T1620: Reflective Code Loading; T1036: Masquerading; T1036.005: Match Legitimate T1036.005: Match Legitimate Name or Location; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1132: Data Encoding; T1132.002: Non-Standard Encoding; T1092: Communication Through Removable Media; T1052: Exfiltration Over Physical Medium; T1052.001: Exfiltration over USB; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1123: Audio Capture; T1125: Video Capture

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  Dust Specter | Iran | Government | Iraq |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | SPLITDROP, TWINTASK, TWINTALK, GHOSTFORM | - |

| TTPs |
|---|
| TA0042: Resource Development; TA001: Initial Access; TA002: Execution; TA003: Persistence; TA005: Defense Evasion; TA007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1587: Develop Capabilities; T1587.001: Malware; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL Side-Loading; T1112: Modify Registry; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1205: Traffic Signaling; T1036: Masquerading; T1036.001: Invalid Code Signature; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1001: Data Obfuscation; T1001.003: Protocol or Service Impersonation; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)</td><td>China</td><td rowspan="2">Government, Defense</td><td rowspan="2">Middle East</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>LOTUSLITE</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1566: Phishing, T1566.001: Spearphishing Attachment, TA0002: Execution, T1204: User Execution, T1204.002: Malicious File, TA0003: Persistence, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1574.001: DLL, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, TA0007: Discovery, T1057: Process Discovery, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1105: Ingress Tool Transfer, TA0042: Resource Development, T1584: Compromise Infrastructure, T1584.004: Server, T1588: Obtain Capabilities, T1588.002: Tool</td></tr>
</table>

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  Void Manticore (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Handala Hack) | Iran | Government agencies and services, Critical infrastructure, Oil & Gas, Energy, Telecommunications, Defense, NGOs, Media, Think Tanks, IT and Service Providers, Education, Transportation, Airlines, Maritime and Healthcare | Israel, United States, Albania, Jordan, Gulf States |
| | **MOTIVE** | | |
| | Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | CVE-2019-0604 | BiBi Wiper, Cl Wiper, No-Justice Wiper, Handala Wiper, Handala PowerShell Wiper, Rhadamanthys, Hatef Wiper, Hamsa Wiper | Windows Microsoft SharePoint and Linux |

| TTPs |
|---|
| TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1566: Phishing, TA0002: Execution, T1059: Command and Scripting Interpreter, T1204: User Execution, T1204.002: Malicious File, T1047: Windows Management Instrumentation, TA0003: Persistence, T1505: Server Software Component, T1505.003: Web Shell, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys, T1053: Scheduled Task/Job, TA0004: Privilege Escalation, T1078: Valid Accounts, T1078.002: Domain Accounts, T1068: Exploitation for Privilege Escalation, TA0005: Defense Evasion, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1036: Masquerading, T1140: Deobfuscate/Decode Files or Information, T1070: Indicator Removal, TA0006: Credential Access, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1555: Credentials from Password Stores, TA0007: Discovery, T1087: Account Discovery, T1087.002: Domain Account, T1082: System Information Discovery, T1018: Remote System Discovery, T1069: Permission Groups Discovery, T1069.002: Domain Groups, T1016: System Network Configuration Discovery, TA0008: Lateral Movement, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1572: Protocol Tunneling Collection, T1114: Email Collection, T1005: Data from Local System, T1039: Data from Network Shared Drive, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1090: Proxy, T1105: Ingress Tool Transfer, T1572: Protocol Tunneling, TA0010: Exfiltration, T1041: Exfiltration Over C2 Channel, T1567: Exfiltration Over Web Service, TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.006: Web Services, T1587: Develop Capabilities, T1587.001: Malware,T1586: Compromise Accounts, T1585: Establish Accounts, T1585.001: Social Media Accounts, TA0040: Impact, T1485: Data Destruction, T1561: Disk Wipe, T1561.001: Disk Content Wipe, T1561.002: Disk Structure Wipe, T1486: Data Encrypted for Impact, T1491: Defacement, T1491.002: External Defacement, T1489: Service Stop, T1529: System Shutdown/Reboot, T1531: Account Access Removal, TA0043: Reconnaissance, T1590: Gather Victim Network Information, T1589: Gather Victim Identity Information, T1589.001: Credentials |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGION |
|---|---|---|---|
|  APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110) | Russia | Government, Military | Ukraine |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | CVE-2026-21509 | SlimAgent, BeardShell, Covenant | Microsoft Office |

| TTPs |
|---|
| TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.006: Web Services, T1587: Develop Capabilities, T1587.001: Malware, TA0001: Initial Access, T1566: Phishing, T1566.001: Spearphishing Attachment, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1129: Shared Modules, TA0003: Persistence, T1546: Event Triggered Execution, T1546.015: Component Object Model Hijacking, TA0005: Defense Evasion, T1211: Exploitation for Defense Evasion, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1480: Execution Guardrails, T1564: Hide Artifacts, TA0009: Collection, T1056: Input Capture, T1056.001: Keylogging, T1113: Screen Capture, T1115: Clipboard Data, T1005: Data from Local System, TA0007: Discovery, T1082: System Information Discovery, TA0011: Command and Control, T1102: Web Service, T1102.002: Bidirectional Communication, T1573: Encrypted Channel, T1573.002: Asymmetric Cryptography, T1001: Data Obfuscation, T1071: Application Layer Protocol, T1071.001: Web Protocols, TA0010: Exfiltration T1567: Exfiltration Over Web Service, T1567.002: Exfiltration to Cloud Storage |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>Hive0163</td><td>-</td><td rowspan="2">Corporate Enterprises</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial gains</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Slopoly, NodeSnake, Interlock ransomware, InterlockRAT</td><td>Windows, Linux</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution, T1204: User Execution, T1204.004: Malicious Copy and Paste, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1059.007: JavaScript, TA0003: Persistence, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1574: Hijack Execution Flow, T1574.001: DLL, TA0007: Discovery, T1016: System Network Configuration Discovery, T1082: System Information Discovery, T1046: Network Service Discovery, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1572: Protocol Tunneling, T1090: Proxy, T1090.001: Internal Proxy, T1102: Web Service, TA0010: Exfiltration, T1567: Exfiltration Over Web Service, TA0040: Impact, T1486: Data Encrypted for Impact, T1489: Service Stop</td></tr>
</table>

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
| UNK_InnerAmbush | China | Government, Diplomatic Organizations, Think Tanks | Middle East, Europe, United States, India |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | - | - |

| TTPs |
|---|
| T1586: Compromise Accounts; T1586.002: Email Accounts; T1583: Acquire Infrastructur; T1583.001: Domains; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
| TA402 (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5, Frankenstein, Cruel Jackal) | Gaza | Government, Diplomatic Organizations, Think Tanks | Middle East, Europe, United States, India |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | - | - |

| TTPs |
|---|
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  UNK_RobotDreams | Pakistan | Government, Diplomatic Organizations, Think Tanks | Middle East, Europe, United States, India |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | - | - |

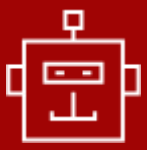
| TTPs |
|---|
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>UNK_NightOwl</td><td>-</td><td rowspan="2">Government, Diplomatic Organizations, Think Tanks</td><td rowspan="2">Middle East, Europe, United States, India</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>TA473 (aka Winter Vivern, UAC-0114, UNC4907, TAG-70)</td><td>-</td><td rowspan="2">Government, Diplomatic Organizations, Think Tanks</td><td rowspan="2">Middle East, Europe, United States, India</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link</td></tr>
</table>

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  TA453 (aka Charming Kitten, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress) | Iran | Government, Diplomatic Organizations, Think Tanks | Middle East, Europe, United States, India |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | - | - |

| TTPs |
|---|
| TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>CL-STA-1087</td><td>China</td><td rowspan="3">Military, Defense</td><td rowspan="3">Southeast Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>AppleChris, MemFun, Getpass</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0043: Reconnaissance; T1586: Compromise Accounts T1586.002: Email Accounts; T1583: Acquire Infrastructure T1583.001: Domains; T1585: Establish Accounts T1585.001: Social Media Accounts; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1574.001: DLL Search Order Hijacking; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Evasion; T1056: Input Capture; T1056.003: Web Portal Capture; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1090: Proxy; T1090.001: Internal Proxy; T1021: Remote Services; T1041: Exfiltration Over C2 Channel; T1598: Phishing for Information; T1598.003: Spearphishing Link</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>Konni</td><td>North Korea</td><td rowspan="3">Human Rights Organizations</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>EndRAT, RftRAT, RemcosRAT</td><td>KakaoTalk PC Application</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.010: AutoHotKey & AutoIt; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1036: Masquerading; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1070: Indicator Removal; T1070.004: File Deletion; T1082: System Information Discovery; T1083: File and Directory Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>MuddyWater (aka Earth Vetala, Mango Sandstorm, MUDDYCOAST, Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Boggy Serpens, Yellow Nix)</td><td>Iran</td><td rowspan="3">Aviation, Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Shipping and Logistics, Telecommunications, Transportation, Software/Technology, Critical Infrastructure</td><td rowspan="3">Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Portugal, Qatar, Russia, Saudi Arabia, Sudan, Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA, Canada, North Africa</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Cyber Espionage, Intelligence Collection, Pre-positioning for Potential Destructive Operations</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-1731<br>CVE-2026-1281</td><td>Dindoor, Fakeset, Stagecomp, Darkcomp, LampoRAT, UDPGangster, BlackBeard, Nuso, Phoenix</td><td>Windows, Linux</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1566: Phishing; T1566.001: Spear-Phishing Attachment; T1190: Exploit Public-Facing Application Execution; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.006: Python; T1059.001: PowerShell; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1219: Remote Access Software; T1027: Obfuscated Files or Information; T1553: Subvert Trust Controls ; T1553.002: Code Signing; T1110: Brute Force ; T1110.003: Password Spraying Discovery ; T1082: System Information Discovery; T1021: Remote Services; T1115: Clipboard Data; T1071: Application Layer Protocol ; T1071.001: Web Protocols; T1102: Web Service; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1588: Obtain Capabilities ; T1588.006: Vulnerabilities</td></tr>
</table>

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  Prince of Persia (alias Infy, Operation Mermaid, APT-C-07) | Iran | Government, NGOs, Human Rights Organizations, Media/Journalism, Energy, Marine Services, Telecommunications, Critical Infrastructure | Global |
| | **MOTIVE** | | |
| | Information theft and Espionage | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | - | Windows |
| **TTPs** | | | |
| T1589: Gather Victim Identity Information, T1598: Phishing for Information, T1583: Acquire Infrastructure, T1587: Develop Capabilities , T1587.001: Malware, T1585: Establish Accounts, T1585.001: Social Media Accounts, T1566: Phishing , T1566.003: Spearphishing via Service, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter , T1059.001: PowerShell, T1547: Boot or Logon Autostart, T1547.001: Registry Run Keys /Startup Folder, T1036: Masquerading , T1036.005: Match Legitimate Name or Location, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1113: Screen Capture, T1123: Audio Capture, T1005: Data from Local System, T1560: Archive Collected Data , T1560.001: Archive via Utility, T1567: Exfiltration Over Web Service, T1041: Exfiltration Over C2 Channel, T1102: Web Service, T1071: Application Layer Protocol , T1071.001: Web Protocols | | |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">  <br>TeamPCP</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide (Primary focus on Iran)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Sabotage, Disruption, Financial Gains</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>CanisterWorm</td><td>Docker APIs, Kubernetes clusters, and CI/CD pipelines</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1195.001: Compromise Software Dependencies and Development Tools; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1059.006: Python; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1053: Scheduled Task/Job; T1611: Escape to Host; T1027: Obfuscated Files or Information; T1027.001: Binary Padding; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion ; T1497.003: Time Based Evasion; T1528: Steal Application Access Token; T1552: Unsecured Credentials; T1552.005: Cloud Instance Metadata; T1552.004: Private Keys; T1003: OS Credential Dumping; T1082: System Information Discovery; T1083: File and Directory Discovery; T1021: Remote Services; T1021.004: SSH; T1610: Deploy Container; T1560: Archive Collected Data ; T1560.001: Archive via Utility; T1102: Web Service ; T1102.001: Dead Drop Resolver; T1572: Protocol Tunnelling; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1485: Data Destruction; T1496: Resource Hijacking</td></tr>
</table>

# MITRE ATT&CK TTPS

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0001: Initial Access | T1078: Valid Accounts | T1078.001: Default Accounts |
| | | T1078.002: Domain Accounts |
| | | T1078.003: Local Accounts |
| | T1133: External Remote Services | |
| | T1189: Drive-by Compromise | |
| | T1190: Exploit Public-Facing Application | |
| | T1195: Supply Chain Compromise | T1195.001: Compromise Software Dependencies and Development Tools |
| | | T1195.002: Compromise Software Supply Chain |
| | T1199: Trusted Relationship | |
| | T1566: Phishing | T1566.001: Spearphishing Attachment |
| | | T1566.002: Spearphishing Link |
| | | T1566.003: Spearphishing via Service |
| TA0002: Execution | T1047: Windows Management Instrumentation | |
| | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.003: Windows Command Shell |
| | | T1059.004: Unix Shell |
| | | T1059.005: Visual Basic |
| | | T1059.006: Python |
| | | T1059.007: JavaScript |
| | T1106: Native API | |
| | T1129: Shared Modules | |
| | T1203: Exploitation for Client Execution | |
| | T1204: User Execution | T1204.001: Malicious Link |
| | | T1204.002: Malicious File |
| | T1569: System Services | T1569.002: Service Execution |
| | T1610: Deploy Container | |
| TA0003: Persistence | T1037: Boot or Logon Initialization Scripts | T1037.003: Network Logon Script |
| | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| | T1078: Valid Accounts | T1078.001: Default Accounts |
| | | T1078.002: Domain Accounts |
| | | T1078.003: Local Accounts |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0003: Persistence | T1098: Account Manipulation | |
| | T1133: External Remote Services | |
| | T1205: Traffic Signaling | |
| | T1505: Server Software Component | T1505.003: Web Shell |
| | T1543: Create or Modify System Process | T1543.002: Systemd Service |
| | | T1543.003: Windows Service |
| | T1546: Event Triggered Execution | T1546.004: Unix Shell Configuration Modification |
| | | T1546.015: Component Object Model Hijacking |
| | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | T1574: Hijack Execution Flow | T1574.001: DLL Search Order Hijacking |
| | | T1574.002: DLL Side-Loading |
| | | T1136.002: Domain Account |
| TA0004: Privilege Escalation | T1037: Boot or Logon Initialization Scripts | T1037.003: Network Logon Script |
| | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| | T1055: Process Injection | T1055.001: Dynamic-link Library Injection |
| | | T1055.012: Process Hollowing |
| | T1068: Exploitation for Privilege Escalation | |
| | T1078: Valid Accounts | T1078.001: Default Accounts |
| | | T1078.002: Domain Accounts |
| | | T1078.003: Local Accounts |
| | T1098: Account Manipulation | T1098.001 : Additional Cloud Credentials |
| | T1134: Access Token Manipulation | T1134.001: Token Impersonation/Theft |
| | T1484: Domain or Tenant Policy Modification | T1484.001: Group Policy Modification |
| | T1543: Create or Modify System Process | T1543.002: Systemd Service |
| | | T1543.003: Windows Service |
| | T1546: Event Triggered Execution | T1546.004: Unix Shell Configuration Modification |
| | | T1546.015: Component Object Model Hijacking |
| | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | T1548: Abuse Elevation Control Mechanism | T1548.002: Bypass User Account Control |
| | T1574: Hijack Execution Flow | T1574.001: DLL Search Order Hijacking |
| | | T1574.002: DLL Side-Loading |
| | T1611: Escape to Host | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0005: Defense Evasion | T1027: Obfuscated Files or Information | T1027.001: Binary Padding |
| | | T1027.002: Software Packing |
| | | T1027.009: Embedded Payloads |
| | | T1027.013: Encrypted/Encoded File |
| | T1036: Masquerading | T1036.001: Invalid Code Signature |
| | | T1036.004: Masquerade Task or Service |
| | | T1036.005: Match Legitimate Name or Location |
| | T1055: Process Injection | T1055.001: Dynamic-link Library Injection |
| | | T1055.012: Process Hollowing |
| | T1070: Indicator Removal | T1070.002: Clear Linux or Mac System Logs |
| | | T1070.004: File Deletion |
| | | T1070.006: Timestomp |
| | T1078: Valid Accounts | T1078.001: Default Accounts |
| | | T1078.002: Domain Accounts |
| | | T1078.003: Local Accounts |
| | T1112: Modify Registry | |
| | T1134: Access Token Manipulation | T1134.001: Token Impersonation/Theft |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1205: Traffic Signaling | |
| | T1211: Exploitation for Defense Evasion | |
| | T1218: System Binary Proxy Execution | T1218.007: Msiexec |
| | | T1218.009: Regsvcs/Regasm |
| | T1480: Execution Guardrails | T1480.001: Environmental Keying |
| | T1484: Domain or Tenant Policy Modification | T1484.001: Group Policy Modification |
| | T1497: Virtualization/Sandbox Evasion | T1497.003: Time Based Evasion |
| | T1548: Abuse Elevation Control Mechanism | T1548.002: Bypass User Account Control |
| | T1553: Subvert Trust Controls | T1553.002: Code Signing |
| | | T1553.005: Mark-of-the-Web Bypass |
| | T1562: Impair Defenses | T1562.001: Disable or Modify Tools |
| | | T1562.004: Disable or Modify System Firewall |
| | T1564: Hide Artifacts | T1564.001: Hidden Files and Directories |
| | T1574: Hijack Execution Flow | T1574.001: DLL Search Order Hijacking |
| | | T1574.002: DLL Side-Loading |
| | T1610: Deploy Container | |
| | T1620: Reflective Code Loading | |
| | T1622: Debugger Evasion | |
| | T1656: Impersonation | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0006: Credential Access | T1003: OS Credential Dumping | T1003.001: LSASS Memory |
| | | T1003.002: Security Account Manager |
| | | T1003.005: Cached Domain Credentials |
| | T1056: Input Capture | T1056.001: Keylogging |
| | | T1056.003: Web Portal Capture |
| | T1110: Brute Force | T1110.003: Password Spraying |
| | T1111: Multi-Factor Authentication Interception | |
| | T1528: Steal Application Access Token | |
| | T1539: Steal Web Session Cookie | |
| | T1552: Unsecured Credentials | T1552.001: Credentials In Files |
| | | T1552.004: Private Keys |
| | | T1552.005: Cloud Instance Metadata API |
| | T1555: Credentials from Password Stores | T1555.003: Credentials from Web Browsers |
| | T1558: Steal or Forge Kerberos Tickets | T1558.003: Kerberoasting |
| | T1649: Steal or Forge Authentication Certificates | |
| TA0007: Discovery | T1016: System Network Configuration Discovery | |
| | T1018: Remote System Discovery | |
| | T1033: System Owner/User Discovery | |
| | T1046: Network Service Discovery | |
| | T1049: System Network Connections Discovery | |
| | T1057: Process Discovery | |
| | T1069: Permission Groups Discovery | T1069.002: Domain Groups |
| | T1082: System Information Discovery | |
| | T1083: File and Directory Discovery | |
| | T1087: Account Discovery | T1087.003: Email Account |
| | T1120: Peripheral Device Discovery | |
| | T1135: Network Share Discovery | |
| | T1497: Virtualization/Sandbox Evasion | T1497.003: Time Based Evasion |
| | T1622: Debugger Evasion | |
| TA0008: Lateral Movement | T1021: Remote Services | T1021.001: Remote Desktop Protocol |
| | | T1021.002: SMB/Windows Admin Shares |
| | | T1021.004: SSH |
| TA0009: Collection | T1005: Data from Local System | |
| | T1039: Data from Network Shared Drive | |
| | T1056: Input Capture | T1056.001: Keylogging |
| | | T1056.003: Web Portal Capture |
| | T1113: Screen Capture | |
| | T1114: Email Collection | T1114.002: Remote Email Collection |
| | T1115: Clipboard Data | |
| | T1119: Automated Collection | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0009: Collection | T1123: Audio Capture | |
| | T1125: Video Capture | |
| | T1185: Browser Session Hijacking | |
| | T1213: Data from Information Repositories | |
| | T1560: Archive Collected Data | T1560.001: Archive via Utility |
| TA0010: Exfiltration | T1041: Exfiltration Over C2 Channel | |
| | T1048: Exfiltration Over Alternative Protocol | T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol |
| | T1052: Exfiltration Over Physical Medium | T1052.001: Exfiltration over USB |
| | T1567: Exfiltration Over Web Service | T1567.002: Exfiltration to Cloud Storage |
| TA0011: Command and Control | T1001: Data Obfuscation | |
| | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | | T1071.004: DNS |
| | T1090: Proxy | T1090.001: Internal Proxy |
| | | T1090.002: External Proxy |
| | | T1090.003: Multi-hop Proxy |
| | T1092: Communication Through Removable Media | |
| | T1102: Web Service | T1102.001: Dead Drop Resolver |
| | | T1102.002: Bidirectional Communication |
| | T1105: Ingress Tool Transfer | |
| | T1132: Data Encoding | T1132.001: Standard Encoding |
| | | T1132.002: Non-Standard Encoding |
| | T1205: Traffic Signaling | |
| | T1219: Remote Access Software | |
| | T1568: Dynamic Resolution | |
| | T1572: Protocol Tunneling | |
| | T1573: Encrypted Channel | T1573.001: Symmetric Cryptography |
| | | T1573.002: Asymmetric Cryptography |
| TA0040: Impact | T1485: Data Destruction | |
| | T1486: Data Encrypted for Impact | |
| | T1489: Service Stop | |
| | T1490: Inhibit System Recovery | |
| | T1491: Defacement | T1491.002: External Defacement |
| | T1496: Resource Hijacking | |
| | T1499: Endpoint Denial of Service | T1499.004: Application or System Exploitation |
| | T1529: System Shutdown/Reboot | |
| | T1531: Account Access Removal | |
| | T1561: Disk Wipe | T1561.001: Disk Content Wipe |
| | | T1561.002: Disk Structure Wipe |
| | T1565: Data Manipulation | T1565.001: Stored Data Manipulation |
| | | T1565.002: Transmitted Data Manipulation |
| | T1657: Financial Theft | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0042: Resource Development | T1583: Acquire Infrastructure | T1583.001: Domains |
| | | T1583.003: Virtual Private Server |
| | | T1583.004: Server |
| | | T1583.006: Web Services |
| | T1584: Compromise Infrastructure | |
| | T1585: Establish Accounts | T1585.001: Social Media Accounts |
| | T1586: Compromise Accounts | T1586.001: Social Media Accounts |
| | | T1586.002: Email Accounts |
| | T1587: Develop Capabilities | T1587.001: Malware |
| | T1588: Obtain Capabilities | T1588.001: Malware |
| | | T1588.002: Tool |
| | | T1588.003: Code Signing Certificates |
| | | T1588.005: Exploits |
| | | T1588.006: Vulnerabilities |
| TA0043: Reconnaissance | T1589: Gather Victim Identity Information | T1589.001: Credentials |
| | T1590: Gather Victim Network Information | T1590.002: DNS |
| | | T1590.005: IP Addresses |
| | T1592: Gather Victim Host Information | T1592.001: Hardware |
| | T1595: Active Scanning | T1595.002: Vulnerability Scanning |
| | T1598: Phishing for Information | T1598.002: Spearphishing Attachment |
| | | T1598.003: Spearphishing Link |

# Top 5 Takeaways

**#1** In March 2026, **5 zero-day vulnerabilities** surfaced. These zero-days were found across products from **Google, Hikvision,** and **Cisco.**

**#2** Newly identified malware active in March included a broad mix of **malware**. Key discoveries were **SPLITDROP, TWINTASK, TWINTALK,** and **GHOSTFORM**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

**#3** Cyberattacks concentrated heavily on the **United States, Kuwait, Bahrain, Qatar, Israel, United Arab Emirates**, which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

**#4** **Government, Healthcare, Defense, Financial, Education, and NGOs** sectors absorbed the bulk of targeted activity, with malware operations, data theft, and espionage campaigns driving operational disruption. Attackers continued refining techniques and expanding pressure across these industries.

**#5** Activity during the period was dominated by **Void Manticore, APT28,** and **MuddyWater,** all well-resourced groups known for sustained, high-impact operations. Their campaigns shaped a threat landscape defined by disciplined tradecraft, rapid exploitation cycles, and a clear focus on high-value targets across public and private sectors.

# Recommendations

**Security Teams**

This digest can be used as a guide to help security teams prioritize the **20 significant vulnerabilities** and block the indicators related to the **17 active threat actors, 50 active malware,** and **228 potential MITRE TTPs.**

**Uni5 Users**

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

• Running a scan to discover the assets impacted by the **20 significant vulnerabilities**

• Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

# 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.

**Social engineering:** is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

**Supply chain attack:** Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

**Eavesdropping:** Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

**Glossary:**

**CISA KEV -** Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
**CVE -** Common Vulnerabilities and Exposures
**CPE -** Common Platform Enumeration
**CWE** - Common Weakness Enumeration

# Indicators of Compromise (IOCs)

| Attack Name | TYPE | VALUE |
|---|---|---|
| Dohdoor | SHA256 | 54e18978c6405f56cd59ba55a62291436639f21cf325ae509f0599b15e8f7f53 |
| RESTLEAF | MD5 | ad556f4eb48e7dba6da14444dcce3170 |
| | SHA256 | cf2e3f46b26bae3d11ab6c2957009bc1295b81463dd67989075592e81149c8ec |
| SNAKEDROPPER | MD5 | 098d697f29b94c11b52c51bfe8f9c47d |
| THUMBSBD | Domains | philion[.]store,<br>homeatedke[.]store,<br>hightkdhe[.]store |
| VIRUSTASK | MD5 | 5c6ff601ccc75e76c2fc99808d8cc9a9 |
| FOOTWINE | MD5 | 476bce9b9a387c5f39461d781e7e22b9 |
| | SHA256 | c61c679eec1c1b43bbd01727fdfb6a69b11485931eb8569e6b20ada30bfe84af |
| | IPv4:Port | 144[.]172[.]106[.]66[:]8080 |
| BLUELIGHT | MD5 | 585322a931a49f4e1d78fb0b3f3c6212 |
| | SHA256 | a8b8a92d170029885d4e7763675f10eb172150f8503592677cadedc392edccf4 |
| SPLITDROP | MD5 | 78275f3fc7e209b85bff6a6f99acc68a |
| | SHA1 | fc08f8403849c6233978a363f4cdc58cd7041823 |
| | SHA256 | 6bb0d45799076b3f2d7f602b978a0779868fc72a1188374f6919fbbfba23efce |
| TWINTASK | MD5 | 19ab3fd2800f62a47bf13a4cc4e4c124 |
| | SHA1 | c79c261457def606c3393dde77c82832a5c0ded3 |
| | SHA256 | ad26cd72a83b884a8bc5aaa87309683953e151ebb3fde42eda7bf9a4406e530d |
| TWINTALK | MD5 | 63702bd6422ec2d5678d4487146ea434 |
| | SHA1 | c7dff3a0675f330feb9a7c469f8340369451d122 |
| | SHA256 | f3f2dc31f70a105db161a5e7b463b2215d3cbd64ac0146fd68e39da1c279f7ef |
| GHOSTFORM | MD5 | b19add5ccaa17a1308993e6f3f786b06,<br>7f17fa22feaced1a16d4d39c545cdb16,<br>70a9b537b9b7e1b410576d798e6c5043,<br>a7561eb023bb2c4025defcfe758d8ac2,<br>809139c237c4062baecab43570060d67 |
| | SHA1 | 51a746c85bd486f223130173b7e674379a51b694,<br>369b56a89b2fce2cbdc36f5a23bdec6067242911,<br>cb1760c90fb6c399e0125c7aa793efe37c4ce533,<br>df04e36c106691f9fe88e5798e4ae86438bd4f1d,<br>8735ee29c409b8d101eb3170f011455be41b7a91 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| GHOSTFORM | SHA256 | 69294ad90aeb7f05e501e7191c95beb14e23da5587dd75557c867e2944a57fdc, fa51aff99d86a9f1f65aa0ebbf6ca40411d343cea59370851ab328b97e2164bb, a27d53608ab05b5c7cb86bcf4a273435238beeb7e7efd7845375b2aa765f51e2, eb5b7275c41de8e98d72696eeac9cba3719f334f8e7974e6b8760ece820b1d0c, 3a66ae5942f6feb79cf81ee70451f761253e0e0bde95f0840abdd42a804fad39, 797325b3c8a9356dcace75d93cb5cfb7847d2049c66772d4cc2cee821618cb96 |
| ClipXDaemon | SHA256 | b6bb28160532400eafad532842e4ba9add6d6bbba4f7e7c85e3dbb650369eb00 |
| A0Backdoor | Domain | fsdgh[.]com |
| | SHA256 | 26db06a2319c09918225e59c404448d92fe31262834d70090e941093e6bb650a |
| LOTUSLITE | MD5 | 10fb1122079b5ae8e4147253a937f40f |
| | SHA1 | 7d4e31c8b11be7c970860c4fbc8fe85c70724cb1 |
| | SHA256 | 856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216 |
| BiBi Wiper | SHA256 | 74d8d60e900f931526a911b7157511377c0a298af986d42d373f51aac4f362f6 |
| Cl Wiper | SHA256 | e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0 |
| No-Justice Wiper | SHA256 | 36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f |
| SlimAgent | SHA1 | 5603e99151f8803c13d48d83b8a64d071542f01b |
| | SHA256 | 9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c |
| BeardShell | SHA1 | 6d39f49aa11ce0574d581f10db0f9bae423ce3d5 |
| | SHA256 | 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1 |
| Covenant | SHA256 | 27a331384cfca9a4d2aa45afdc12c7156cfb4da775f1380d4870f06fbb77ccf2, 62d3b82ac3688b1c00adce7cd241de2a50c24caac4ed6b8e46b16da1266457eb, 1b2b83d462493eb63d6655103cf968d396ee7bdf7dd317f8cb5a5eadee6b560f |

| Attack Name | TYPE | VALUE |
|---|---|---|
| VENON | IPv4 | 206[.]0[.]29[.]58,<br>51[.]222[.]75[.]250,<br>51[.]222[.]75[.]248,<br>192[.]99[.]226[.]117,<br>212[.]69[.]5[.]84,<br>34[.]227[.]229[.]85 |
| | SHA256 | c482286a7fdfb64d308c197a4deabcd773b8b62d9e74d1d08fcfd02568d75d72,<br>d61be2b21e135726c547a388ecb47552559e5221894f5005ce35bdb24efc0c26 |
| Slopoly | SHA256 | 0884e5590bdf3763f8529453fbd24ee46a3a460bba4c2da5b0141f5ec6a35675 |
| | Domain | plurfestivalgalaxy[.]com |
| | IPv4 | 94[.]156[.]181[.]89 |
| AppleChris | SHA256 | 9e44a460196cc92fa6c6c8a12d74fb73a55955045733719e3966a7b8ced6c500,<br>5a6ba08efcef32f5f38df544c319d1983adc35f3db64f77fa5b51b44d0e5052c,<br>0e255b4b04f5064ff97da214050da81a823b3d99bce60cdd9ee90d913cc4a952,<br>413daa580db74a38397d09979090b291f916f0bb26a68e7e0b03b4390c1b472f,<br>2ee667c0ddd4aa341adf8d85b54fbb2fce8cc14aa88967a5cb99babb08a10fae |
| MemFun | SHA256 | ad25b40315dad0bda5916854e1925c1514f8f8b94e4ee09a43375cc1e77422ad |
| Getpass | SHA256 | ee4d4b7340b3fa70387050cd139b43ecc65d0cfd9e3c7dcb94562f5c9c91f58f |
| Deno | Domains | okobojirent[.]com,<br>mshealthmetrics[.]com,<br>verify-safeguard[.]top,<br>neremedysoft[.]com,<br>ndibstersoft[.]com,<br>windowallclean[.]com,<br>cnoocim[.]com,<br>delhedghogeggs[.]com,<br>serialmenot[.]com,<br>crahdhduf[.]com,<br>weaplink[.]com |
| | IPv4 | 194[.]31[.]223[.]42,<br>144[.]31[.]2[.]161,<br>87[.]121[.]79[.]6,<br>87[.]121[.]79[.]25,<br>144[.]31[.]54[.]243,<br>144[.]31[.]224[.]98 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| EndRAT | IPv4 | 157[.]180[.]88[.]26 |
| | SHA256 | a10d308d0d3db17f8f87c5a9d0e7ed3791fb20b590b7a323476992107f54e0f6 |
| RftRAT | IPv4 | 96[.]62[.]214[.]5 |
| RemcosRAT | IPv4 | 178[.]16[.]54[.]208 |
| | SHA256 | aa51573f9abcd4a1ec4a61ee7e5811c0279e015ea22bdb787780d67ce7153a57 |
| Vidar Stealer 2.0 | SHA256 | d1258b4c2b9849833651d1e844d1a99a5bc7febbb751548f960e92525afe6c26, bfee57d9e1b68c5c5aa63792b4e67b94f3361749e186531bd01609d9382672f3, 496d15810c25136955dd9aed6d018519380ee431f28c1bca715da59fe1385d12 |
| Interlock Ransomware Group | SHA256 | e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, 28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f |
| Rhadamanthys | SHA256 | aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f |
| Hatef | SHA256 | e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35 |
| Hamsa | URL | hxxp[:]//sjc1[.]vultrobjects[.]com/f5update/update[.]sh |
| | SHA256 | 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad |
| Handala | MD5 | 5986ab04dd6b3d259935249741d3eff2 |
| | SHA256 | 454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8 |
| Handala PowerShell | MD5 | 3cb9dea916432ffb8784ac36d1f2d3cd |

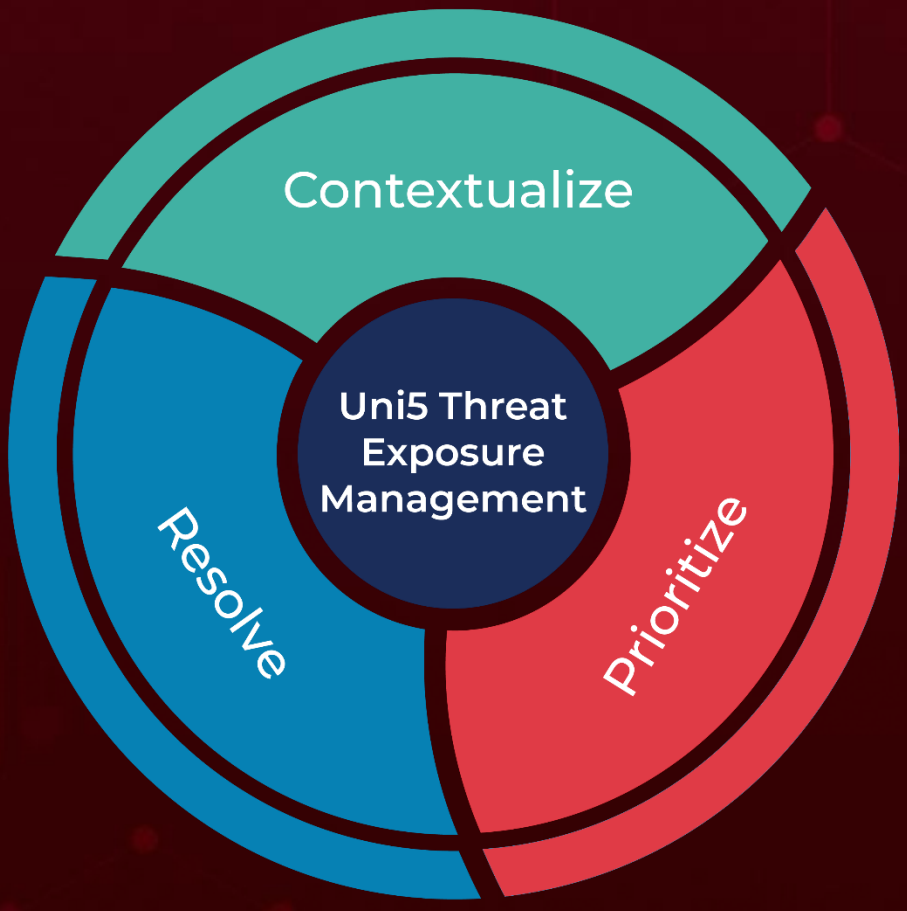
| Attack Name | TYPE | VALUE |
|---|---|---|
| Dindoor | SHA256 | 0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542, 1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1, 2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043, 2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5, 42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f, 7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4, 7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef, b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0, bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a, c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e |
| Fakeset | SHA256 | 077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de, 15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84, |
| Darkcomp | SHA256 | 3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90, 1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6 |
| UDPGangster | PDB Path | C:\Users\piper\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb, C:\Users\gangster\source\repos\udp_3.0 - Copy - Copy\x64\release_86\udp_3.0.pdb, C:\Users\SURGE\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb |
| BlackBeard | IPv4 | 159[.]198[.]68[.]25, 159[.]198[.]66[.]153 |
| | SHA256 | 156b325231742a73ded4104fbde1c55ad3913d2eaf09b5194ef74c81ee3ba393, cc2ec568f978f328b6de112670a1b35ca1f9db377ff32cb9d313a5b2ac3c127b, 7523e53c979692f9eecff6ec760ac3df5b47f172114286e570b6bba3b2133f58, 0be499354dc498248d27f6d186eb3bb75a607ae4a2c0a6734c76f1a1b7b1d316, |

| Attack Name | TYPE | VALUE |
|---|---|---|
| BlackBeard | SHA256 | a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79, 1bcd8d7dc7bed5873bbdd2822e84e19773a33d659b16587ca9dc6db204447a86 |
| Nuso | SHA256 | 1b9e6fe4b03285b2e768c57e320d84323ac9167598395918d56a12e568b0009a, 9c207c51c448f96eaae91241a39c8bb85e2307f2d2a99244763a53176cf4c02f, c91413ad7c94c0e2694862b9d671d1204873bf65576ba2cb91fbd562a4ccf79b |
| | PDB Path | C:\Users\nuso\source\repos\http_vip\http_vip\f*ckAnalyzor.pdb, C:\Users\nuso\source\repos\http_last_ver\http_last_ver\f*ckAnalyser.pdb |
| Phoenix | IPv4 | 46[.]101[.]36[.]39 |
| | SHA256 | 668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839 |
| | PDB Path | C:\Users\win10\Desktop\phonix\phoenix\x64\Release\phoenix.pdb, D:\phonix\phoenixV3\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Debug\phoenix.pdb |
| CanisterWorm | SHA256 | c37c0ae9641d2e5329fcdee847a756bf1140fdb7f0b7c78a40fdc39055e7d926 |
| Beast Ransomware | SHA256 | 6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0, 479d0947816467d562bf6d24b295bf50512176a2d3d955b8f4d932aea2378227, cc0680de960f3e1b727b61a42e59f9c282bd8e41fe20146ed191c7f4bf9283a7, cf5c45be416d1b18dd67ffa95c6434691f1f9ba9c30754fa6fc9978c1f975750, 2ce62601491549ab91c9517e0accf3286ed29976f6ec359d31ddc060a8d99eb3, 812df0efea089b956d08352ff0a7e8789d43862dc3764f4441d4e1c1d1fb7957, 5bd8f9cbd108abc53fb1c44b8d10239a2a0a9dd20c698fd2fb5dc1938ae7ba96 |
| | IPv4 | 5[.]78[.]84[.]144 |

# 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 2, 2026 . 1:30 AM**



More at www.hivepro.com