Date of Publication
December 16, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

09 to 15 DECEMBER 2024

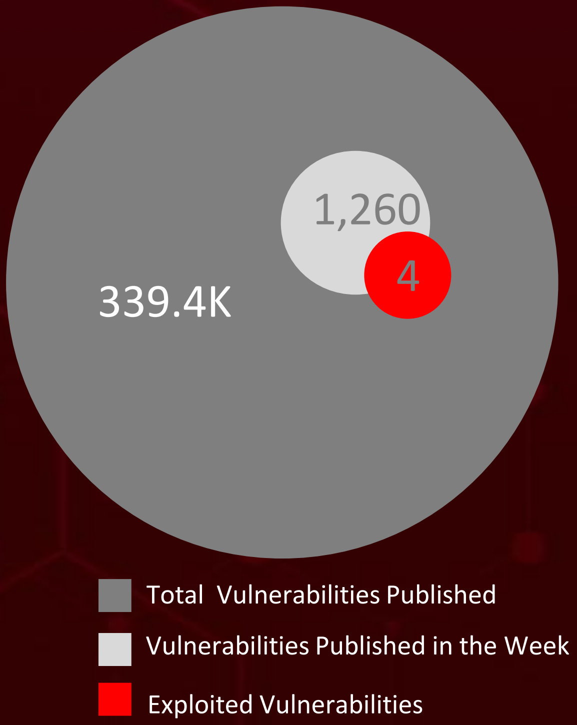
Table Of Contents

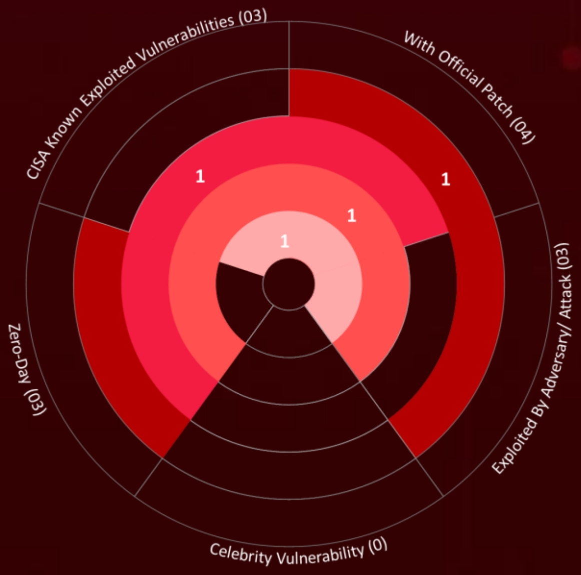
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **thirteen** attacks were executed, **four** vulnerabilities were uncovered, and **one** active adversaries were identified, underscoring the persistent danger of cyberattacks.

HiveForce Labs has uncovered that threat actors are actively exploiting **CVE-2023-46604** in Apache ActiveMQ to achieve remote code execution, install backdoors, deploy **Quasar RAT** and proxy tools, and potentially trigger **Mauri** ransomware to encrypt data. To mitigate this threat, immediate patching and proactive security measures are crucial.

Furthermore, **CVE-2024-50623** and **CVE-2024-55956** critical zero-day vulnerabilities in Cleo's file transfer solutions, are being exploited in the wild. These flaw allows unrestricted file uploads and downloads, leading to remote code execution (RCE) and posing a severe risk to affected organizations. Additionally, **Pumakit**, a sophisticated Linux rootkit, employs advanced stealth techniques and privilege escalation, featuring a multi-layered design with a dropper, executables, and rootkits. These escalating threats represent a significant and urgent risk to global users.





High Level Statistics

13
Attacks Executed

- Termite
- Realst Stealer
- Black Basta
- Zbot
- DarkGate
- Mauri
- Quasar RAT
- TinyTurla
- TwoDash
- Wainscot
- CrimsonRAT
- PUMAKIT
- Cl0p

4
Vulnerabilities Exploited

- CVE-2023-46604
- CVE-2024-50623
- CVE-2024-49138
- CVE-2024-55956

1
Adversaries in Action

- Secret Blizzard

Insights

Secret Blizzard has used tools from at least six other threat actors over seven years, deploying backdoors like TwoDash and TinyTurla

Black Basta’s Evolution now using payloads like Zbot and DarkGate, alongside email bombing to flood victims with subscription notifications, masking malicious actions while maintaining its core objective

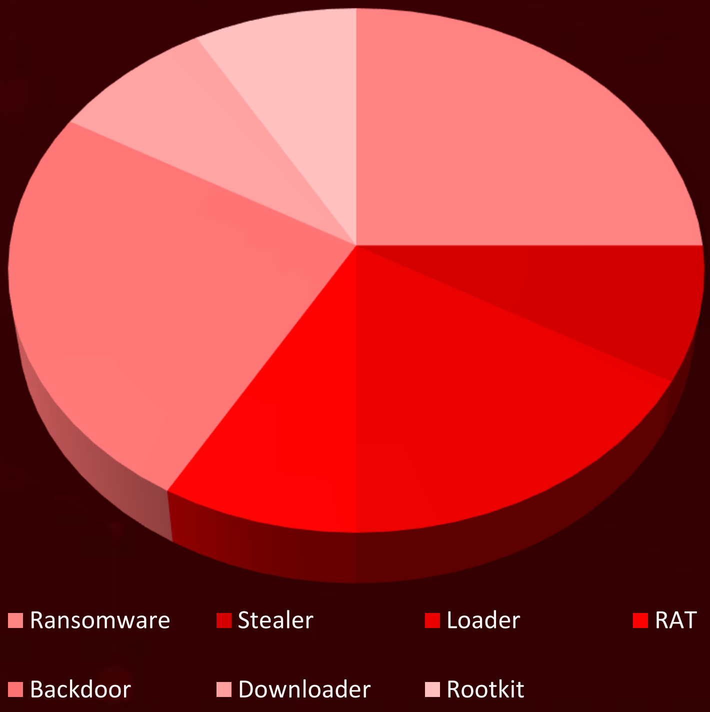
CVE-2023-46604 Exploited by threat actors to gain remote code execution to install backdoors

Cleo’s Zero-Day Flaws exploited by the Cl0p ransomware gang, allow unrestricted file uploads and downloads, potentially enabling remote code execution (RCE)

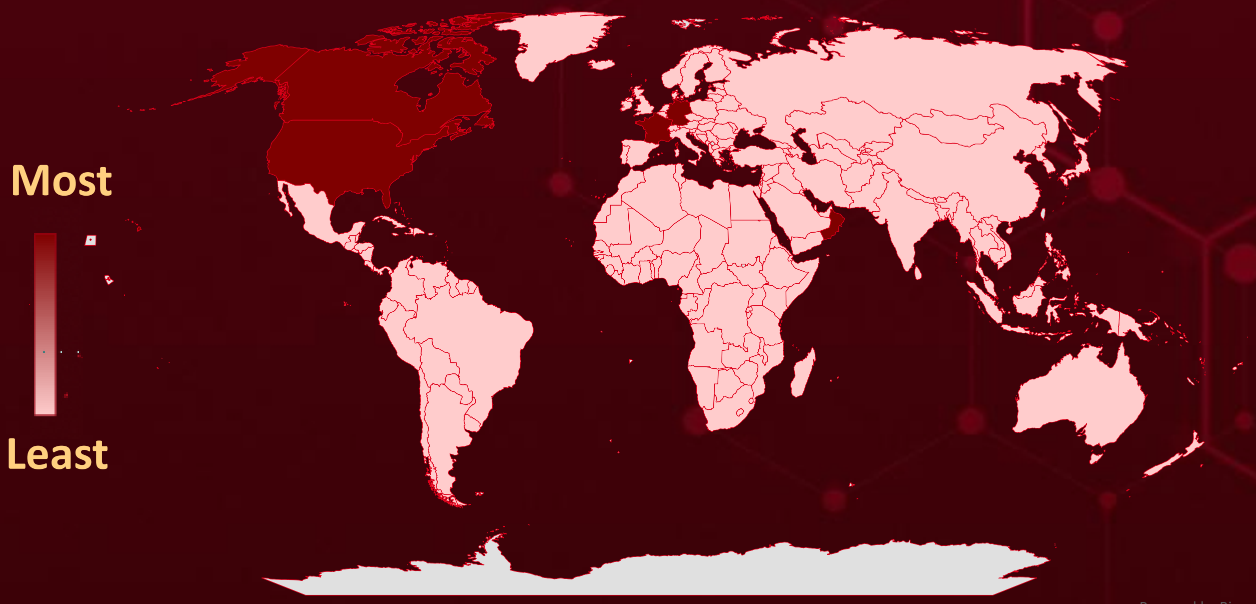
Termite ransomware an advanced offshoot of Babuk, has targeted organizations globally, exfiltrating 680 GB of sensitive data while disrupting operations

PUMAKIT uses advanced stealth and privilege escalation with a multi-layered design, including a dropper, executables, and rootkits

Threat Distribution



Targeted Countries



Powered by Bing

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

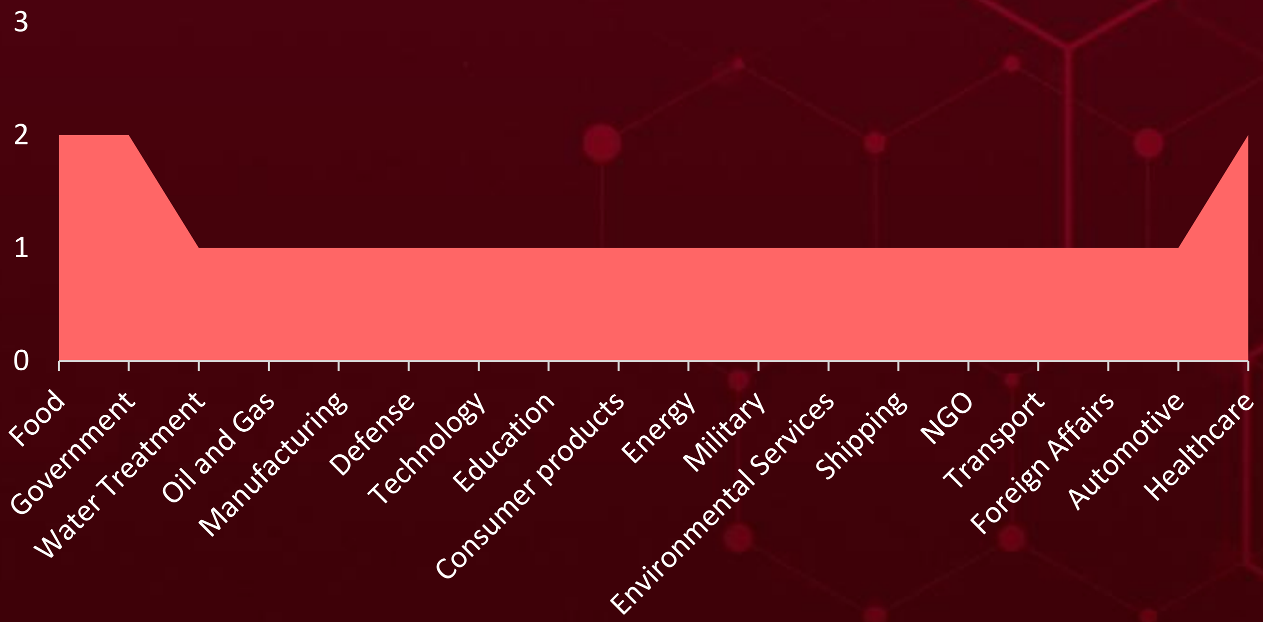
	Countries
■	United States
■	France
■	Oman
■	Canada
■	Germany
□	Angola
□	Liechtenstein
□	Sudan
□	Argentina
□	Mongolia
□	Armenia
□	Senegal
□	Australia
□	Uganda
□	Austria
□	Malta
□	Azerbaijan
□	Netherlands
□	Bahamas
□	Russia
□	Bahrain
□	Somalia

	Countries
□	Bangladesh
□	Timor-Leste
□	Barbados
□	Venezuela
□	Belarus
□	Malawi
□	Belgium
□	Mexico
□	Belize
□	Myanmar
□	Benin
□	Nigeria
□	Bhutan
□	Portugal
□	Bolivia
□	Samoa
□	Bosnia and Herzegovina
□	Singapore
□	Botswana
□	Spain
□	Brazil

	Countries
□	Syria
□	Brunei
□	Tunisia
□	Bulgaria
□	Andorra
□	Burkina Faso
□	Zimbabwe
□	Burundi
□	Luxembourg
□	Cabo Verde
□	Maldives
□	Cambodia
□	Mauritania
□	Cameroon
□	Moldova
□	Albania
□	Morocco
□	Central African Republic
□	Nauru
□	Chad
□	Nicaragua

	Countries
□	India
□	South Africa
□	Indonesia
□	South Sudan
□	Iran
□	Sri Lanka
□	Iraq
□	State of Palestine
□	Ireland
□	Suriname
□	Israel
□	Switzerland
□	Italy
□	Tajikistan
□	Jamaica
□	Thailand
□	Japan
□	Togo
□	Jordan
□	Trinidad and Tobago
□	Kazakhstan

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1070
Indicator Removal

T1588
Obtain Capabilities

T1036
Masquerading

T1082
System Information Discovery

T1041
Exfiltration Over C2 Channel

T1059.001
PowerShell

T1566
Phishing

T1005
Data from Local System

T1033
System Owner/User Discovery

T1068
Exploitation for Privilege Escalation

T1588.006
Vulnerabilities

T1190
Exploit Public-Facing Application

T1498
Network Denial of Service

T1587.001
Malware

T1055
Process Injection

T1587
Develop Capabilities

T1056
Input Capture

T1204
User Execution

T1056.001
Keylogging

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Termite	Termite Ransomware is a variant of the notorious Babuk ransomware, designed to encrypt targeted files on infected systems. Once executed, it appends the .termite extension to affected files, rendering them inaccessible. Victims also find a ransom note titled "How To Restore Your Files.txt", which provides minimal details about the attack.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55
MD5	6b06aae5ec596cdbc1b9d4c457fd5f81
SHA1	a515b7d89676b1401eeb9eb776190a1179c386cf

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Realst	Realst Stealer is a sophisticated infostealer written in Rust, specifically designed to target macOS users. This malware focuses on exfiltrating sensitive information, including stored passwords, browser data, and cryptocurrency wallets. Realst Stealer can extract credentials from the macOS Keychain, harvest data from popular Chromium-based browsers, and compromise widely used cryptocurrency wallets, posing a significant risk to users' digital assets and personal information.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	a0b8789ef3249b5fa8eb3590cd6f183e24273b5886560233025fc9d8de52ce0b, b08740de7bd8d6805ca2c3c8be1db69fbb7aa9bd6aad1c0582881e4196574aa9, fc438c6e231c80c0d5de5b5a194fdba87f88e334414b248047c5e412ed613a6a, 4b93ec3fd49c0111e8a11ac8a0a197f5366cda19732932ce4cb84e024c648a38, 78b2fa0df9fba56ba6a773faa0d280977a1a830fce4f2427935f87de11cb9012

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Black Basta	Black Basta is a ransomware-as-a-service (RaaS) variant that was first identified in April 2022. They employ a double-extortion model, where they not only encrypt the victim's systems but also exfiltrate data. This dual approach increases the pressure on victims to pay the ransom, as they face the threat of data leaks in addition to system inaccessibility.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	a6d653d2887f0ce4029a94616464ad74c4f770fe, 0fbed8d60e2d940882e01a2bf11003f6bd59f883, 22f10e42683501fb2ea6962e44eefd64848aefe7

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Zbot	Zbot is a notorious malware family that primarily targets Microsoft Windows systems to steal financial data. It operates as a financial services Trojan, using sophisticated techniques like website monitoring and keylogging to capture sensitive banking credentials. The malware records keystrokes, bypassing robust security measures. This capability allows Zbot to steal login information directly as users enter it, compromising accounts and financial transactions with ease.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	640640d6651c4ac2f66ed8312084849ad9f0124e, ab1271b4316eb4a5d6ea03b4c24d56cef1e8524a, f09804b59a3aac7c1dd47c7e027182fb54f9a277, f1d299336aac1a1314b36064ffa9ae12ebdb3e4c

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkGate	DarkGate is a powerful and adaptable malware loader equipped with advanced features, making it a popular tool in the cybercrime landscape. Its capabilities include downloading and executing files directly in memory, operating a Hidden Virtual Network Computing (HVNC) module, logging keystrokes, stealing sensitive information, and escalating privileges on compromised systems. DarkGate leverages legitimate AutoIt files to evade detection, often executing multiple AutoIt scripts as part of its operations.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA1	577EFD1534DD2C4133EA2E4B16A21672D257AF72, bccf867716709ce0167cc72f16d4a14f159e459f, 0fdb26c6202acb33eea938da1a492504035ff8c1

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mauri	Mauri ransomware employs AES-256 CTR encryption to lock files, rendering them inaccessible and leaving behind ransom notes. It targets a broad spectrum of file types while deliberately avoiding system-critical paths to maintain operational integrity. In addition to encryption, Mauri ransomware operators use proxy tools like FRP (Fast Reverse Proxy) to expose private network services, such as Remote Desktop Protocol (RDP), to external access.	Exploiting Vulnerability	CVE-2023-46604
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	Apache ActiveMQ
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604

IOC TYPE	VALUE
MD5	07894bc946bd742cec694562e730bac8, 25b1c94cf09076eb8ce590ee2f7f108e, 2c93a213f08a9f31af0c7fc4566a0e56, 2e8a3baeaa0fc85ed787a3c7dfd462e7, 3b56e1881d8708c48150978da14da91e

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Quasar RAT</td><td rowspan="5">Quasar RAT is a remote access trojan (RAT) written in .NET, designed to target Windows devices. Known for being open-source and fully functional, it has become a popular tool among attackers due to its accessibility and flexibility. While its open-source nature allows legitimate use, cybercriminals frequently pack the malware to obfuscate its source code and hinder analysis. Once deployed, Quasar RAT enables attackers to gain unauthorized remote control of infected systems. Its capabilities include spying on victims, stealing sensitive information, and deploying additional malware.</td><td>Exploiting Vulnerabilities</td><td>CVE-2023-46604</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>RAT</td><td rowspan="3">System Compromise, Deploy another malware</td><td>Apache ActiveMQ</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>https://activemq.apache.org/security-advisories.data/CVE-2023-46604</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>IPv4: Port</td><td colspan="3">18[.]139[.]156[.]111:4782</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>TinyTurla</td><td rowspan="5">TinyTurla is a highly covert backdoor that disguises itself as the legitimate Windows Time service (W32Time). By mimicking the behavior of W32Time, the malware avoids detection while carrying out its malicious activities. TinyTurla replicates the service's legitimate functionalities but adds the capability to upload, execute, and exfiltrate files. It can also download additional malware, making it a versatile tool for attackers.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Secret Blizzard</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381,
c039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a</td></tr>
<tr><td>Domains</td><td colspan="3">connectotels[.]net,
hostelhotels[.]net</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TwoDash	TwoDash is a covert malware that combines the characteristics of a trojan and a downloader, enabling it to infiltrate systems undetected. Upon infection, TwoDash collects detailed system information and establishes a connection to a hard-coded command and control (C2) server via port 9443. It proceeds to download and install various programs, including additional malware, onto the compromised device.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Downloads other malware	-
ASSOCIATED ACTOR			**PATCH LINK**
Secret Blizzard			-

IOC TYPE	VALUE
SHA256	dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced, 7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912
IPv4	146[.]70[.]158[.]90, 143[.]198[.]73[.]108, 161[.]35[.]192[.]207

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Wainscot	Wainscot is a backdoor written in Golang, designed to provide attackers with extensive control over compromised systems. Once deployed, it connects to a command-and-control (C2) server and is capable of executing a variety of commands. Key functionalities include launching arbitrary commands, uploading and downloading files, and capturing screenshots from the infected host.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
Secret Blizzard			-

IOC TYPE	VALUE
SHA256	e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273, 08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2
IPv4	130[.]185[.]119[.]198, 176[.]57[.]184[.]97, 173[.]212[.]252[.]2

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CrimsonRAT	Crimson RAT once installed, it allows attackers to remotely control infected systems, steal sensitive, and spy on users. The malware can also lock infected computers, take full control, and demand extortion payments.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
Secret Blizzard			-

IOC TYPE	VALUE
SHA256	aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c
IPv4	45[.]14[.]194[.]253, 37[.]60[.]236[.]186, 5[.]189[.]183[.]63

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PUMAKIT	PUMAKIT is a sophisticated loadable kernel module (LKM) rootkit that uses advanced stealth techniques to hide its presence and communicate with C2 servers. It hooks 18 syscalls and kernel functions through an internal function tracer (ftrace), enabling manipulation of core system behaviors. Key features include privilege escalation via the rmdir() syscall, hiding files and directories, evading detection, and anti-debugging measures. The malware combines a dropper, memory-resident executables, an LKM rootkit, and an SO userland rootkit, activating only under specific conditions.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit, loader		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f, cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe, 8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03
Domains	sec[.]opsecurity1[.]art, rhel[.]opsecurity1[.]art

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Cl0p</td><td rowspan="5">Clop is a type of ransomware that is known for encrypting a victim's files and appending the ".clop“ extension to them. One distinctive feature of Clop ransomware is the string "Dont Worry C|0P“ that is often included in the ransom notes left behind for the victim. Clop is known to attempt to disable Windows Defender and remove Microsoft Security Essentials from the infected system, aiming to evade detection by security software running in the userspace.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-50623
CVE-2024-55956</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt Data</td><td>Cleo Harmony, Cleo VLTrader, Cleo LexiCom</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956 , https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA1</td><td colspan="3">40b7b386c2c6944a6571c6dcfb23aaae026e8e82,
46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5,
4fa2b95b7cde72ff81554cfbddc31bbf77530d4d,
77ea0fd635a37194efc1f3e0f5012a4704992b0e,
a1a628cca993f9455d22ca2c248ddca7e743683e</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46604	✗	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*:*:*	Mauri ransomware, Quasar RAT
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories.data/CVE-2023-46604

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50623	✗	Cleo Harmony (versions upto 5.8.0.21) Cleo VLTrader (versions upto 5.8.0.21) Cleo LexiCom (versions upto 5.8.0.21)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cleo:vltrader:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:lexicom:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:harmomy:*:*:*:*:*:*:*:*	Cl0p
Cleo Multiple Products Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter; T1105: Ingress Tool Transfer	https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623 , https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49138	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Common Log File System Driver Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55956	☒	Cleo Harmony (prior to version 5.8.0.24) Cleo VLTrader (prior to version 5.8.0.24) Cleo LexiCom (prior to version 5.8.0.24)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cleo:vltrader:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:lexicom:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:harmomy:*:*:*:*:*:*:*:*	Cl0p
Cleo Multiple Products Remote Code Execution Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956 , https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Pensive Ursa, Blue Python)	Russia	Foreign Affairs, Embassies, Government, Defense, Military, Aerospace, Defense, Education, Embassies, Energy, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail	Worldwide
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	TinyTurla, TwoDash, Wainscot, CrimsonRAT	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0040: Impact; TA0042: Resource Development; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1203: Exploitation for Client Execution; T1071: Application Layer Protocol; T1071.004: DNS; T1055: Process Injection; T1036: Masquerading; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1012: Query Registry; T1082: System Information Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1078: Valid Accounts; T1570: Lateral Tool Transfer; T1005: Data from Local System; T1105: Ingress Tool Transfer; T1583: Acquire Infrastructure; T1560: Archive Collected Data; T1584: Compromise Infrastructure; T1584.004: Server; T1213: Data from Information Repositories; T1587: Develop Capabilities; T1587.001: Malware; T1083: File and Directory Discovery; T1588: Obtain Capabilities; T1588.002: Tool; T1057: Process Discovery; T1041: Exfiltration Over C2 Channel

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actor **Secret Blizzard** and malware **Termite ransomware, Realst Stealer, Black Basta Ransomware, Zbot, DarkGate, Mauri ransomware, Quasar RAT, TinyTurla, TwoDash, Wainscot, CrimsonRAT, PUMAKIT, Cl0p.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Secret Blizzard** and malware **Termite ransomware, Realst Stealer, Black Basta Ransomware, Zbot, DarkGate, Mauri ransomware, TinyTurla, TwoDash, Wainscot, CrimsonRAT, PUMAKIT** in Breach and Attack Simulation(BAS).

Threat Advisories

Termite Ransomware Weaponizes Babuk’s Legacy to Strike High-Profile Targets

Web3 Under Siege: AI-Powered Scam Deploys Realst Malware to Steal Crypto

Black Basta’s Evolution: Sophisticated Social Engineering Meets Advanced Payloads

Persistent Attacks Exploiting Apache ActiveMQ CVE-2023-46604

Cleo Zero-Day File Transfer Vulnerabilities Exploited in the Wild

Microsoft’s December 2024 Patch Tuesday Addresses 72 Vulnerabilities

Inside Secret Blizzard’s Seven-Year Espionage Odyssey

PUMAKIT Unveiled: A Stealthy Malware Redefining Linux Threats

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Termite	MD5	6b06aae5ec596cdbc1b9d4c457fd5f81
	SHA1	a515b7d89676b1401eeb9eb776190a1179c386cf
	SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55
	TOR Address	termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion
Realst	SHA256	a0b8789ef3249b5fa8eb3590cd6f183e24273b5886560233025fc9d8de52ce0b, b08740de7bd8d6805ca2c3c8be1db69fbb7aa9bd6aad1c0582881e4196574aa9, fc438c6e231c80c0d5de5b5a194fdba87f88e334414b248047c5e412ed613a6a, 4b93ec3fd49c0111e8a11ac8a0a197f5366cda19732932ce4cb84e024c648a38, 78b2fa0df9fba56ba6a773faa0d280977a1a830fce4f2427935f87de11cb9012, e39cca965dbf7957d04f848572aacfbb736e6aff71e319a788c3f61e52abe795, 2c321b1416fb7226bffd1633a2a053ef3921fef9a1de5c49b71ef9c7b0914b00, 5e6cc2ed3876197561ba60a8d8aa7042d025e997cc1046ea351b5b2bc48f9dd7
Black Basta	SHA1	a6d653d2887f0ce4029a94616464ad74c4f770fe, 0fbed8d60e2d940882e01a2bf11003f6bd59f883, 22f10e42683501fb2ea6962e44eefd64848aefe7
	SHA256	ec669387150865b59bbf98b41a770235ba4fd632aab33433c2d493460ef52479, 95a6c06ac691bec0ac2140b6590c96488feb8bc6c3ca501d1fe8ee7cbf9d0f8b
Zbot	Domains	bigdealcenter[.]world, brownswer[.]com
	SHA1	640640d6651c4ac2f66ed8312084849ad9f0124e, ab1271b4316eb4a5d6ea03b4c24d56cef1e8524a, f09804b59a3aac7c1dd47c7e027182fb54f9a277, f1d299336aac1a1314b36064ffa9ae12ebdb3e4c
	IPv4	45[.]61[.]152[.]154, 185[.]229[.]66[.]224

Attack Name	TYPE	VALUE
Zbot	SHA256	a9f2c4bc268765fc6d72d8e00363d2440cf1dcbd1ef7ee08978959fc118922c9, 22c5858ff8c7815c34b4386c3b4c83f2b8bb23502d153f5d8fb9f55bd784e764
DarkGate	IPv4	179[.]60[.]149[.]194
	SHA1	577EFD1534DD2C4133EA2E4B16A21672D257AF72, bccf867716709ce0167cc72f16d4a14f159e459f, 0fdb26c6202acb33eea938da1a492504035ff8c1
	SHA256	4f30d975121d44705a79c4f5c8aeba80d8c97c8ef10c86fee011b99f12b173b4
Mauri	MD5	07894bc946bd742cec694562e730bac8, 25b1c94cf09076eb8ce590ee2f7f108e, 2c93a213f08a9f31af0c7fc4566a0e56, 2e8a3baeaa0fc85ed787a3c7dfd462e7, 3b56e1881d8708c48150978da14da91e
	SHA256	9c87ef43719d6070e186f2be44ffe51b7c6e57728594928915d7b736bfa87b01
Quasar RAT	IPv4:Port	18[.]139[.]156[.]111:4782
TinyTurla	SHA256	e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381, c039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a
	Domains	connectotels[.]net, hostelhotels[.]net
	IPv4	94[.]177[.]198[.]94, 162[.]213[.]195[.]129, 46[.]249[.]58[.]201, 95[.]111[.]229[.]253
TwoDash	SHA256	dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced, 7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912
	IPv4	146[.]70[.]158[.]90, 143[.]198[.]73[.]108, 161[.]35[.]192[.]207, 91[.]234[.]33[.]48
Wainscot	SHA256	e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273, 08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2
	IPv4	130[.]185[.]119[.]198, 176[.]57[.]184[.]97, 173[.]212[.]252[.]2, 209[.]126[.]11[.]251

Attack Name	TYPE	VALUE
CrimsonRAT	SHA256	aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c
	IPv4	45[.]14[.]194[.]253, 37[.]60[.]236[.]186, 5[.]189[.]183[.]63
PUMAKIT	SHA256	30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f, cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe, 8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03
	Domains	sec[.]opsecurity1[.]art, rhel[.]opsecurity1[.]art
	IPv4	89[.]23[.]113[.]204
Cl0p	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8
	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56

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

What Next?

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

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

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

December 16, 2024 • 9:30 PM

More at www.hivepro.com