Date of Publication
February 6, 2024

Hive Pro®

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JANUARY 2024

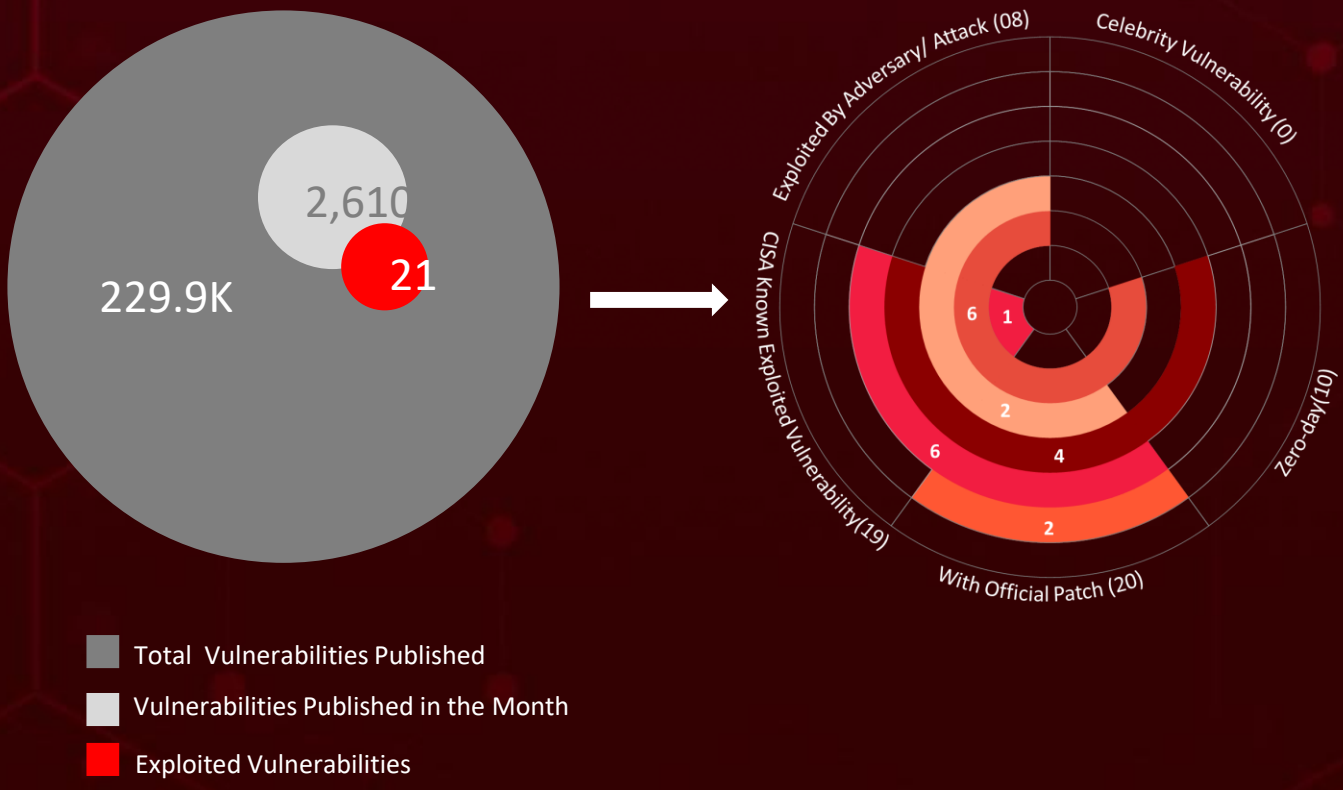
Table Of Contents

Summary

In **January**, the cybersecurity landscape witnessed a surge in attention due to the discovery of **ten zero-day** vulnerabilities. Notably, **two** of these vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways were exploited by the **UTA0178** group, a Chinese nation-state-level actor, leading to a sense of urgency among security teams to patch their systems.

During the same period, ransomware attacks experienced a noticeable uptick, with strains such as **Black Basta, Kasseika, FAUST, and Medusa** actively targeting victims. As ransomware continues to advance in sophistication, organizations are urged to fortify their defenses by implementing robust backup and disaster recovery strategies. Additionally, employee training to recognize and thwart phishing attacks is crucial.

In parallel, **eleven adversaries** were active across diverse campaigns. **Midnight Blizzard** exploited a legacy test OAuth application with elevated access due to a common password and lack of MFA. The attackers leveraged this access to move laterally within Microsoft's network, potentially exfiltrating data and gaining broader control. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

Lumma Stealer adapts to the constantly changing landscape by exploiting users' interest in cracked software through YouTube

Citrix Zero-day NetScaler ADC and NetScaler Gateway are affected by actively exploited zero-day Flaws, identified as CVE-2023-6548 and CVE-2023-6549

APT 28 Targets Ukrainian government and Polish organizations, aiming to deploy new malware for gathering sensitive information

BlueSky Ransomware Deployed worldwide by exploiting CVE-2023-27350

Androxgh0st malware is constructing a botnet focused on illicitly acquiring cloud credentials from popular platforms like Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio

Apple Zero-day CVE-2024-23222 vulnerability in Apple's WebKit is being actively exploited, which results in arbitrary code execution

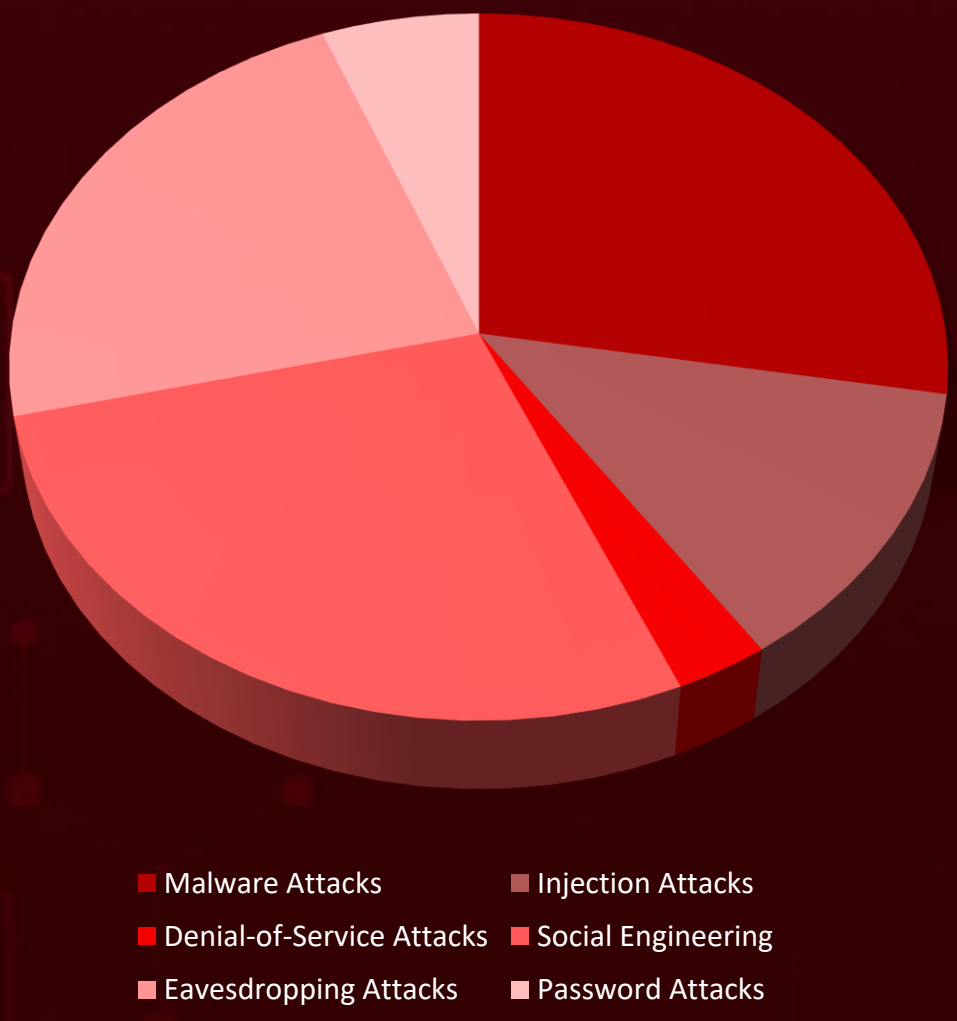
Zloader Resurges after a pause of nearly two years, with fresh iteration that began development in September 2023

Jenkins Flaws Multiple vulnerabilities are found in Jenkins, allowing attackers unauthorized data access and execute arbitrary commands

In January 2024, a geopolitical cybersecurity landscape unfolds, revealing **France, Norway, Oman, US** and **UK** as the top-targeted countries

Highlighted in January 2024 is a cyber battleground encompassing the **Government**, **Technology, NGOs, Media,** and **Financial** sectors, designating them as the top industries

Threat Landscape



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-49897	FXC OS command injection vulnerability	FXC OS	✓	✓	✓
CVE-2023-47565	QNAP VioStor OS command injection vulnerability	QVR Firmware	✓	✓	✓
CVE-2023-39336	Ivanti Endpoint Manager SQL injection Vulnerability	Ivanti Endpoint Manager	✗	✗	✓
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-29357	Microsoft SharePoint Server Privilege Escalation Vulnerability	Microsoft SharePoint Server	✗	✓	✓
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-0519	Google Chrome Out of bounds memory access Vulnerability	Google Chrome	✓	✓	✓
CVE-2023-6548	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-6549	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2017-9841	PHPUnit Command Injection Vulnerability	PHPUnit	✗	✓	✓
CVE-2018-15133	Laravel Deserialization of Untrusted Data Vulnerability	Laravel Framework	✗	✓	✓
CVE-2021-41773	Apache HTTP Server Path Traversal Vulnerability	Apache HTTP Server	✓	✓	✓
CVE-2024-23222	Apple Multiple Products Type Confusion Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Atlassian Confluence Data Center and Server	✗	✓	✓
CVE-2024-0204	Fortra GoAnywhere MFT Authentication bypass Vulnerability	Fortra GoAnywhere MFT	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
InfectedSlurs	Botnet	CVE-2023-49897 CVE-2023-47565	QNAP VioStor NVR, FXC AE1021, AE1021PE	✓	Exploiting vulnerabilities
JenX Mirai	Botnet	CVE-2023-49897 CVE-2023-47565	QNAP VioStor NVR, FXC AE1021, AE1021PE	✓	Exploiting vulnerabilities
OCEANMAP	Backdoor	-	-	-	Phishing
MASEPIE	Backdoor	-	-	-	Phishing
STEELHOOK	Stealer	-	-	-	Phishing
Nim Backdoor	Backdoor	-	-	-	Phishing
Lumma	Infostealer	-	-	-	Exploiting Google OAuth endpoint
Rhadamanthys	Stealer	-	-	-	Exploiting Google OAuth endpoint
RisePro	Stealer	-	-	-	Exploiting Google OAuth endpoint
Meduza	Stealer	-	-	-	Exploiting Google OAuth endpoint
Stealc	Stealer	-	-	-	Exploiting Google OAuth endpoint
Remcos	RAT	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Pikabot	Loader	-	-	-	Malvertising and phishing campaigns
Black Basta	Ransomware	-	-	-	Pikabot
Silver RAT	RAT	-	Windows and Android	-	Social engineering tactics
SnappyTCP	WebShell	-	-	-	Compromised cPanel account
FBot	Exploit tool	-	AWS, Office365, PayPal, Sendgrid, and Twilio	-	Credential harvesting
Medusa	Ransomware	-	Windows	-	Exploiting vulnerable services
Monero	Cryptominer	-	-	-	Phishing
Phemedrone	Information Stealer	CVE-2023-36025	Microsoft Windows	✓	Exploiting vulnerabilities
MediaPL	Backdoor	-	-	-	Phishing
Androxgh0st	SMTP cracker	CVE-2017-9841 CVE-2018-15133 CVE-2021-41773	Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio	✓	Exploiting vulnerabilities
MischiefTut	Backdoor	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SPICA	Backdoor	-	-	-	Phishing
WasabiSeed	Downloader	-	-	-	Phishing
Screenshotter	Stealer	-	-	-	Phishing
Zloader	Trojan	-	-	-	-
RokRAT	Backdoor	-	-	-	Phishing
NS-STEALER	Stealer	-	-	-	ZIP archives that disguise cracked software
Kasseika	Ransomware	-	-	-	Phishing
AsyncRAT	RAT	-	-	-	Phishing
VenomRAT	RAT	-	-	-	Phishing
AllaKore RAT	RAT	-	-	-	Phishing
CherryLoader	Downloader	-	-	-	Phishing
PlugX	RAT	-	-	-	Phishing
Gh0st RAT	RAT	-	-	-	Phishing
FAUST	Ransomware	-	-	-	Phishing

Adversaries Summary

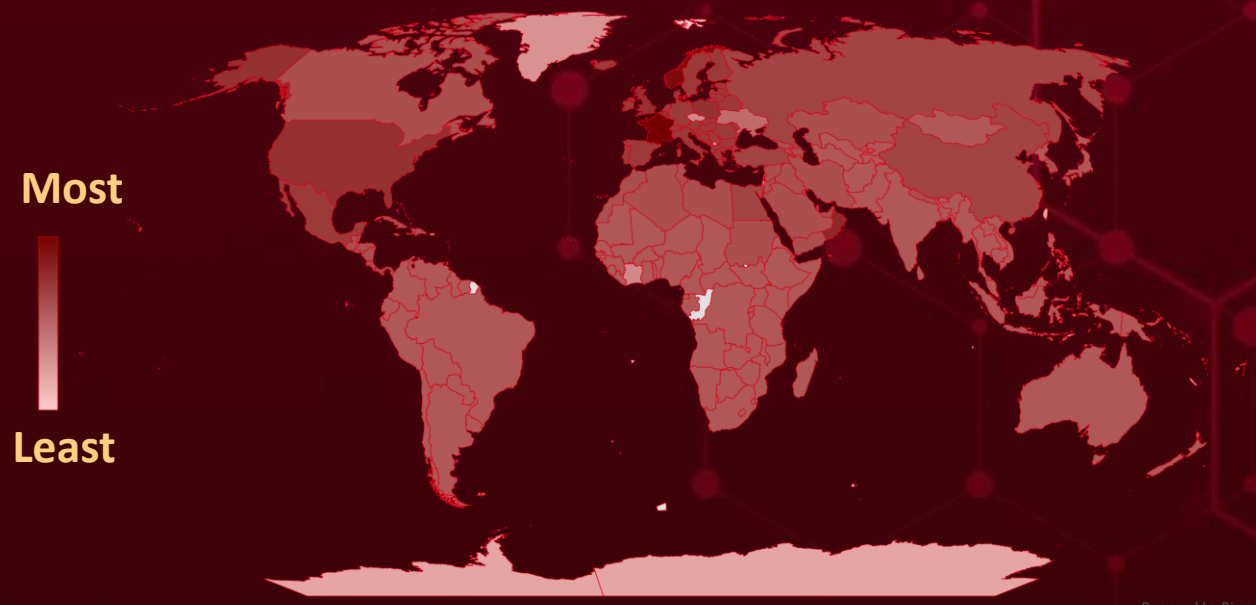
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT28	Information theft and espionage	Russia	-	OCEANMAP, MASEPIE, and STEELHOOK	-
UAC-0050	Information theft and espionage	Unknown	-	Remcos RAT	-
Water Curupira	Financial gain, Information Theft and Espionage	Unknown	-	PikaBot, Black Basta	-
Anonymous Arabic	Hacktivist and Financial gain	Russia	-	Silver RAT	Windows and Android
Sea Turtle	Information theft and espionage	Turkey	-	SnappyTCP	-
Mint Sandstorm	Information theft and espionage	Iran	-	MediaPl backdoor, MischiefTut	-
COLDRIVER	Information theft and espionage	Russia	-	SPICA backdoor	-
TA866	Financial gain	Unknown	-	WasabiSeed and Screenshotter	-
TA571	Financial gain and espionage	Unknown	-	WasabiSeed and Screenshotter	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
ScarCruft	Information theft and espionage	North Korea	-	RokRAT backdoor	-
Midnight Blizzard	Information theft and espionage	Russia	-	-	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
FXC	Operating system	FXC OS
QNAP	Network-Attached Storage (NAS) devices	QVR Firmware
ivanti	Application	Ivanti Connect Secure and Policy Secure
Microsoft	Server	Microsoft SharePoint Server
	Operating system	Microsoft Windows
	Browser	Google Chrome
citrix	Application	Citrix NetScaler ADC and NetScaler Gateway
PHPUnit	Framework	PHPUnit
	Framework	Laravel Framework
APACHE HTTP SERVER PROJECT	Server	Apache HTTP Server
	Operating System	Apple Multiple Products
ATLASSIAN	Data Center and Server	Atlassian Confluence Data Center and Server
FORTRA	MFT	Fortra GoAnywhere MFT

Targeted Countries



Color	Countries
	France
	Norway
	Oman
	United States
	United Kingdom
	Poland
	Belgium
	Slovenia
	Belarus
	Monaco
	Croatia
	Romania
	Denmark
	Mexico
	Estonia
	Netherlands
	Finland
	Bosnia and Herzegovina
	Andorra
	Serbia
	Germany
	Sweden

Color	Countries
	Greece
	Moldova
	Hungary
	Montenegro
	Iceland
	North Macedonia
	Ireland
	Albania
	Austria
	Portugal
	Latvia
	San Marino
	Switzerland
	Slovakia
	Lithuania
	Spain
	Luxembourg
	Bulgaria
	Malta
	Liechtenstein
	Italy

Color	Countries
	Russia
	Turkey
	China
	Cyprus
	Egypt
	Israel
	Iraq
	Haiti
	Qatar
	Cuba
	Canada
	Yemen
	Tunisia
	Bahrain
	Kazakhstan
	Dominica
	Honduras
	Dominican Republic
	Iran
	Jordan
	Syria
	El Salvador
	Libya

Color	Countries
	Barbados
	Guatemala
	Morocco
	Saint Lucia
	Nepal
	Saudi Arabia
	Antigua and Barbuda
	Azerbaijan
	Nicaragua
	South Korea
	Armenia
	Sudan
	Georgia
	Kuwait
	United Arab Emirates
	Trinidad and Tobago
	Costa Rica
	Bahamas
	Algeria
	Grenada
	Belize
	Panama

Color	Countries
	Jamaica
	Lebanon
	Fiji
	Papua New Guinea
	Tonga
	Guinea
	Rwanda
	Guinea-Bissau
	Sri Lanka
	Guyana
	Vanuatu
	Burundi
	Bhutan
	Cambodia
	Senegal
	Cameroon
	South Africa
	India
	Tajikistan
	Indonesia
	Tuvalu
	Angola
	Zambia

Targeted Industries

Most

Least

TOP 25 MITRE ATT&CK TTPS

T1588 Obtain Capabilities	**T1059** Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1082** System Information Discovery	**T1027** Obfuscated Files or Information
T1566 Phishing	**T1588.005** Exploits	**T1140** Deobfuscate/ Decode Files or Information	**T1059.001** PowerShell	**T1083** File and Directory Discovery
T1036 Masquerading	**T1055** Process Injection	**T1659** Content Injection	**T1041** Exfiltration Over C2 Channel	**T1204** User Execution
T1547 Boot or Logon Autostart Execution	**T1071.001** Web Protocols	**T1204.002** Malicious File	**T1053** Scheduled Task/Job	**T1071** Application Layer Protocol
T1053.005 Scheduled Task	**T1203** Exploitation for Client Execution	**T1105** Ingress Tool Transfer	**T1560** Archive Collected Data	**T1070** Indicator Removal

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Nim Backdoor	MD5	e2a3edc708016316477228de885f0c39, 777fcc34fef4a16b2276e420c5fb3a73, EF834A7C726294CE8B0416826E659BAA, 32C5141B0704609B9404EFF6C18B47BF
	SHA1	3aa803baf5027c57ec65eb9b47daad595ba80bac, 5D2E2336BB8F268606C9C8961BED03270150CF65, 4CAE7160386782C02A3B68E7A9BA78CC5FFB0236, 0599969CA8B35BB258797AEE45FBD9013E57C133
	Hostname	mail[.]mofa[.]govnp[.]org, nitc[.]govnp[.]org, mx1[.]nepal[.]govnp[.]org, dns[.]govnp[.]org
	SHA256	b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e, 696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83, 88FA16EC5420883A9C9E4F952634494D95F06F426E0A600A8114F69A6127347F, 1246356D78D47CE73E22CC253C47F739C4F766FF1E7B473D5E658BA1F0FDD662
Lumma	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f
SnappyTCP	MD5	102d8524f21d1b6b0380c817a435e9a7, 80aa20453ca295467bff3f8708a06280, 2a684c83401ec4706f81bf4a3503e096, 19021c37d8adda5fa509dd242629cd50, 8640f22e5a859ea2216d0e9dacef4f50
	SHA256	1ac0b2e91ba3d33ed6b8cd90f5c1f63454bfdf7aad7dbf4f239445f31dfc6eb5, f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f, aea947f06ac36c07ae37884abc5b6659d91d52aa99fd7d26bd0e233fd0fe7ad4

Attack Name	TYPE	VALUE
Fbot	SHA1	1ad78e99918fd66ed43d42a93d2f910a2173b3c5, 2becd32162b2b0cb1afc541e33ace3a29dad96f1, 8ba3fca4deada6dbdc94b17a0c3c55a0b785331e
PikaBot	SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8, 6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8, ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d, 1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b, b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7, 980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753, 6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193, 3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624, 8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004, ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21, 07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632, 2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34, 1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34, 6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e, 7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3, 2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe, 8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df, 79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21

Attack Name	TYPE	VALUE
Silver RAT	SHA256	0ace7ae35b7b44a3ec64667983ff9106df688c24b52f8fcb25729c70a00cc319, 3b06b4aab7f6f590aeac5afb33bbe2c36191aeee724ec82e2a9661e34679af0a, 27b781269be3b0d2f16689a17245d82210f39531e3bcb88684b03ae620ac5007
SPICA backdoor	SHA256	84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507, 37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9, C97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d
Zloader	SHA256	038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55, 16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d, 25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d, 2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456, 83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3, 98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2, adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa, b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93, b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378, d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d, eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499, f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb, f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8, fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616, fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75
	URLs	hxxps://adslstickerhi[.]world, hxxps://adslstickerni[.]world, hxxps://dem.businessdeep[.]com

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-49897	✗	FXC AE1021 & AE1021PE version 2.0.9 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fxc:ae1021_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:fxc:ae1021:-:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
FXC OS command injection vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://www.fxc.jp/form/certify/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47565	✗	QVR Firmware 4.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:qnap:qvr_firmware:*:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
QNAP VioStor OS command injection vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://www.qnap.com/en/download

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-39336</td><td>  </td><td rowspan="2">Ivanti Endpoint Manager: Before 2022 SU5</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:ivanti:ivanti_endpoint_manager:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Endpoint Manager SQL injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-89</td><td>T1059: Command and Scripting Interpreter
T1055: Process Injection</td><td>https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-46805</td><td>  </td><td rowspan="2">Ivanti Pulse Connect Secure: 9.x and 22.x
Ivanti Pulse Policy Secure: 9.x and 22.x</td><td rowspan="2">UTA0178</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:connect_secure:*:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>MITIGATION</td></tr>
<tr><td>CWE-287</td><td>T1588: Obtain Capabilities, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>Import the mitigation.release.20240107.1.xml file via the download portal to address the vulnerabilities temporarily. https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗ ZERO-DAY	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	UTA0178
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**MITIGATION**
	CWE-78	T1059: Command and Scripting Interpreter	Import the mitigation.release.20240107.1.xml file via the download portal to address the vulnerabilities temporarily. https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29357		Microsoft SharePoint Server: 2019	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*	-
Microsoft SharePoint Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36025		Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Phemedrone Stealer
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0519	✗ ZERO-DAY	Google Chrome prior to 120.0.6099.224	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Out of bounds memory access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1082: System Information Discovery	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6548	✗ ZERO-DAY	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15, NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21, NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1055: Process Injection, T1059: Command and Scripting Interpreter	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6549	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15, NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21, NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1059: Command and Scripting Interpreter	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9841	✗	PHPUnit: 4.8.0 - 5.6.2	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:phpunit_project:phpunit:*:*:*:*:*:*:*:*	Androxgh0st
PHPUnit Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94	T1055: Process Injection, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpuoct2021.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23222		iPhone, iPad, tvOS, Safari and Mac running macOS Monterey, Ventura, Sonoma	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*	-
Apple Multiple Products Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1588.006: Vulnerabilities T1203: Exploitation for Client Execution	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22527	✗	Atlassian Confluence Data Center and Server: 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.0-8.5.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:* cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*	-
Atlassian Confluence Data Center and Server Template Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1221: Template Injection T1055: Process Injection	https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-executionvulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0204	✗	Fortra GoAnywhere MFT 6.x from 6.0.1 Fortra GoAnywhere MFT 7.x before 7.4.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortra:goanywhere_mft:*:*:*:*:*:*:*:*	-
Fortra GoAnywhere MFT Authentication bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-425	T1588.006: Vulnerabilities T1556: Modify Authentication Process	https://www.fortra.com/security/advisory/fi-2024-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-15133	✗	Laravel Framework: 5.5.0 - 5.6.29	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:laravel:laravel:*:*:*:*:*:*:*:*	Androxgh0st
Laravel Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-41773	✗	Apache HTTP Server versions 2.4.49 or 2.4.50	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*	Androxgh0st
Apache HTTP Server Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter	https://httpd.apache.org/security/vulnerabilities_24.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23897		Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*:*:*:*	-
Jenkins Arbitrary File Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23898		Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*:*:*:*	-
Jenkins Cross-site WebSocket Hijacking Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1385	T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23899		Git server version 99.va_0826a_b_cdfa_d	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:Gitserver:*:*:*:*:*:*:*:*	-
Jenkins Git Server File Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23905		Red Hat Dependency Analytics version 0.7.1 and prior versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:RedHat_Dependency_Analytics:*:*:*:*:*:*:*:*	-
Jenkins Red Hat Dependency Analytics Plugin Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-23904</td><td>  </td><td rowspan="2">Log Command versions 1.0.2 and prior versions</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:jenkins:Log_Command:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Jenkins Log Command File Read Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-200</td><td>T1059: Command and Scripting Interpreter</td><td>-</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
InfectedSlurs	InfectedSlurs is a new Mirai- based malware botnet, and is actively conducting a sophisticated campaign by exploiting two zero day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, facilitate the creation of a distributed denial-of-service (DDoS) botnet.	Exploiting vulnerabilities	CVE-2023-49897 CVE-2023-47565
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Launch DDoS attacks And Data Theft	QNAP VioStor NVR, FXC AE1021, AE1021PE
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.fxc.jp/form/certify/ , https://www.qnap.com/en/download

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JenX Mirai	The JenX Mirai variant, like many Mirai variants, prints a unique hard-coded string to the console when compromising a machine.	Exploiting vulnerabilities	CVE-2023-49897 CVE-2023-47565
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Launch DDoS attacks And Data Theft	QNAP VioStor NVR, FXC AE1021, AE1021PE
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.fxc.jp/form/certify/ , https://www.qnap.com/en/download

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
OCEANMAP	OCEANMAP is a malicious program developed using the C# programming language. The main functionality consists in executing commands using cmd.exe. The IMAP protocol is used as a control channel.	distribution of e-mails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
APT28			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MASEPIE	MASEPIE is a malicious program developed using the Python programming language. The main functionality consists in uploading/unloading files and executing commands. The TCP protocol is used as a control channel. Data is encrypted using the AES-128-CBC algorithm	distribution of e-mails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Upload or unload files, execute commands	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
APT28			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
STEELHOOK	STEELHOOK is a PowerShell script that provides the theft of Internet browser data ("Login Data", "Local State") and the DPAPI master key by sending them to the management server using an HTTP POST request in base64-encoded form.	distribution of e-mails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
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 CVEs
Nim Backdoor	Nim Backdoor is written in Nim programming language . A backdoor is a hidden way to access a system or application that is not intended for public use.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data theft, Spying on victims	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma Infostealer	Lumma is an information stealer, developed using the C programming language. It is offered for sale as a malware-as-a-service, with several plans available. It usually targets cryptocurrency wallets, login credentials, and other sensitive information on a compromised system.	Exploiting Google OAuth Endpoint and Disguised as cracked software	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys	Rhadamanthys is a C++ information stealer that first emerged in August 2022, targeting email, FTP, and online banking service account credentials.	Exploiting Google OAuth endpoint	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data theft	-
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Risepro	RisePro is a stealer that is spread through downloaders like win.privateloader. Once executed on a system, the malware can steal credit card information, passwords, and personal data.	Exploiting Google OAuth endpoint	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Meduza	The Meduza Stealer malware has a singular objective: comprehensive data theft. It pilfers users' browsing activities, extracting a wide array of browser-related data.	Exploiting Google OAuth endpoint	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Stealc	Stealc is an information stealer sold as a Malware-as-a-Service since January 9, 2023. It is a non-resident stealer with flexible data collection settings and its development is relied on other prominent stealers. Stealc is written in C and uses WinAPI functions. It mainly targets date from web browsers, extensions and Desktop application of cryptocurrency wallets.	Exploiting Google Oauth endpoint	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	-
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes but has been used in numerous hacking campaigns. Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		remote surveillance and control	-
ASSOCIATED ACTOR			PATCH LINK
UAC-0050			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PikaBot	Pikabot is a sophisticated piece of multi-stage malware with a loader and core module within the same file. Pikabot, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising and phishing campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft, Downloading other malware	-
ASSOCIATED ACTOR			PATCH LINK
Water Curupira			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Black Basta	Black Basta ransomware has been actively using Pikabot a loader malware in spam campaigns throughout 2023.Black Basta deploys a range of second-stage tactics to acquire Windows Domain credentials and penetrate a target's network laterally	Pikabot	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Steal credentials, data theft and Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
Water Curupira			-

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
Silver RAT	Silver RAT, a Windows-based RAT written in C# and developed by a group known as "Anonymous Arabic," exhibits advanced capabilities, including antivirus evasion and ransomware encryption.	Social engineering tactics	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Executes custom commands, data encryption, and system restore point deletion.	Windows and Android
ASSOCIATED ACTOR			**PATCH LINK**
Anonymous Arabic			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SnappyTCP	A reverse TCP shell named SnappyTCP for Linux/Unix with basic command-and-control capabilities has been used to establish persistence on systems.	Compromised cPanel account	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
WebShell		Man-in-the-middle attacks to harvest credentials	-
ASSOCIATED ACTOR			**PATCH LINK**
Sea Turtle			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Fbot	FBot, a Python-based exploit tool, has systematically targeted critical infrastructures. Its primary objective is to infiltrate these services, acquiring credentials to subsequently monetize unauthorized access by selling it to other malicious entities.	Credential harvesting	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Exploit tool		Data loss, Hijack cloud, SaaS, and web services	AWS, Office365, PayPal, Sendgrid, and Twilio.
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Medusa	Medusa ransomware employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non-compliant organizations. Operating as a ransomware-as-a-service approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.	Exploiting vulnerable services	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data exfiltration, information theft, and financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Monero	Monero, a privacy-focused cryptocurrency, has become a magnet for cryptominers, both legitimate and malicious. The lure lies in its unique mining algorithm, RandomX, designed to be resistant to specialized hardware (ASICs) and favor consumer-grade CPUs and GPUs.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Cryptominer		Data Theft	-
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Phemedrone	The Phemedrone stealer malware campaign exploits a vulnerability in Microsoft Defender SmartScreen. Phemedrone, an open-source information-stealing malware written in C#, is designed to extract data from web browsers, and cryptocurrency wallets.	Exploiting vulnerabilities	CVE-2023-36025
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MediaPl	MediaPI is a highly sophisticated malware strain crafted to undermine the security of researchers and compromise their data. Functioning as a backdoor trojan, its primary purpose is to illicitly harvest data from compromised computers.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Mint Sandstorm			-

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
Androxgh0st	The Androxgh0st malware is building a botnet, specifically aimed at illicitly obtaining cloud credentials from popular applications such as Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio. This stolen data is then utilized to disseminate additional harmful payloads.	Exploiting vulnerabilities	CVE-2017-9841 CVE-2018-15133 CVE-2021-41773
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio
SMTP cracker			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.oracle.com/security-alerts/cpuoct2021.html; https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30; https://httpd.apache.org/security/vulnerabilities_24.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MischiefTut	MischiefTut, a custom PowerShell-based backdoor, performs reconnaissance, records outputs, and can download additional tools on compromised systems.	Unknown	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Mint Sandstorm			-

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
SPICA	SPICA, written in Rust, employs JSON over websockets for command and control. It executes shell commands, steals browser cookies, uploads/downloads files, and explores the filesystem. Upon execution, it establishes persistence and opens a decoy PDF, awaiting further commands in its C2 loop.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Exfiltration, Disruption	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
COLDRIVER			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WasabiSeed	WasabiSeed is a simple VBS downloader which repeatedly to connect to the C2 server looking for payload to download and run.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Downloads and executes a MSI file	-
Downloader			
ASSOCIATED ACTOR			PATCH LINK
TA866, TA571			-

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
Screenshotter	Screenshotter has a single purpose of taking a screenshot of the victim's screen and sending it to the command and control (C2) server.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Take Screenshots	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
TA866, TA571			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Zloader	Zloader is a trojan designed to steal cookies, passwords and sensitive information. The main audience of this piece of malware are users of financial institutions worldwide.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RokRAT backdoor	It is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode. It is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex.	Phishing emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
ScarCruft			-

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
NS-STEALER	It is a Java-based information stealer, spreads through cracked software ZIP files. It utilizes JDABuilder Classes to create an instance of an EventListener for easy registration, and the stealer uses a Discord bot channel as part of its EventListener functionality.	ZIP archives that disguise cracked software	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Kasseika ransomware	The Kasseika ransomware is a 32-bit Windows PE file packed by Themida. Before encryption, Kasseika terminates all processes and services that are currently accessing Windows Restart Manager.	Phishing emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	-
Ransomware			
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a remote access trojan released in 2019, primarily as a credential stealer and loader for other malware, including ransomware. AsyncRAT has botnet capabilities and C2 interface allowing operators to control infected hosts remotely.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remotely record a target's screen, Import and execute additional malware, Exfiltrate files on an infected system	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VenomRAT	VenomRAT is a fork of Quasar RAT that is promoted online as a (benevolent) remote access tool for Windows machines. In reality, it's an info-stealing trojan that can be used for malicious purposes. On a technical level, VenomRAT is poorly designed, with hardcoded IPs and misuses of Ngrok tunneling tools.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	-
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AllaKore RAT	AllaKore RAT is a Remote Access Trojan (RAT) malware used in targeted attacks against Mexican businesses. It's typically distributed through phishing emails containing malicious attachments. Once opened, the attachment downloads and installs the malware on the system.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System compromise	-
RAT			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CherryLoader	CherryLoader, a new Go-based downloader, has surfaced in cyber attacks, masquerading as the legitimate CherryTree note-taking app. This sophisticated threat infiltrates compromised hosts, delivering malicious payloads such as privilege escalation tools for exploitation and persistent control.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Deploy malware	-
Downloader			
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX	PlugX is a well-established Remote Access Trojan (RAT) malware family with a history dating back to 2008. It's known for its modularity, allowing attackers to customize it with various functionalities for different purposes.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gh0st RAT	Gh0st RAT is a Remote Access Trojan (RAT) that allows attackers to remotely control and spy on infected devices. It has been used in various cyberattacks, including those targeting sensitive computer networks. It possesses features like keylogging, screenshot capture, webcam and microphone access, file manipulation, and remote control capabilities.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	-
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.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FAUST ransomware	FAUST ransomware, a variant of the Phobos family, exhibiting intricate deployment stages, from decoding Base64 data to injecting shellcode. Notably, it employs a fileless attack through an Office document with a VBA script, emphasizing the need for user caution with document files from untrusted sources.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Encrypt Data	-
Ransomware			
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 COUNTRIES
APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Energy, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	OCEANMAP, MASEPIE, and STEELHOOK	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1095: Non-Application Layer Protocol; T1567: Exfiltration Over Web Service; T1021: Remote Services; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1003: OS Credential Dumping; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.003: Mail Protocols; T1132: Data Encoding; T1132.001: Standard Encoding; T1572: Protocol Tunneling;

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UAC-0050	-	Government	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Remcos RAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1007: System Service Discovery; T1059.001: PowerShell; T1547: Boot or Logon Autostart Execution; T1216: System Script Proxy Execution; T1027: Obfuscated Files or Information; T1555: Credentials from Password Stores; T1547.001: Registry Run Keys / Startup Folder; T1041: Exfiltration Over C2 Channel; T1204: User Execution;			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Water Curupira	-	-	Worldwide
	MOTIVE		
	Financial gain, Information Theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	PikaBot, Black Basta	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0042: Resource Development; TA0007: Discovery; TA0011: Command and Control; TA0009: Collection; TA0010: Exfiltration; TA0040: Impact; T1082: System Information Discovery; T1057: Process Discovery; T1219: Remote Access Software; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1566: Phishing; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1036: Masquerading; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1041: Exfiltration Over C2 Channel; T1140: Deobfuscate/Decode Files or Information; T1560: Archive Collected Data; T1102: Web Service; T1574: Hijack Execution Flow			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Anonymous Arabic</td><td>-</td><td rowspan="3">-</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Hacktivist and Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Silver RAT</td><td>Windows and Android</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0007: Discovery; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0010: Exfiltration; TA0003: Persistence; TA0004: Privilege Escalation; T1027: Obfuscated Files or Information; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1055: Process Injection; T1112: Modify Registry; T1497: Virtualization/Sandbox Evasion; T1056: Input Capture; T1539: Steal Web Session Cookie; T1552: Unsecured Credentials; T1528: Steal Application Access Token; T1057: Process Discovery; T1083: File and Directory Discovery; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

Sea Turtle (aka Teal Kurma, Marbled Dust, SILICON, and Cosmic Wolf)</td><td>Turkey</td><td rowspan="3">Government entities, political groups, telecommunication, ISPs, IT-service providers (including security companies), NGO and Media & Entertainment sectors</td><td rowspan="3">Europe, Middle East and North Africa</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>SnappyTCP</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; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.001: Malware; T1133: External Remote Services; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1505: Server Software Component; T1505.003: Web Shell; T1070: Indicator Removal; T1070.003: Clear Command History; T1070.002: Clear Linux or Mac System Logs; T1114: Email Collection; T1114.001: Local Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1567: Exfiltration Over Web Service</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Mint Sandstorm (aka Charming Kitten, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Ballistic Bobcat)	Iran	High-profile Individuals of research organizations and universities	Belgium, France, Gaza, Israel, the United Kingdom, and the United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MediaPl backdoor, MischiefTut	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting: Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1036: Masquerading; T1573: Encrypted Channel; T1053: Scheduled Task/Job; T1204: User Execution; T1204.002: Malicious File; T1132: Data Encoding; T1132.001: Standard Encoding

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
COLDRIVER (aka Star Blizzard, Nahrelbared, NahrElbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto)</td><td>Russia</td><td rowspan="3">High profile individuals in NGOs, former intelligence and military officers and NATO governments</td><td rowspan="3">Ukraine, NATO countries</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>SPICA backdoor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1539: Steal Web Session Cookie; T1083: File and Directory Discovery; T1053: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1560: Archive Collected Data; T1105: Ingress Tool Transfer; T1071: Application Layer: Protocol; T1071.001: Web Protocols</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA866	Unknown	All	United States and Germany
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	WasabiSeed and Screenshotter	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1218: System Binary Proxy Execution; T1218.007: Msiexec			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA571	Unknown	All	Worldwide
	MOTIVE		
	Financial gain and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	WasabiSeed and Screenshotter	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1218: System Binary Proxy Execution; T1218.007: Msiexec			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ScarCruft (aka Reaper, TEMP.Reaper, APT 37, Ricochet Chollima, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet)	North Korea	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RokRAT backdoor	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1598.002: Spearphishing Attachment; T1204.002: Malicious File; T1105: Ingress Tool Transfer; T1005: Data from Local System; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1562: Impair Defenses; T1083: File and Directory Discovery; T1041: Exfiltration Over C2 Channel; T1537: Transfer Data to Cloud Account

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Midnight Blizzard (aka APT 29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)</td><td>Russia</td><td rowspan="3">Governments, Diplomatic entities, Non-Governmental Organizations (NGOs) and IT service providers</td><td rowspan="3">US and Europe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0006: Credential Access; TA0042: Resource Development; TA0005: Defense Evasion; T1110.003: Password Spraying; T1110: Brute Force; T1027: Obfuscated Files or Information; T1586: Compromise Accounts; T1190: Exploit Public-Facing Application; T1583: Acquire Infrastructure; T1583.006: Web Services; T1586.002: Email Accounts</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
	T1593: Search Open Websites/Domains	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	T1590.004: Network Topology
	T1592: Gather Victim Host Information	T1592.002: Software
	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
	T1598: Phishing for Information	
TA0042: Resource Development	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.001: Malware
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.002: DNS Server
		T1583.005: Botnet
		T1583.008: Malvertising
		T1583.004: Server
		T1583.006: Web Services
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.003: Cloud Accounts
		T1585.002: Email Accounts
	T1584: Compromise Infrastructure	T1584.004: Server
TA0001: Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
	T1189: Drive-by Compromise	
	T1133: External Remote Services	
	T1190: Exploit Public-Facing Application	
	T1659: Content Injection	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.004: Cloud Accounts

Tactic	Technique	Sub-technique
TA0002: Execution	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1106: Native API	
	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
	T1129: Shared Modules	
	T1559: Inter-Process Communication	T1559.001: Component Object Model
		T1559.002: Dynamic Data Exchange
	T1047: Windows Management Instrumentation	
	T1569: System Services	T1569.002: Service Execution
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1136: Create Account	T1136.002: Domain Account
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1133: External Remote Services	
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1176: Browser Extensions	
TA0004: Privilege Escalation	T1055: Process Injection	
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1098: Account Manipulation	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1036: Masquerading	T1036.007: Double File Extension
		T1036.005: Match Legitimate Name or Location
	T1202: Indirect Command Execution	
	T1480: Execution Guardrails	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
	T1070: Indicator Removal	T1070.006: Timestomp
		T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1564: Hide Artifacts	T1564.002: Hidden Users
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1027: Obfuscated Files or Information	T1027.009: Embedded Payloads
	T1220: XSL Script Processing	
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1134: Access Token Manipulation	
	T1622: Debugger Evasion	
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
		T1555.004: Windows Credential Manager
	T1040: Network Sniffing	
	T1557: Adversary-in-the-Middle	
	T1539: Steal Web Session Cookie	
	T1110: Brute Force	
	T1056: Input Capture	T1056.001: Keylogging
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1558: Steal or Forge Kerberos Tickets	T1558.001: Golden Ticket
	T1606: Forge Web Credentials	
	T1552: Unsecured Credentials	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1007: System Service Discovery	
	T1040: Network Sniffing	
	T1018: Remote System Discovery	
	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1046: Network Service Discovery	
	T1087: Account Discovery	
	T1518: Software Discovery	
	T1482: Domain Trust Discovery	
	T1217: Browser Information Discovery	
	T1622: Debugger Evasion	
	T1083: File and Directory Discovery	
	T1016: System Network Configuration Discovery	
	T1135: Network Share Discovery	
	T1497: Virtualization/Sandbox Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote DesktopProtocol
	T1210: Exploitation of Remote Services	
	T1570: Lateral Tool Transfer	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
TA0009: Collection	T1114: Email Collection	T1114.002: Remote Email Collection
		T1114.003: Email Forwarding Rule
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1074: Data Staged T1557: Adversary-in-the-Middle	
	T1056: Input Capture	T1056.001: Keylogging
		T1114.003: Email Forwarding Rule
	T1005: Data from Local System	
	T1119: Automated Collection	
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.004: DNS
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1105: Ingress Tool Transfer	
	T1104: Multi-Stage Channels	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1572: Protocol Tunneling	
	T1008: Fallback Channels	
	T1568: Dynamic Resolution	

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1020: Automated Exfiltration	
	T1029: Scheduled Transfer	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0040: Impact	T1489: Service Stop	
	T1498: Network Denial of Service	
	T1490: Inhibit System Recovery	
	T1486: Data Encrypted for Impact	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation

Top 5 Takeaways

#1 In January, we identified twenty critical vulnerabilities, including ten zero-day vulnerabilities. Two of these vulnerabilities were exploited by the UTA0178 group, a Chinese nation-state-level actor.

#2 Throughout the month, ransomware strains including **Black Basta , Kasseika, FAUST,** and **Medusa** actively targeted victims.

#3 Numerous malware families have been observed targeting victims in the wild. These include **Zloader, AsyncRAT, PlugX, Pikabot, Black Basta,** and **Androxgh0st**.

#4 There were a total of **11** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: Government, Technology, NGOs, Media, and Financial.

#5 Finally, Midnight Blizzard exploited a legacy test OAuth app with a common password and no MFA, moving laterally in Microsoft's network for potential data exfiltration and broader control.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **21 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 37 active malware,** and **219 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 **21 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).

Hive Pro Threat Advisories (JANUARY 2024)

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

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.

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
InfectedSlurs	SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380, f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1, a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26, cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87, 8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6, 35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a, 7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2, 29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff, cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9, a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1
JenX Mirai	SHA256	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1
OCEANMAP	MD5	6fdd416a768d04a1af1f28ecaa29191b, 5db75e816b4cef5cc457f0c9e3fc4100
	SHA256	fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23, 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04
	IP	74[.]124.219.71

Attack Name	TYPE	VALUE
OCEANMAP	Domains	jrb@bahouholdings[.]com, qasim.m@facadesolutionsuae[.]com, webmail.facadesolutionsuae[.]com
MASEPIE	MD5	47f4b4d8f95a7e842691120c66309d5b
	SHA256	18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
STEELHOOK	SHA256	6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
	MD5	5f126b2279648d849e622e4be910b96c
Nim Backdoor	MD5	e2a3edc708016316477228de885f0c39, 777fcc34fef4a16b2276e420c5fb3a73, EF834A7C726294CE8B0416826E659BAA, 32C5141B0704609B9404EFF6C18B47BF
	SHA1	3aa803baf5027c57ec65eb9b47daad595ba80bac, 5D2E2336BB8F268606C9C8961BED03270150CF65, 4CAE7160386782C02A3B68E7A9BA78CC5FFB0236, 0599969CA8B35BB258797AEE45FBD9013E57C133
	Hostname	mail[.]mofa[.]govnp[.]org, nitc[.]govnp[.]org, mx1[.]nepal[.]govnp[.]org, dns[.]govnp[.]org
	SHA256	b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e, 696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83, 88FA16EC5420883A9C9E4F952634494D95F06F426E0A600A8114F69A6127347F, 1246356D78D47CE73E22CC253C47F739C4F766FF1E7B473D5E658BA1F0FDD662
Remcos	MD5	56154fedaa70a3e58b7262b7c344d30a, 9b777d69b018701ec5ad19ae3f06553f, 74865c6c290488bd5552aa905c02666c, 7c05cfed156f152139a6b1f0d48b5cc1, 7c05cfed156f152139a6b1f0d48b5cc1, 0b2d0eb5af93a3355244e1319e3de9da, 7f87d36c989a11edf0de9af392891d89, f5ee6aa31c950dfe55972e50e02201d3, 5c734bb1e41fab9c7b2dabd06e27bc7b, 1c3e1e0319dc6aa24166d5e2aaaec675, 818beece85ecd90d413782dd51d939b1,

Attack Name	TYPE	VALUE
Lumma	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd
Rhadamanthys	SHA256	bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

Attack Name	TYPE	VALUE
Risepro	SHA256	e8b221cba5c3598522f1ebd2b5e52b2f45699a1965b5dd677a9b9d074677873e, 356019c5f0ab89bcaff1639b2b2a427d7777fcfa13c09f889ef5ea8eb1c031c7, 5aa9cbeb84e41ab814e989920c76278d94827fb490f05d7421082570d1a1a3bb
Meduza	MD5	eba71e82cb96780b4711bf898067ba81, 5c1e871a99108b68c90f6adbac5b190f, 3894a29e43d8847778f0fbb81bb479b9, 73070434952f46d1f37f9ab4bb99754f, eb52c4a4bef2367e721bbe13e89aacf5, adc35bb330618a365685b5864e403007, 02fa600eb8a92d7ce676f87269365ca0, 021b649ce9d11e2ca9c67761953b1408, c1824076854acac6858177062c1f5493, 80136b6c96f8b23f8e938e38e01c58e6, c712a1b8a70fb7d0c7a714e12eff0e38
Stealc	SHA256	e6e1106fec7137b46da15bdd0853b1b9a6104bce649a24145793e4d451261c6b, d63a83fb534fd92df1de5373ce6fa7febf6ca715c7528a2a806de49da2889078
PikaBot	SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589cefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8, 6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8, ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d, 1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b, b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7, 980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753, 6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193, 3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624, 8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004,

Attack Name	TYPE	VALUE
PikaBot	SHA256	ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21, 07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632, 2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34, 1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a, 33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34, 6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e, 7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3, 2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe, 8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df, 79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21, 1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a, eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a, 7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7, 46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66, 4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, 7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2
	URLs	hxxps://sindicaturadetecate[.]gob[.]mx/pe/?IDbHJCMofpEIzDQjrcwNcDqHoiQRnSKZQcA, hxxps://lsn[.]edu[.]dz/pqis/?aWDzZBatBsyv, hxxp:188[.]34[.]192[.]184/76DKN6/Wheez, hxxps://brouweres[.]com:443/vvs49/0.8450027286577588.dat, hxxps://brouweres[.]com:443/vvs49/0.15313287608559223.dat, hxxps://brouweres[.]com:443/vvs49/0.9900618798908114.dat
	IPv4:Port	15[.]235[.]202[.]109:2226, 15[.]235[.]44[.]231:5938, 15[.]235[.]45[.]155:2221, 15[.]235[.]47[.]206:13783, 15[.]235[.]47[.]80:23399, 154[.]221[.]30[.]136:13724, 154[.]61[.]75[.]156:2078, 154[.]92[.]19[.]139:2222, 188[.]26[.]127[.]4:13785,

Attack Name	TYPE	VALUE
PikaBot	IPv4:Port	210[.]243[.]8[.]247:23399, 51[.]195[.]232[.]97:13782, 51[.]68[.]147[.]114:2083, 51[.]79[.]143[.]215:13783, 64[.]176[.]5[.]228:13783, 154[.]221[.]30[.]136:13724, 137[.]220[.]55[.]190:2223, 210[.]243[.]8[.]247:23399, 65[.]20[.]78[.]68:13721, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 154[.]92[.]19[.]139:2222, 172[.]233[.]156[.]100:13721, 154[.]61[.]75[.]156:2078, 64[.]176[.]67[.]194:2967, 158[.]247[.]253[.]155:2225, 139[.]180[.]216[.]25:2967, 70[.]34[.]209[.]101:13720, 172[.]233[.]156[.]100:13721, 154[.]92[.]19[.]139:2222, 154[.]61[.]75[.]156:2078, 137[.]220[.]55[.]190:2223
Black Basta	Domains	lindacolor[.]com, withclier[.]com, unougn[.]com, bluenetworking[.]net, getfnewsolutions[.]com, conitreid[.]com, allcompanycenter[.]com, sandelias[.]com, getfnewssolutions[.]com, erihudeg[.]com, reganter[.]com, masterunis[.]net, masterunis[.]net, taskthebox[.]net, taskthebox[.]net, settingfir[.]com, magementfair[.]com, businesforhome[.]com, ruggioil[.]com, gertefin[.]com, gartenlofti[.]com, garbagemoval[.]com, constrtionfirst[.]com, animalsfast[.]net, schumacherbar[.]com, maluisepaul[.]com, masterunix[.]net, wardeli[.]com,

Attack Name	TYPE	VALUE
Black Basta	Domains	nutiensel[.]com, jessvisser[.]com, caspercan[.]com, kolinileas[.]com, unitedfrom[.]com, brendonline[.]com, septcntr[.]com, auuditoe[.]com, conectmeto[.]net, startupbusiness24[.]net, seohomee[.]com, softradar[.]net, investsystemus[.]net, blocknowtech[.]net, mytrailinvest[.]net, realeinvestment[.]net, cloudwebstart[.]net, monitor-websystem[.]net, karmafisker[.]com, airbusco[.]net, trailgroupl[.]net, monitorsystem[.]net, cloudworldst[.]net, neobeelab[.]net, stockinvestlab[.]net, prettyanimals[.]net, gift4animals[.]com, ionoslaba[.]com, buyadvisershop[.]net, blockcentersys[.]net, startuptechnologyw[.]net, investmentrealtyhp[.]net, mynewbee[.]net, buzzybeet[.]net, wellsystemte[.]net, investmendvisor[.]net, reelsysmoona[.]net, startupbizaud[.]net, building4business[.]net, steamteamdev[.]net, audsystemecll[.]net, welausystem[.]net, treeauwin[.]net, clearsystemwo[.]net
Silver RAT	SHA256	79a4605d24d32f992d8e144202e980bb6b52bf8c9925b1498a1da59e50ac51f9, a9fa8e14080792b67a12f682a336c0ea9ff463bbcb27955644c6fcaf80023641, 7a9aeea5e65a0966894710c1d9191ba4cbd6415cba5b10b3b75091237a70a5b8,

Attack Name	TYPE	VALUE
Silver RAT	SHA256	0ace7ae35b7b44a3ec64667983ff9106df688c24b52f8fcb25729c70a00cc319, 3b06b4aab7f6f590aeac5afb33bbe2c36191aeee724ec82e2a9661e34679af0a, 27b781269be3b0d2f16689a17245d82210f39531e3bcb88684b03ae620ac5007
SnappyTCP	MD5	102d8524f21d1b6b0380c817a435e9a7, 80aa20453ca295467bff3f8708a06280, 2a684c83401ec4706f81bf4a3503e096, 19021c37d8adda5fa509dd242629cd50, 8640f22e5a859ea2216d0e9dacef4f50
	SHA256	1ac0b2e91ba3d33ed6b8cd90f5c1f63454bfdf7aad7dbf4f239445f31dfc6eb5, f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f, aea947f06ac36c07ae37884abc5b6659d91d52aa99fd7d26bd0e233fd0fe7ad4
Fbot	SHA1	1ad78e99918fd66ed43d42a93d2f910a2173b3c5, 2becd32162b2b0cb1afc541e33ace3a29dad96f1, 8ba3fca4deada6dbdc94b17a0c3c55a0b785331e
Lumma	SHA256	01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f
Medusa	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270
MediaPl backdoor	SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f
SPICA backdoor	SHA256	84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507, 37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9, C97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d

Attack Name	TYPE	VALUE
Monero cryptominer	SHA256	eea29961fc606fdc27bd77707bd3f7e4b8a1b17d73d7c6fcd20c014ecdb4e3fb, 61531092cd9111095aef20168c61a85f61e2bdc7341adbcdb60c39adba4d395c, 8afc300d41966777e10c321153a106125bd29ee6cf5cc0d8794697da826b5b65, 04aceaa4d58f373e64c78d19cb0d37da3453374014b2f391684958b6bb10e7f4, 7dafec3494c7b178e9cec154b89b520e789c117d735fdabb2dd9c0bd5338548b, a3af09049c4ba6ef13bf2ec645cf653777ede84c0cfc04f2aa6c0c9fa6e93dac, 6ef7e257764b1438c3a83f46699c81ad46ec35a38737f7980d65debc0fbf2007, ab8601854e04de69ec28b2996a364854a8a9ff238574569305d7455e6c52f690, 4d2c328739e69a3dcb457ca7447eba21b8d364af33539fbc2a51c24dafd28eb4, 1727ffd1ed79775dd36fc812381aea3414a2f235ff8ce7755eb0b1b7388af7cc, d073960d52393ccf2af5a7cc0661a41a913a5c440158a29794a8461bf27bd8b6, e613ef1133c27266edf01b389575336b471101f202cc92e513a40ca7b91b9dfe, 0375749ada9056ed6e9c38ece8956172605470fd1d13685a6b03a376c2566076, 14ddc4e3184c6212e656b267f8a600bb0aac606d6c48d1e0854d6a3f6ce867fd, 0b9cdd16c45db58d1e69804953d38b1ed6b063989d2c125054f3a94b0f79f591, a1dea403ba55e900419ef7cd355253b4e9d08005cf44918a8993df844b616e10, c0eda3d6d769d945595e6d4fa2b68e3186fa66b662d4feb42173026c438626a0, 745a736dd76e415ab9e42688f9d4d21616ce182451f0afa760156b76f07194f9, 73d68aed6e9a5789938b86c450e50dc5151dbec0bc7c272f57d58229bfd9b4a9, 90898ba98f396d9fcb621b7c1ff58e12f00c05e6caf026d9855ebc507666f203

Attack Name	TYPE	VALUE
Phemedrone Stealer	SHA256	f32964087462ba3c96a87ee8387f89de8fa605f2f5bb84cb5f754cd736683f2d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424, 815b2125d6f0a5d99750614731aaad2c6936a1dc107a969408a88973f35064c0, ccd19ef6e81e936fc944ebafaefd2ad99ccd11dd15fbc7d3460726bb38237595, ea9b0dee3b7583ce60bba277e2189acb660284abf6b3b9273b6a60c85b0a5ce3, 9a96406ae06b703d827fffd1f1ced0781f89ca2af6d5041721e9fbd2647c8430, 22236e50b5f700f5606788dcd5ab1fb69ee092e8dffdd783ac3cab47f1f445ab, 1433efd142007ce809aff5b057810f5a1919ea1e3ff740ff0fcc2fc729226be5, ad513d2cba6cc82a50ee6531b275e937480d8fee20af2b4f41da5f88e408a4e9, 7c0a1e11610805bd187ef6e395c8fa31c1ae756962e26cdbff704ce54b9e678a, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c9743e7ffb6f6978f08f86e970ddb82e24920d266b32bd242254fbf51abfe6ce, 1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415, b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53, f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, 8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d, 9b9ba722b314febfc44919551a03dde1539f115333183c2cb5e74b8e644ba5b3, 568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322563,

Attack Name	TYPE	VALUE
Phemedrone Stealer	SHA256	c3bfaa1f52abdbb673d83af67090112dfdfe9ea8ff7a613f62bd48bace205f75, 6bd8449de1e1bdd62a86284ed17266949654f758e00e10d8cd59ec4d233c32e5, 4446d5b475ce8aed5244da917ae42b6cb9744ffc4efd766af8e4dee7dd5a3e19, 70c23213096457df852b66443d9a632e66816e023fdf05a93b9087ffb753d916, 69941417f26c207f7cbbbe36ce8b4d976640a3d7f407d316932428e427f1980b, e2d19a23b19a07d35d16990e78c5cfaa3dd97b9ce92201f4db18a7da95fe6ff8, b7f53c507a1aa4254b66a883285e27b42d65ea4ea4206fe674e0d03738f52141, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, f24a8b3144e89b9bececfbf76add87ddefbd19a024a85692026e97f3a9911902, e64b185c149cb523d13cb46ea3911e2c0595b6f10ae86e6a14b15e8d45c0cdcb, cb58bf466675be9e11cfb404503cb122514f47b9708d033e381f28a60535812c, 80f88566fda41ebc1b4e35d89748a804740bba0d03049c33c536cffd5e0491e2, 4a36cc607ca5c2acc536510fd1b0ddd43a9403dac168d2420d474611909ed9e6, 89caa1568fcff162086dae91e6bd34fd04facba50166ebff800d45a999d0be8b, 188c72f995ebd5e1e8d0e3b9d34eeeec2ec95d4d0fee30d2ea0f317ab1596eef, e326c1b9e61cca6823300158e55381c6951b09d2327a89a8d841539cad3b4df3, 4da33c7fe62f71962913d7b40ff76aff9f1586e57db707b3d6b88162c051f402, ff44e502bd5ea36e17b3fc39b480e65971b36002f27fb441e4acadd6bf604a20, b7980f64f892d70b1cd72a8c80f8319f50c3c410aba4e4bc63fd6494bcb4f313, 480fae3bdc2604cba846779dd7dced95b3ce036bdef629ded247771a2e4d5d58, 348aea633c99e5f6a0ac7b850961be0a145a35678e5bd074b4852f7a2419f518,

Attack Name	TYPE	VALUE
Phemedrone Stealer	SHA256	1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415, b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53, f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, 8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d, 9b9ba722b314febfc44919551a03dde1539f115333183c2cb5e74b8e644ba5b3, 568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322563, 5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211, d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e364d437a454b, 5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326, 40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc6d266, 3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871, 5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211, d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e364d437a454b, 5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326, 40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc6d266, 3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871
Androxgh0st	SHA256	0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef, 23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066, 59e90be75e51c86b4b9b69dcede2cf815da5a79f7e05cac27c95ec35294151f4, 6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc, bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7,

Attack Name	TYPE	VALUE
Androxgh0st	SHA256	ca45a14d0e88e4aa408a6ac2ee3012bf9994b16b74e3c66b588c7eabaaec4d72, dcf8f640dd7cc27d2399cce96b1cf4b75e3b9f2dfdf19cee0a170e5a6d2ce6b6, de1114a09cbab5ae9c1011ddd11719f15087cc29c8303da2e71d861b0594a1ba
	SHA1	06641b9b3b5088c48c7660ad3bf160bc87a929fd, 7d1beb03c32db43f5edd4c28f3c905954e40dbd6, 59ce7486745b08d1adba49f2413133c441194986, 79d3143a47dc02768ff5fda8dbcf464c5cdf115b, 09bd9b17a64b20ba66582dbc3ce08169697177a8
	MD5	95f745a5db131b1ca34e44848fd52edb, 3fae93618edffe4331d18d8b8e6df693, c1070aca9fcff4a32934e6c8aee4ea48, 9039ae16e5aaa63d9ffe88dfaf0f5108, fe53c38f61588efd90af97185e315612, 62a06bea8c6e276b5e532944cfc863e5, 6e793efe40e355643423f53de43952d3, 1fb78440dc44b0900b27260a16d9771e
WasabiSeed	SHA256	29e447a6121dd2b1d1221821bd6c4b0e20c437c62264844e8bcbb9d4be35f013, 292344211976239c99d62be021af2f44840cd42dd4d70ad5097f4265b9d1ce01
	URL	hxxp[:]//109[.]107.173.72/%serial%
Screenshotter	SHA256	02049ab62c530a25f145c0a5c48e3932fa7412a037036a96d7198cc57cef1f40, d0a4cd67f952498ad99d78bc081c98afbef92e5508daf723007533f000174a98, 6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc, 322dccd18b5564ea000117e90dafc1b4bc30d256fe93b7cfd0d1bdf9870e0da6
	URL	hxxp[:]//109[.]107.173.72/screenshot/%serial%
Zloader	URLs	hxxps://adslstickerhi[.]world, hxxps://adslstickerni[.]world, hxxps://dem.businessdeep[.]com

Attack Name	TYPE	VALUE
Zloader	SHA256	038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55, 16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d, 25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d, 2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456, 83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3, 98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2, adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa, b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93, b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378, d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d, eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499, f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb, f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8, fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616, fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75
RokRAT backdoor	SHA256	79c9f770470510034e29ef80d8d7e894ba65bdbff5bdf603c31559b1f0ab67fd, 1fb020554ae92ddc57622e53f61b05cfeab901ed8c4ca80af015eeff7ef59c8e, 48358a167e2697c6c86086505e714f4bc32655fecf59f97d3d34a13f93091e67, 67dd5d076d301e61256bb0558d23c118a71491081a019a88a7aab54c13084af6, 54ea66fc97a35c8bc37bff02bb8c94c28449fe7ee53d6bdb0310a5c5a569d2e7, 3f8ec06a3777d3732c340fe349b922f878ce3a5d9a86938574c7a041e2964b3c, 05024d1e718e904713053563c4ec11dddde928d7e53555c58d54163417e11854, 77f03d83db91b777be49e2badd1be0f4b085bb1c7c1b227dd65bdead4dd54ae6

Attack Name	TYPE	VALUE
NS-STEALER	SHA256	85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10, 3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4, 3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f, 9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113, 3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83, eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224, 89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e, bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1
Kasseika ransomware	SHA256	8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7, 63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196, 3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa, cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37, c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0
AsyncRAT	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa,

Attack Name	TYPE	VALUE
AsyncRAT	SHA256	124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99
VenomRAT	SHA256	22101f7ae824387a41052dfc0891096efb5ab47859727131465eeadcc1412a58, cd5a8de963a29d07bb003a8d03fa7ba38e5004641fe8138885c967db46bef0fc, 5b11f30be6e3bfb808c25d07b492cfa12840fd0efa795d8af397feba045d1c59
AllaKore RAT	SHA256	13d88bcf312896fae6d03d59c564bc9521e0916096098cfe41508395955aab0e, 168ac972b7f0610f978e50b426e39938f889422b1bcfaf9cddf518e3e1ed9aa9, 2ff3cdb886b1caf3eaad9a2467bfa16b9269b88695b76bb6a0da481458e30aa3, 305cde85573131949fab5a3973525a886962c4f8c02558d3a215689a49f53406, 33578228c11ad0b3d86a198a32b602aa93a91d2feeae2fb2e83f8c6595c8acd9, 422c9471c29fe17457e142df1a567c273212019eb20b0b4783891c529c1248a8, 46c14c2f0d04710f53db16473877d3315c13e1a33a3236846a87e8f91808c8eb, 49a04f31e49cee3ae65e9d776bc0f8aedf40c52fafcd002ccf7de4044abec2dd, 52134d02cd77f8a65fd5b15c7c57ff2909ac39f0b5779592c533a18bf6b23879, 5961b42f8efad58c437bdad862a0337c6bcd57f7cbf35184f2de60f4609fd477, 673d4fe6f9e46fae37649c525f1d0d89cfd3b8310210dff4ddc7349418d9e80f, 6d516a96d6aa39dd9fc2d745ea39658c52ab56d62ef7a56276e2e050d916e19f, 89206ca169747d4aa70d49350415f21df7f1a00a3bf8d0c253b6beda2eb919d9, 8fce1d24cf952528169f473b9462724482511615ed31165710e5e3a74cefdd02, 911e45d053bdf3a41e812203ae29db739cf3505a4e37209936c1cc83ee42e8e9,

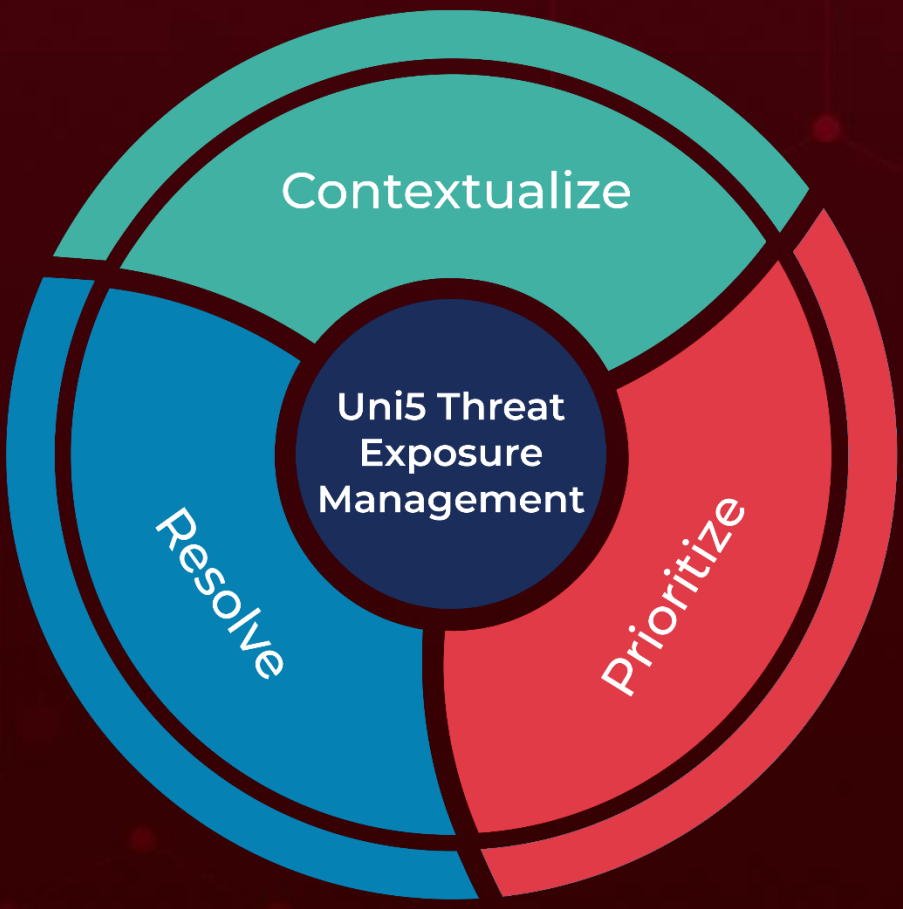
Attack Name	TYPE	VALUE
AllaKore RAT	SHA256	9221470c77b46bcd457951ae3a3d31d60ad4602ea9d152d51d1e4f9a5b3bca3a, a5af60355c423fa4cc9695b86a5697f847259eaee724065162d303cc4523d447, b858d451804a641fc51dd6d3c50668d6a08dc9033252aee52f582264a970cff8, bc423bd9acd7c5a1f2849091f21de5429f2fc79e2655f92866e1c8b7b1f96f7e, c778739c5214aa580cba05f01afe2d9fc8f12d3fa7ad864a279bcb4ad6d266b4, cde045a0269a5a05928128c6ca7c030947f96034c9204e2b747a0d626e3f22f3, e2d82ab6cc71a1d8d2a2ba2312b0d8a4a3d23e3902d5b180383d9e406097a9ff, ee772e1260c6adc532bed57cacdbb6e0b8db311996074ad42eaf1aefd243187a, eecc201c80809b636d945aa537b954dd2e39382c36067a040a672167a1257a09, fba031543c3ab694a09e603a7df6417f93742f0b87f9fedaf9ab84d11340ccb5, fd8c49d00effa8bc730e06ae217655a430ba03122ca974945d41642299853dfa
Cherry Loader	SHA256	8c42321dd19bf4c8d2ef11885664e79b0064194e3222d73f00f4a1d67672f7fc
PlugX	SHA256	d6a4bc7940f98b926b66fed5d3cb1a444c527d02c906beabd53856022edd4f4a, 7df1864afc8dfee93722735a7512b748e2b1ddd8f0701275fe0c9798fd14400c, 4d0f6cce0e423a96ff3b76a8e41bca9e3bb97ff0f78d57fe45494b97415c2dfe, e42ba4c493d6841f24667db5c1c6ad9a0107833e5a27d930e2ce454d6194b9d0, 0b81b33d24ad693be288a9a14a091210b90c8d8ba20b9b205c52e66b50728050, c79550db4bc421bc8d5ed5db6dc9f608724f6934a41f5501333bde78f731ecb2, a54b3c1cfd65f351c9eb28cb293d338598267a8923c7f447a7e4244eb374238a, 9da62b3d6805d77c13cc58bbcbfcbe51cb1b95b956654082fdf26828756b7e00, c0545f119cea422f092a3c358a3ce4888d212ccb7531bf161c8f4fa46d97a587, ee82542d12b1620add9191bb3dbd947192ee900cb9f3d16dc36b346e76361fe5,

Attack Name	TYPE	VALUE
PlugX	SHA256	149b86e1877fa6f7600c4154be07b2fc90b9ee30e988d8f2f67130069d6fd80e, a281d5e93518d3a0e6e83f2874297389aec4d42ece26b358623e902cd1959189, bf0bfdf017bdce9ba2359784a42c4ce7ee3e1a6ce47716e0b31c40be8c61e18a, 405bac66c665f2ffe99811b1b73716d663e91f93a9dd469eb361df63da4c1ee3, 9c4c4c770a018612b780162bd046fd713e6347a72a5176ed0ee3e51b11823534, d8d59353d0e19957cd4cce5102dff5b706ed9c412db6b8778b3ea4726b2429b3, 72120bf8bf604bc1f1aa455b22d3df431cc95836306fab186cd64da53527a274, 503e7059334032bfa50ba878f0992a3b909952d380fc9757949c43109973ede7, 2dc28b596c37dac4771a628ae5c67de9e77f528e309b0972f4360cacd3171680, 096ab2d8480196d6e16de70d9698f2cf9e1c0eff906e5e3bbd13dd2251c858f1, 0af8058a65750350c95ac26df850a9a2505d2098414f54bfa1a289cd93f746f5, dbf692a521ff5c28e2ca25afa0b37bdcec77177a7ba8f27086708b4806a670e4, 4ed7053705a49a742ed3034da2fc834d9790e63d10c4162175dcb9f6b7715451
Gh0st RAT	SHA256	954337ceb86b9aec6dcd3a09ec713161281c8ac78dbc8c68ee94747e89dcff3f, 4adb1fb761af827cea1bc674dd08b572ac5af7bc8d441e022d557430b167cb67, 21c3b30041dc16f6fb0fe758c4cd1767e272133ff45dd21aee22506e6d9199aa, 83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6
FAUST ransomware	SHA256	426284b7dedb929129687303f1bf7e4def607f404c93f7736d17241e43f0ab33, 50e2cb600471fc38c4245d596f92f5444e7e17cd21dd794ba7d547e0f2d9a9d5, a0a59d83fa8631d0b9de2f477350faa89499e96fd5ec07069e30992aaabe913a, ebe77c060f8155e01703cfc898685f548b6da12379e6aefb996dbcaac201587c, c10dc2f6694414b68c10139195d7db2bb655f3afdcc1ac6885ef41ef1f0078df

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

February 6, 2024 . 2:30 AM

More at www.hivepro.com