Date of Publication
March 19, 2024

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

11 to 17 MARCH 2024

Table Of Contents

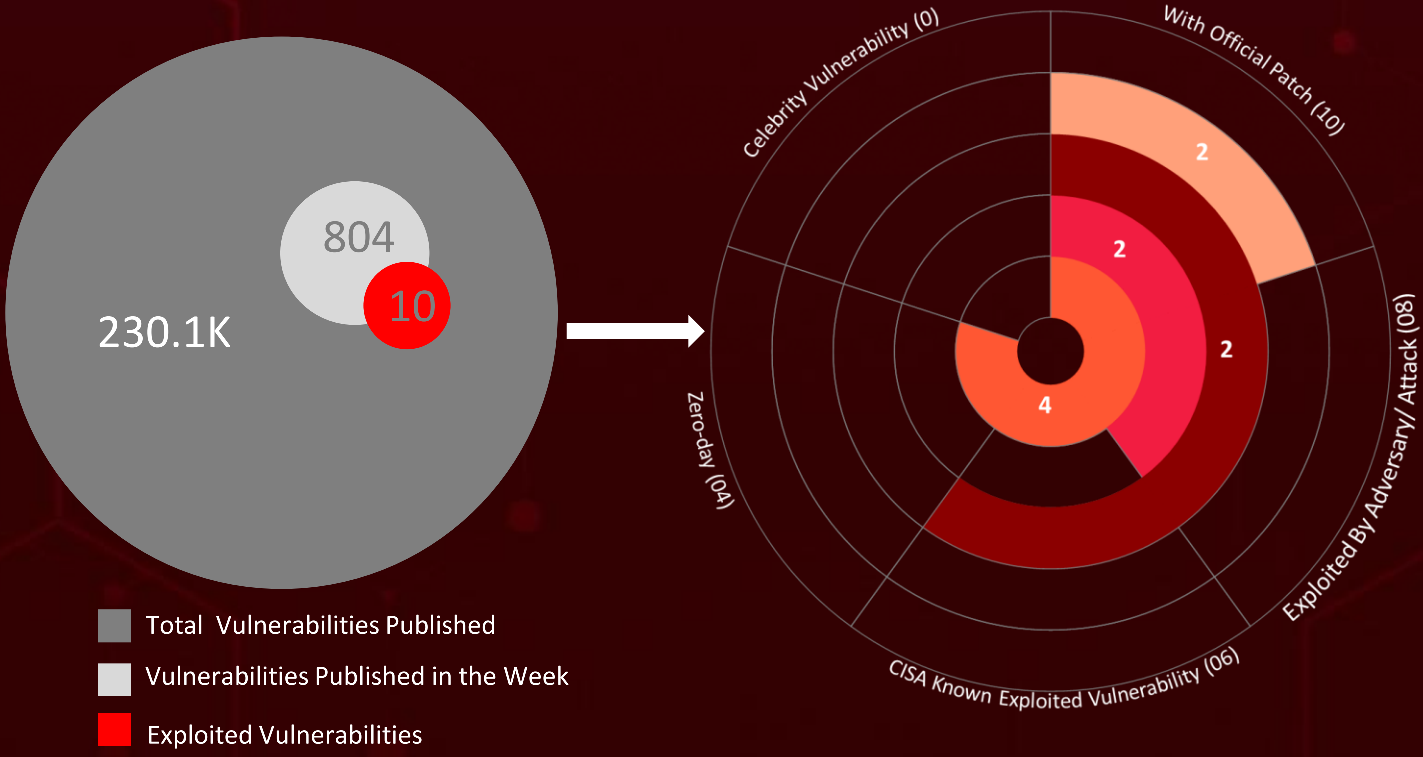
Summary

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

Furthermore, HiveForce Labs' discovered threat actor dubbed **Magnet Goblin**, known for its financial incentives, strategically exploits zero-day vulnerabilities within publicly accessible services. It achieves this by employing sophisticated malware sourced from the **Nerbian** family, which includes **NerbianRAT** and **MiniNerbian**.

Evasive Panda, a notorious threat actor group, has orchestrated an intricate cyberespionage campaign targeting Tibetan users since at least September 2023. This operation employs both watering hole and supply chain attacks to achieve its objectives.

A sophisticated phishing campaign is targeting personnel in various sectors, with the intent of distributing **VCURMS** and **STRRAT** RATs. High-severity vulnerabilities have been discovered in **Cisco**, **WordPress**, and **Fortinet**. These attacks are on the rise, posing a significant and immediate threat to users worldwide.



High Level Statistics

8

Attacks Executed

- MgBot
- Nightdoor
- VCURMS
- STRRAT
- TimbreStealer
- NerbianRAT
- WARPWIRE
- MiniNerbian

10

Vulnerabilities Exploited

- CVE-2024-20337
- CVE-2023-46805
- CVE-2024-21887
- CVE-2022-24086
- CVE-2023-41265
- CVE-2023-41266
- CVE-2023-48365
- CVE-2024-21888
- CVE-2024-21893
- CVE-2024-2194

2

Adversaries in Action

- Evasive Panda
- Magnet Goblin

Insights

Locking Down Loopholes: Microsoft's Patch Tuesday Shields Against 60 Flaws

Inside the Mind of Evasive Panda: Targeting Tibetan Users Since 2023

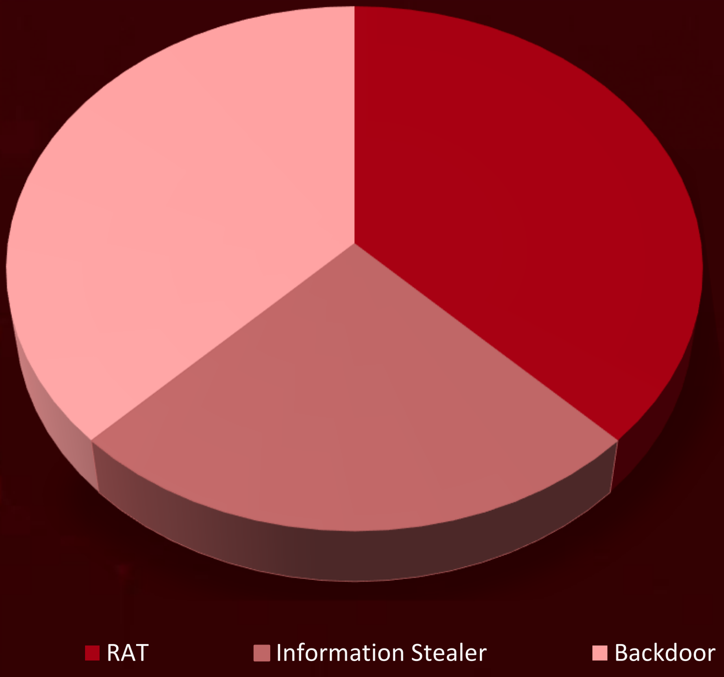
The Trojan's Gateway: How a Click Could Spell Disaster with VCURMS and STRRAT

Click with Caution: The Adobe Reader Infostealer Prowling in PDFs

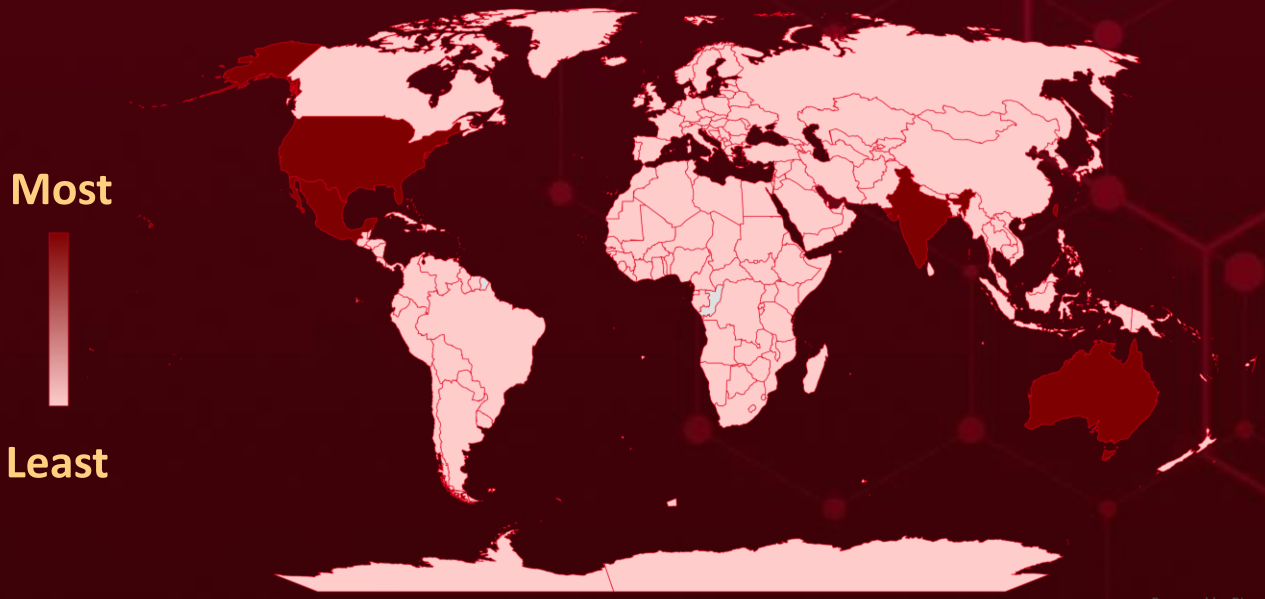
Money Talks: Magnet Goblin's Hunt for Zero-Day Vulnerabilities and its Strategic Malware Tactics

Breaking Point: Cisco's **CVE-2024-20337** Vulnerability Threatens VPN Security

Threat Distribution



Targeted Countries



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

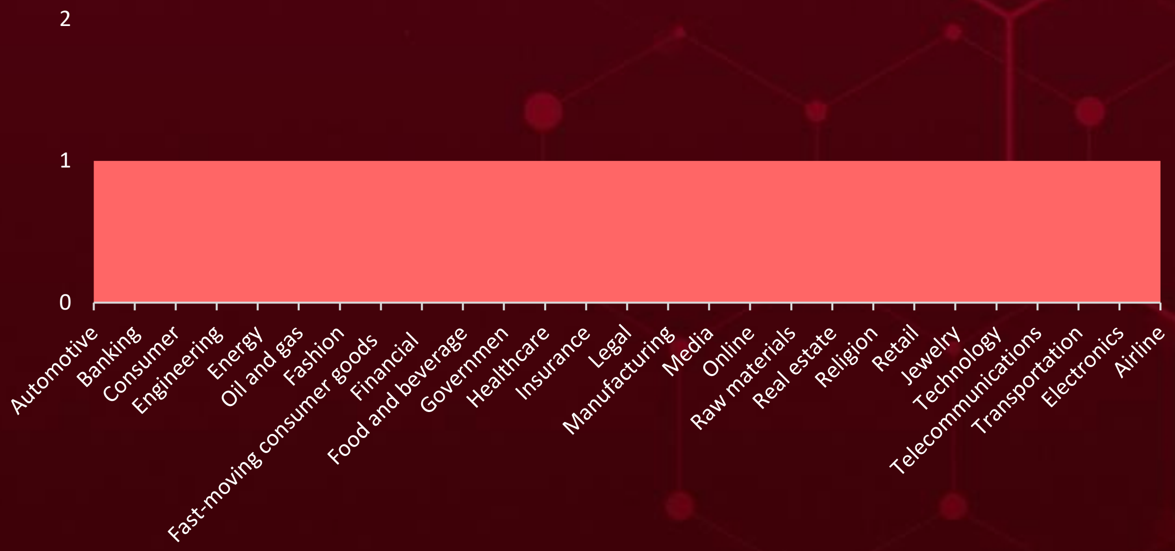
	Countries
■	India
■	Hong Kong
■	Mexico
■	Australia
■	USA
■	Taiwan
□	Lebanon
□	Saint Lucia
□	New Zealand
□	American Samoa
□	Switzerland
□	Andorra
□	Mauritius
□	Angola
□	Papua New Guinea
□	Anguilla
□	Slovenia
□	Antarctica
□	United Kingdom
□	Antigua and Barbuda
□	Madagascar
□	Argentina
□	Morocco
□	Armenia
□	Northern Cyprus
□	Aruba
□	Qatar

	Countries
□	Ashmore and Cartier Islands
□	Senegal
□	Afghanistan
□	South Sudan
□	Austria
□	Turkmenistan
□	Azerbaijan
□	Wallis and Futuna
□	Bahamas
□	Liechtenstein
□	Bahrain
□	Mali
□	Bangladesh
□	Monaco
□	Barbados
□	Nauru
□	Belarus
□	Niue
□	Belgium
□	Pakistan
□	Belize
□	Pitcairn Islands
□	Benin
□	Saba
□	Bermuda
□	Samoa
□	Bhutan

	Countries
□	Singapore
□	Bir Tawil
□	South Africa
□	Bolivia
□	Sudan
□	Bonaire
□	Transnistria
□	Bosnia and Herzegovina
□	U.S. Virgin Islands
□	Botswana
□	Vanuatu
□	Bouvet Island
□	Zimbabwe
□	Brazil
□	Liberia
□	British Indian Ocean Territory
□	Luxembourg
□	British Virgin Islands
□	Malaysia
□	Brunei
□	Marshall Islands
□	Bulgaria
□	Micronesia
□	Burkina Faso
□	Montenegro
□	Burundi

	Countries
□	Myanmar
□	Cambodia
□	Netherlands
□	Cameroon
□	Niger
□	Canada
□	North Korea
□	Cape Verde
□	Norway
□	Cayman Islands
□	Palestine
□	Central African Republic
□	Peru
□	Chad
□	Portugal
□	Chile
□	Russia
□	China
□	Saint Helena, Ascension and Tristan da Cunha
□	Christmas Island
□	Saint Pierre and Miquelon
□	Clipperton Island
□	São Tomé and Príncipe

Targeted Industries



TOP MITRE ATT&CK TTPs

T1588.006
Vulnerabilities

T1059
Command and Scripting Interpreter

T1566
Phishing

T1140
Deobfuscate/ Decode Files or Information

T1588
Obtain Capabilities

T1204
User Execution

T1036
Masquerading

T1027
Obfuscated Files or Information

T1082
System Information Discovery

T1041
Exfiltration Over C2 Channel

T1190
Exploit Public-Facing Application

T1071.001
Web Protocols

T1588.005
Exploits

T1560
Archive Collected Data

T1105
Ingress Tool Transfer

T1566.001
Spearphishing Attachment

T1498
Network Denial of Service

T1071
Application Layer Protocol

T1083
File and Directory Discovery

T1033
System Owner/User Discovery

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>MgBot</td><td rowspan="5">MgBot is a modular backdoor malware framework that is actively maintained and equipped with various plugins, allowing attackers to gather extensive information from compromised machines, indicating that the attackers' primary objective was information-gathering.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise, Information theft</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Evasive Panda</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">34395ced1d44af75c510c6709bff51c94417558304daff35a9d07c8e628d6624,
ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024,
2500aa8729f9e82765443141111614c73867f162c28b2e2283749bc208ad9e70</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Nightdoor</td><td rowspan="6">The Nightdoor backdoor talks with its C&C server via UDP or the Google Drive API. Each message sent between Nightdoor and the C&C server is stored as a file.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">System Compromise, Information theft</td><td rowspan="2">-</td></tr>
<tr><td>Backdoor</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Evasive Panda</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA1</td><td colspan="3">7a3fc280f79578414d71d70609fbdb49ec6ad648,
70b743e60f952a1238a469f529e89b0eb71b5ef7,
59aa9be378371183ed419a0b24c019ccf3da97ec</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">VCURMS</td><td rowspan="8">VCURMS bears similarities to another Java-based infostealer called Rude Stealer. This similarity encompasses the ability to execute arbitrary commands, gather system data, search and transmit files of interest, and acquire additional information stealer and keylogger modules from the same AWS endpoint.</td><td>Phishing</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="6">Information theft, Espionage</td><td rowspan="2">AWS and GitHub</td></tr>
<tr><th>TYPE</th></tr>
<tr><td rowspan="2">RAT</td><th>PATCH LINK</th></tr>
<tr><td rowspan="3">-</td></tr>
<tr><th>ASSOCIATED ACTOR</th></tr>
<tr><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">STRRAT</td><td rowspan="7">STRRAT, also a Java-built RAT, has been observed in the wild since 2020, frequently propagated through deceptive JAR files.</td><td>Phishing</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="5">Information theft, Espionage</td><td rowspan="3">AWS and GitHub</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>RAT</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">97e67ac77d80d26af4897acff2a3f6075e0efe7997a67d8194e799006ed5efc9,
8d72ca85103f44742d04ebca02bff65788fe6b9fc6f5a411c707580d42bbd249,
38a74520d86f5dd21bf5c447c92a9e5c0c3f69db84b1666e33d5d86784bead3a</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">TimbreStealer</td><td rowspan="6">TimbreStealer is an advanced malware designed to Collect credential information from the victim’s machine, Search for Files, Collect OS information, Search for file extensions, Look for URLs Accessed, Disable System Protections, Look for Remote Desktop Software, POST data to remote site.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Information theft, System Compromise</td><td rowspan="2">-</td></tr>
<tr><td>Information Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

IOC TYPE	VALUE
SHA256	e87325f4347f66b21b19cfb21c51fbf99ead6b63e1796fcb57cd2260bd720929, 103d3e03ce4295737ef9b2b9dfef425d93238a09b1eb738ac0e05da0c6c50028, a579bd30e9ee7984489af95cffb2e8e6877873fd881aa18d7f5a2177d76f7bf2

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
NerbianRAT	NerbianRAT was first publicly disclosed in 2022. NerbianRAT stands as a versatile remote access trojan (RAT), customized for both Windows and Linux environments, accompanied by MiniNerbian, a compact yet potent Linux-based backdoor.	Exploiting Vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893
		IMPACT	AFFECTED PRODUCTS
TYPE		Espionage, Financial Gains	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
RAT			
ASSOCIATED ACTOR			PATCH LINK
Magnet Goblin			https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US, https://helpx.adobe.com/security/products/magento/apsb22-12.html, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510, https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

IOC TYPE	VALUE
SHA256	027d03679f7279a2c505f0677568972d30bc27daf43033a463fafeee0d7234f6, 9cb6dc863e56316364c7c1e51f74ca991d734dacef9029337ddec5ca684c1106

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
WARPWIRE	WARPWIRE, a JavaScript-based credential theft tool further enables access to accounts for lateral movement or espionage by capturing plaintext login credentials.	Exploiting Vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Information theft, Espionage, Financial Gains	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
ASSOCIATED ACTOR			PATCH LINK
Magnet Goblin			https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US, https://helpx.adobe.com/security/products/magento/apsb22-12.html, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510, https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

IOC TYPE	VALUE
SHA256	1079e1b6e016b070ebf3e1357fa23313dcb805d3a6805088dbc3ab6d39330548, e134e053a80303d1fde769e50c2557ade0852fa827bed9199e52f67bac0d9efc

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
MiniNerbian	MiniNerbian, a compact yet potent Linux-based backdoor. MiniNerbian is a simplified version of NerbianRAT, which has one main functionality which is command execution.	Exploiting Vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Espionage, Financial Gains	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US, https://helpx.adobe.com/security/products/magento/apsb22-12.html, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801, https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510, https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure
Magnet Goblin			

IOC TYPE	VALUE
SHA256	d3fbae7eb3d38159913c7e9f4c627149df1882b57998c8acaac5904710be2236, df91410df516e2bddfd3f6815b3b4039bf67a76f20aecabccffb152e5d6975ef, 99fd61ba93497214ac56d8a0e65203647a2bc383a2ca2716015b3014a7e0f84d

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20337	⊗	Cisco Secure Client: 4.10.04065 - 5.1	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:anyconnect_secure_mobility_client cpe:2.3:a:cisco:secure_client	-
Cisco Secure Client Carriage Return Line Feed Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-93	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/series.html#~tab-downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46805	✗	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	Magnet Goblin
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	Magnet Goblin
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-24086	✗	Adobe Commerce and Magento Open Source	Magnet Goblin
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:*:*:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Adobe Commerce and Magento OpenSource Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow	https://helpx.adobe.com/security/products/magento/apsb22-12.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41265	✗	Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise Privilege escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1068: Exploitation for Privilege Escalation	https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41266	✗	Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise path traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1005: Data from Local System, T1222: File and Directory Permissions Modification	https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48365	✗	Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise remote code execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1059: Command and Scripting Interpreter	https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21888	✗	Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x	Magnet Goblin
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21893	✗	Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x	Magnet Goblin
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy, T1135: Network Share Discovery, T1005: Data from Local System	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-2194	⊗	WordPress WP Statistics Plugin all versions up to 14.5	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wp_statistics_plugin:wp_statistics_plugin:14.0:*:*:*:*:*:*:*	-
WordPress WP Statistics plugin Cross-Site Scripting Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by Compromise, T1204.001: Malicious Link	https://wordpress.org/plugins/wp-statistics/

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Evasive Panda (aka Daggerfly, Bronze Highland)	China	All	India, Taiwan, Hong Kong, Australia, USA
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MgBot, Nightdoor	Windows and macOS
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.004: Server; T1583.006: Web Services; T1584.004: Server; T1585.003: Cloud Accounts; T1587.001: Malware; T1588.003: Code Signing Certificates; T1608.004: Drive-by Target; T1189: Drive-by Compromise; T1195.002: Compromise Software Supply Chain; T1106: Native API; T1053.005: Scheduled Task; T1543.003: Windows Service; T1574.002: DLL Side-Loading; T1140: Deobfuscate/Decode Files or Information; T1562.004: Disable or Modify System Firewall; T1070.004: File Deletion; T1070.009: Clear Persistence; T1036.004: Masquerade Task or Service; T1036.005: Match Legitimate Name or Location; T1027.009: Embedded Payloads; T1055.001: Dynamic-link Library Injection; T1620: Reflective Code Loading; T1087.001: Local Account; T1083: File and Directory Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1049: System Network Connections Discovery; T1560: Archive Collected: Data; T1119: Automated Collection; T1005: Data from Local System; T1074.001: Local Data Staging; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1571: Non-Standard Port; T1572: Protocol Tunneling; T1102: Web Service; T1020: Automated Exfiltration; T1567.002: Exfiltration to Cloud Storage			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">Magnet Goblin</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Financial Gain</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>CVE-2023-46805
CVE-2024-21887
CVE-2022-24086
CVE-2023-41265
CVE-2023-41266
CVE-2023-48365
CVE-2024-21888
CVE-2024-21893</td><td>NerbianRAT, WARPWIRE, MiniNerbian</td><td>Ivanti, Magento, Qlink Sense, and Apache ActiveMQ</td></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1041: Exfiltration Over C2 Channel; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1573.001: Symmetric Cryptography; T1071.001: Web Protocols; T1573: Encrypted Channel; T1071: Application Layer Protocol; T1588.006: Vulnerabilities; T1588.001: Malware; T1105: Ingress Tool Transfer</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **Evasive Panda, Magnet Goblin,** and malware **MgBot, Nightdoor, VCURMS, STRRAT, TimbreStealer, NerbianRAT, WARPWIRE, MiniNerbian.**

Uni5 Users

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

- Running a Scan to discover the assets impacted by the **ten exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Evasive Panda, Magnet Goblin,** and malware **TimbreStealer, NerbianRAT, and Mini Nerbian** in Breach and Attack Simulation(BAS).

Threat Advisories

[Evasive Panda China-Linked Cyberespionage Targeting Tibetans]

[Cisco Secure Client Flaw Enables Attackers To Steal VPN Sessions]

[Microsoft's March 2024 Patch Tuesday Addresses 60 Vulnerabilities]

[VCURMS and STRRAT Trojans Using AWS and GitHub as Launchpads]

[Malware Concealed Within PDFs for Data Theft]

[Fortinet Releases Patches for Critical Vulnerabilities in Various Products]

[TimbreStealer Focuses On Mexico With Social Engineering]

[Magnet Goblin Strikes Public-Facing Servers]

[Critical XSS Flaw Discovered in WP Statistics Impacting 600K Sites]

[Cisco IOS XR Flaws Enable Privilege Elevation and DoS Attacks]

Appendix

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

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
MgBot	SHA256	34395ced1d44af75c510c6709bff51c94417558304daff35a9d07c8e628d6624, ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024, 2500aa8729f9e82765443141111614c73867f162c28b2e2283749bc208ad9e70, a4387c36bf1a150ac3a0f6d7a3ea55170fe63e772dac41ca0bc0b775a968498a, ab9c9017e53be3382867562915a2082cb4b3fdedc624a20d2dac584cb714c8d1, 00e9025b7353e427cdd0c090859ce5bd2c51a94f8f30d9a017c50c5360cc0467, 15400a1d426333b9463f425e44af721c1005962ac245df40d63c5995524d4434, 2b479ea7e5433c25905e872b8a397fb9c9cab9a9a5b02a636f2f507f55446dd1, 22a7a71608d99c76caf05a3212eb724c0cda6a40f84059fbbfe313a11448c66e, 8a9b2dadd7643cf02a4fe4ad9c6adca2f2eba158f3c3f6853f60ee6f8a789ecb, 43a9db4a84fb27d942a67a7aac15c2d5d4ed1598d73830558f5ac072b4bd9c36, 40e34f73c1efb1de8760e0fb6af044b81fa89ff1de44e0b7e3eb8f7b51ca623a

Attack Name	TYPE	VALUE
Nightdoor	SHA1	7a3fc280f79578414d71d70609fbdb49ec6ad648, 70b743e60f952a1238a469f529e89b0eb71b5ef7, 59aa9be378371183ed419a0b24c019ccf3da97ec, 8591a7ee00fb1bb7cc5b0417479681290a51996e, 82b99ad976429d0a6c545b64c520be4880e1e4b8
	Filename	pidgin.dll, memmgrset.dll, default_ico_1.exe, UjGnsPwFaEtl.exe, default_ico.exe
STRRAT	SHA256	97e67ac77d80d26af4897acff2a3f6075e0efe7997a67d8194e799006ed5efc9, 8d72ca85103f44742d04ebca02bff65788fe6b9fc6f5a411c707580d42bbd249, 38a74520d86f5dd21bf5c447c92a9e5c0c3f69db84b1666e33d5d86784bead3a, 2743fa7e35da259564a4f879b20487577921a3e669d6deb3fa5cca3193f73952, 7ccc38e2616bfb5aef446213a4cab27cffd99e91ba1e035857344a8d5c9454b3, 595ab2d1b7478b6c6a18fec3698cb131d8115c346b0408c6667aa6561a443c2b, 7aabe909ac93d7930bc1195f092cd2f0fb7ca8dbbb543e4a3d442f6bb13121a0, 1d3219b6ccc538b8cbecb13eb9c23ce00a6ed315a2a7fecb9b791e9cd1888bd8, a36323cc7633934af9b10f0c56841e483bb886836ca94fc52ce37ca3f0cfd190, 8efa0e193fb08adf90ba95c2e7f2de6453c3276cd8ae154c4af117a48a668ef3, d38b806812c7610cc3349a2ec4b60b0fcf61a92295fe7eea72da2a255b204b5e, 26104fcd8de196afcbaf13b7a6aa150855ee64060ec9e9444db0448b3524cf80, 85ea19ebad6e8cebdbd3c188964228fab7512b8668633f621bf0d660b8f92a33
TimbreStealer	SHA256	e87325f4347f66b21b19cfb21c51fbf99ead6b63e1796fcb57cd2260bd720929, 103d3e03ce4295737ef9b2b9dfef425d93238a09b1eb738ac0e05da0c6c50028, a579bd30e9ee7984489af95cffb2e8e6877873fd881aa18d7f5a2177d76f7bf2, 010b48762a033f91b32e315ebcefb8423d2b20019516fa8f2f3d54d57d221bdb,

Attack Name	TYPE	VALUE
TimbreStealer	SHA256	024f3c591d44499afb8f477865c557fc15164ab0f35594e0cfdfa76245459762, 03cd17df83a7bdf459f16677560e69143d1788ce1fc7927200a09f82859d90ea, 075910c802f755d3178a8f1f14ee4cd7924fd4463c7491277bdf2681b16e593c, 12bff33da7d9807252bb461d65828154b9b5b1dca505e8173893e3d410d40dd0, 1aaa4fb29a88c83495de80893cd2476484af561bb29e8cdfc73ce38f6cd61a84, 23b9e4103141d6a898773b1342269334e569bcf576cdcb4a905f24e26320cdab, 27c1e41fde9bc0d5027a48ccada1af8c9c8f59937bf5f77edd21e49bd28f29a2, 2a225784289f31adbaa8be0b8770495fa8950fce2b7352a0c7a566fc79067547, 2a38b75e88f91f9cd28ef478e82c3b44f50e57cb958ba63e58f134d8bd368812, 2a3f869e9e78b4d7945a60ceec27586c07bc8b0770be64463358fffe3b6b7395, 2e04c36b7ddd6939b7bef258bfeba6f91a5c37a43389dd6d9a88eff5863df5ed, 43e99539e4b966dde2f9de8dc1ffb4a22bc560e54c01de9aef6b15fac1412714, 46226d4fb7ffe15ba8167e3724f991c543731672e19ef40bb43fddc6df648d0a, 46cc07a9287da26e238a74734d87e0aae984f4648a80a26547afa0de8c850afb, 51be3a3b4ebd15c305c0f9b57388c449f88f0d6d2d46a0a838f046f0fd21b78f, 55b0247b9b574978a4c9abd19c3bcc04ea78598398b9f8aeb35bd51cbd877576, 56612bb0ab00cbb7af24326b027a55ff25852ddab1f1c8e24471b7ce97003505, 5831f4f8ce715d4a021284e68af1b6d8040a2543484ac84b326eea20c543552e, 58562e49c1612f08e56e7d7b3ca6cd78285948018b2998e45bd425b4c79ce1f4, 62495620b0d65d94bc3d68dec00ffbe607eacd20ab43dc4471170aa292cc9b1a, 682546addb38a938982f0f715b27b4ba5cda4621e63f872f19110d174851c4e9, 69019b7b64deb5cc91a58b6a3c5e6b1b6d6665bd40be1381a70690ba2b305790,

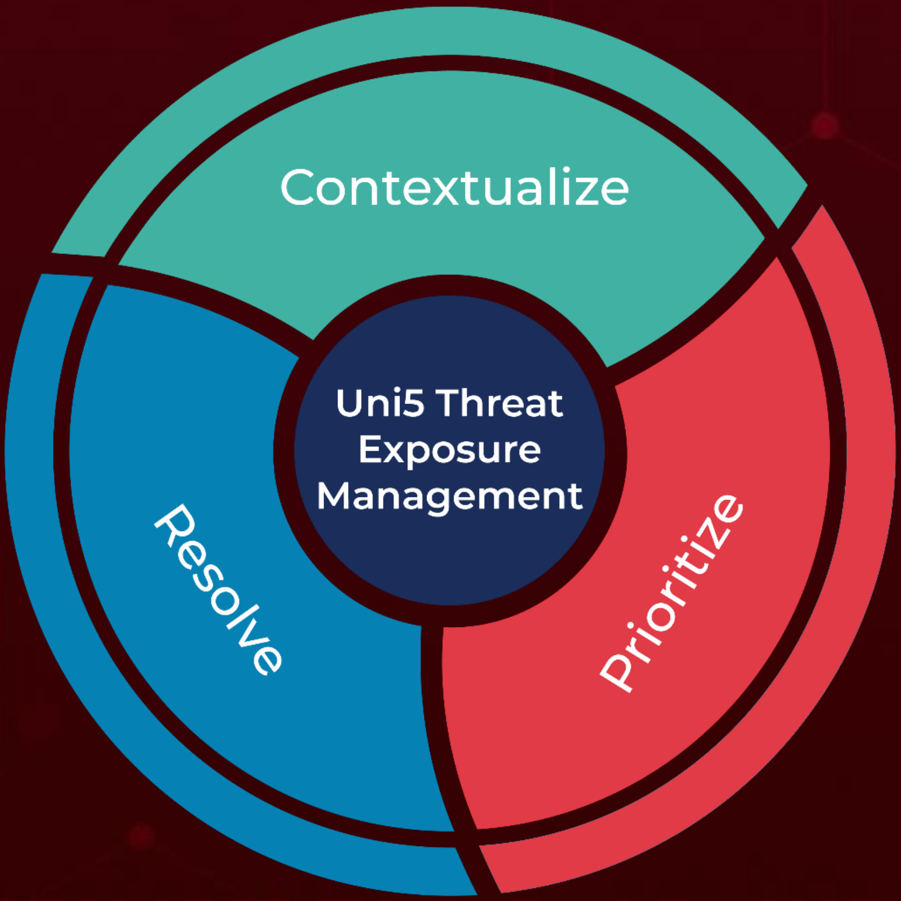
Attack Name	TYPE	VALUE
TimbreStealer	SHA256	6bf082f001f914824a6b33f9bdd56d562c081097692221fb887035e80926d583, 7923d409959acffab49dda63c7c9c15e1bdd2b5c16f7fcfe8ef3e3108e08df87, 7ac22989021082b9a377dcc582812693ce0733e973686b607e8fc2b52dcf181d, 8420d77ba61925b03a1ad6c900a528ecacbb2c816b3e6bc62def40fc14e03b78, 850dd47a0fb5e8b2b4358bf3aa1abd7ebaae577b6fc4b6b4e3d7533313c845b8, 96363b2b9e4ed8044cb90b6619842ba8897b4392f9025cbfdccfda1ea7a14a58, 97157c8bbeb8769770c4cb2201638d9ad0103ba2fdfed9bdbd03c53bd7a5fcb9, a103b0c604ef32e7aabb16c2a7917fd123c41486d8e0a4f43dcf6c48d76de425, a82fb82f3aa2f6123d2c0fb954ae558ac6e8862ef756b12136fbe8d533b30573, a92934c014a7859bd122717f4c87f6bd31896cb87d28c9fac1a6af57ff8110f6, ab2a2465fccd7294580c11492c29a943c54415e0c606f41e08ce86d69e254ee4, ababe815e11b762089180e5fb0b1eaffa6a035d630d7aaf1d8060bd5d9a87ea5, b04a0a4a1520c905007a5d370ed2b6c7cb42253f4722cc55a9e475ae9ece1de7, c29b9f79b0a34948bde1dfca3acecca6965795917c7d3444fcacba12f583fb98, c99237a5777a2e8fa7da33460a5b477d155cc26bc2e297a8563516a708323ead, ca652fc3a664a772dbf615abfe5df99d9c35f6a869043cf75736e6492fbd4bea, b5a272acd842154b2069b60aab52568bbfde60e59717190c71e787e336598912, ce135a7e0410314126cacb2a2dba3d6d4c17d6ee672c57c097816d64eb427735, d3ff98b196717e66213ccf009cbeed32250da0e2c2748d44f4ee8fb4f704407, febf9c5ede3964fdb3b53307a3d5ef7b0e222705a3bb39bef58e28aaba5eed28, Ff3769c95b8a5cdcba750fda5bbbb92ef79177e3de6dc1143186e893e68d45a4
NerbianRAT	IPv4	172.86.66[.]165, 45.153.240[.]73

Attack Name	TYPE	VALUE
NerbianRAT	SHA256	027d03679f7279a2c505f0677568972d30bc27daf43033a463fafeee0d7234f6, 9cb6dc863e56316364c7c1e51f74ca991d734dacef9029337ddec5ca684c1106, 9d11c3cf10b20ff5b3e541147f9a965a4e66ed863803c54d93ba8a07c4aa7e50
WARPWIRE	SHA256	1079e1b6e016b070ebf3e1357fa23313dcb805d3a6805088dbc3ab6d39330548, e134e053a80303d1fde769e50c2557ade0852fa827bed9199e52f67bac0d9efc
MiniNerbian	SHA256	d3fbae7eb3d38159913c7e9f4c627149df1882b57998c8acaac5904710be2236, df91410df516e2bddfd3f6815b3b4039bf67a76f20aecabccffb152e5d6975ef, 99fd61ba93497214ac56d8a0e65203647a2bc383a2ca2716015b3014a7e0f84d, 9ff0dcce930bb690c897260a0c5aaa928955f4ffba080c580c13a32a48037cf7, 3367a4c8bd2bcd0973f3cb22aa2cb3f90ce2125107f9df2935831419444d5276, f23307f1c286143b974843da20c257901cf4be372ea21d1bb5dea523a7e2785d, f1e7c1fc06bf0ea40986aa20e774d6b85c526c59046c452d98e48fe1e331ee4c, 926aeb3fda8142a6de8bc6c26bc00e32abc603c21acd0f9b572ec0484115bb89, 894ab5d563172787b052f3fea17bf7d51ca8e015b0f873a893af17f47b358efe

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

March 19, 2024 • 6:00 AM

More at www.hivepro.com