Date of Publication
August 5, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 July to 4 August 2024

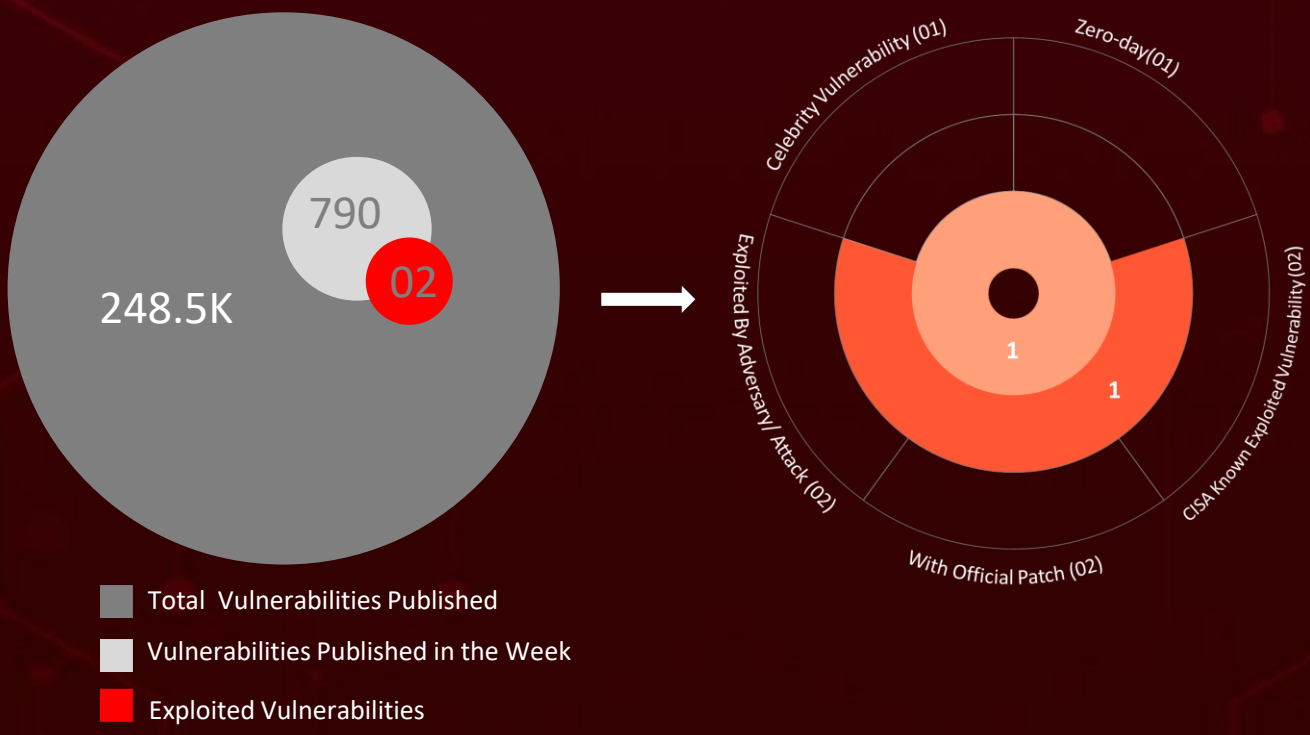
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week alone, HiveForce Labs has detected **fourteen** executed attacks, reported **two** vulnerabilities, and identified **five** active adversary. These findings highlight the relentless and escalating danger of cyber intrusions.

Additionally, multiple ransomware groups exploit **CVE-2024-37085**, an authentication bypass vulnerability in VMware ESXi hypervisors, to gain elevated permissions and deploy file-encrypting malware, despite the flaw being patched on June 25, 2024.

Furthermore, **Andariel**, a North Korean cyber espionage group since 2009, has shifted from destructive attacks to specialized espionage and ransomware, threatening global industries like critical infrastructure and healthcare. These rising threats pose significant and immediate danger to users worldwide.



High Level Statistics

14
Attacks Executed

2
Vulnerabilities Exploited

5
Adversaries in Action

- Atlantida stealer
- Rhadamanthys
- RisePro
- Lumma Stealer
- RedLine
- Akira
- Black Basta
- Babuk
- Lockbit
- Kuiper
- BeaverTail
- InvisibleFerret
- Mint Stealer
- XDSpy.DSDownloader

- CVE-2021-44228
- CVE-2024-37085

- Andariel
- Stargazer Goblin
- Scattered Spider
- Manatee Tempest
- XDSpy

Insights

Andariel group now targets critical infrastructure and healthcare with ransomware and espionage

DEV#POPPER campaign linked to North Korean threat actors, targets software developers with advanced malware and audacious social engineering tactics disguised as job interviews

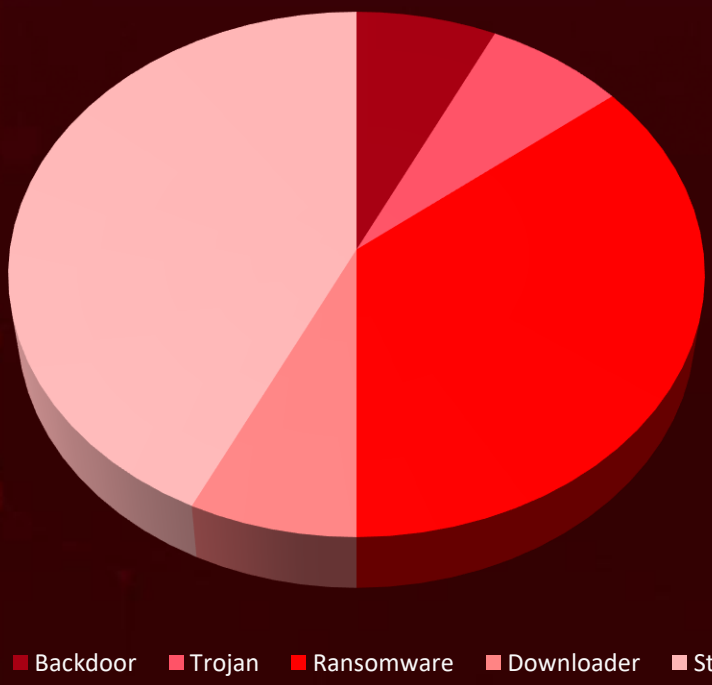
XDSpy's phishing campaign targets Russian entities, resulting in the discovery of new malware, **XDSpy.DSDownloader**

Stargazer Goblin operates the **'Stargazers Ghost Network'** on GitHub, using over 3,000 fake accounts to distribute information-stealing malware

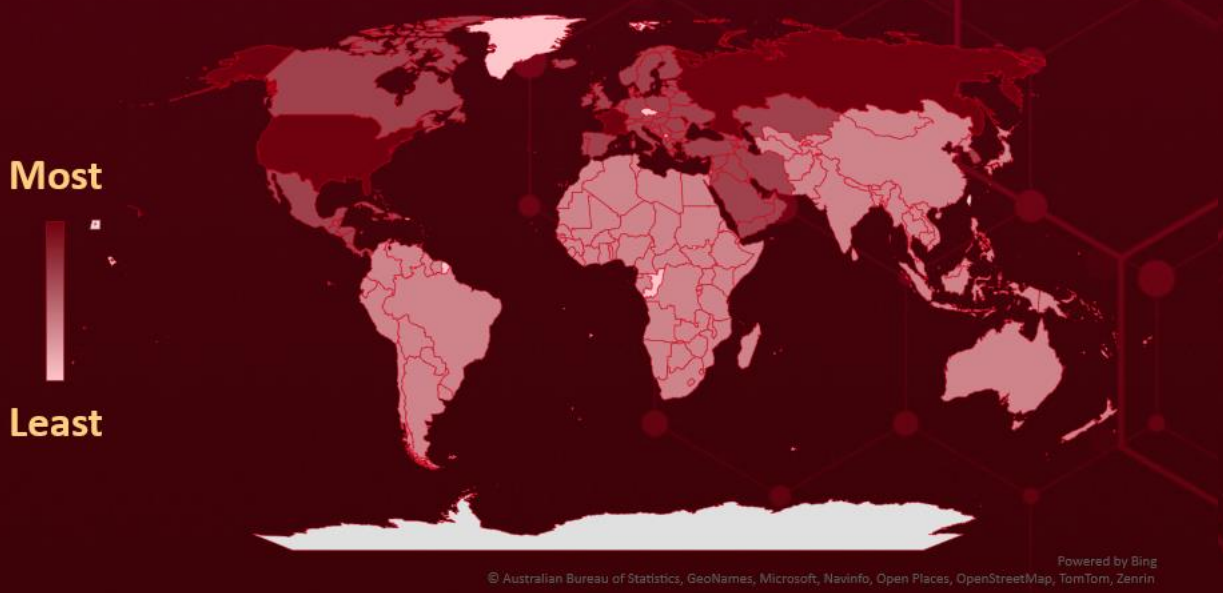
CVE-2024-37085, an authentication bypass flaw in VMware ESXi, allows ransomware groups to gain admin access and deploy file-encrypting malware, despite being patched on June 25, 2024

Mint Stealer is a Python-based info stealer that targets sensitive data and evades detection through encryption, uploading stolen information to file-sharing sites

Threat Distribution

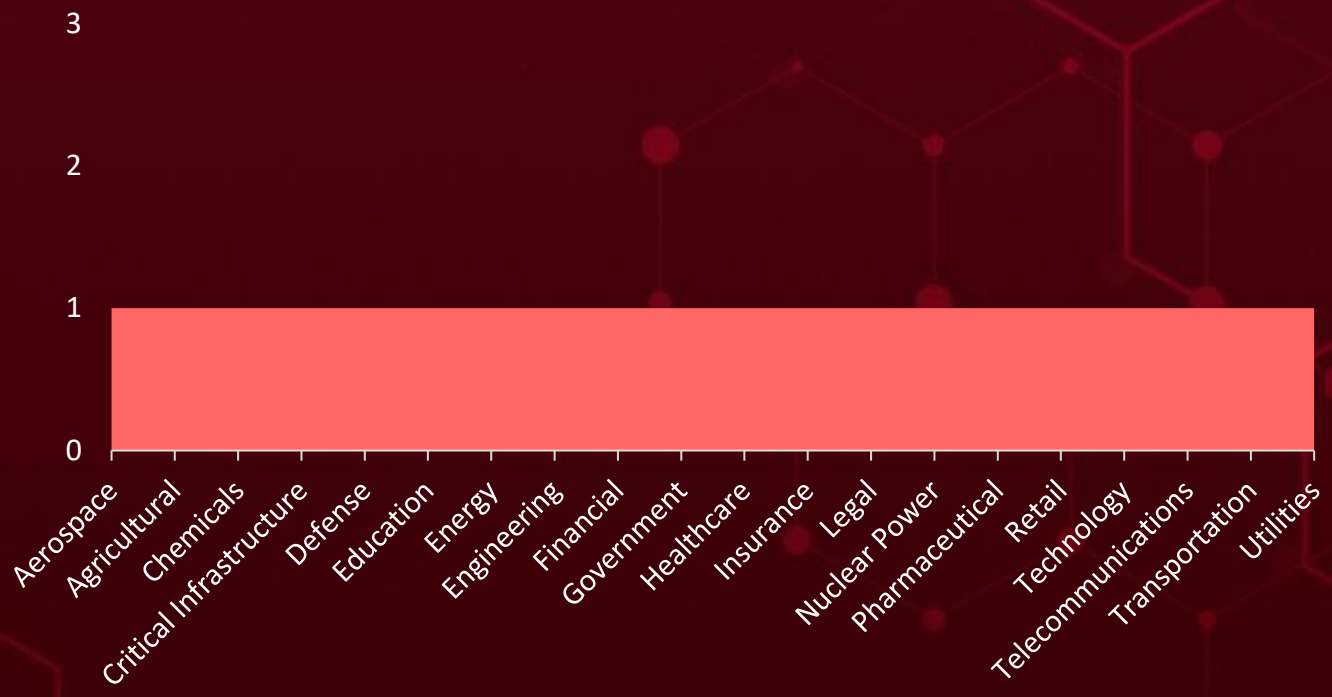


Targeted Countries



Countries	Countries	Countries	Countries
Russia	Monaco	Germany	Jordan
Moldova	Canada	Nicaragua	Italy
France	North Macedonia	Greece	Yemen
United States	Costa Rica	Norway	Samoa
San Marino	Poland	Grenada	Tunisia
Mexico	Croatia	Panama	Australia
Kazakhstan	Antigua and Barbuda	Guatemala	Angola
Austria	Cuba	Portugal	Bangladesh
Oman	Serbia	Haiti	Côte d'Ivoire
Azerbaijan	Cyprus	Romania	Singapore
Switzerland	Spain	Honduras	Japan
Bahamas	Denmark	Saint Lucia	Chad
Liechtenstein	Trinidad and Tobago	Hungary	Algeria
Bahrain	Dominica	Saudi Arabia	Comoros
Netherlands	Armenia	Iceland	Argentina
Barbados	Dominican Republic	Slovakia	Burundi
Qatar	Kuwait	Iran	Kenya
Belarus	El Salvador	South Korea	Senegal
Slovenia	Lebanon	Iraq	Kiribati
Belgium	Estonia	Sweden	Somalia
Ukraine	Lithuania	Ireland	Benin
Belize	Finland	Syria	Sudan
Latvia	Malta	Israel	Kyrgyzstan
Bosnia and Herzegovina	Albania	Turkey	Timor-Leste
Luxembourg	Andorra	United Kingdom	Czech Republic
Bulgaria	Georgia	United Arab Emirates	Uganda
	Montenegro	Jamaica	Bhutan
			Cambodia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566
Phishing

T1190
Exploit Public-Facing Application

T1059
Command and Scripting Interpreter

T1204
User Execution

T1055
Process Injection

T1588.005
Exploits

T1027
Obfuscated Files or Information

T1204.002
Malicious File

T1041
Exfiltration Over C2 Channel

T1068
Exploitation for Privilege Escalation

T1587.001
Malware

T1036
Masquerading

T1082
System Information Discovery

T1588
Obtain Capabilities

T1588.006
Vulnerabilities

T1083
File and Directory Discovery

T1547
Boot or Logon Autostart Execution

T1486
Data Encrypted for Impact

T1498
Network Denial of Service

T1057
Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atlantida Stealer	Atlantida stealer is an info-stealer malware targeting sensitive information from various applications, including Telegram, Steam, FileZilla, cryptocurrency wallets, and web browsers. This malware extracts stored sensitive and potentially valuable data, such as passwords and cookies, and collects files with specific extensions from the infected system's desktop. Additionally, Atlantida stealer captures the victim's screen and gathers comprehensive system information, enhancing its ability to exploit compromised systems.	Exploiting Vulnerabilities	CVE-2024-38112
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	Windows MSHTML
ASSOCIATED ACTOR			**PATCH LINK**
Void Banshee, Stargazer Goblin			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

IOC TYPE	VALUE
SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750, 2b6c8aa2ac917d978dfec53cef70eaca36764a93d01d93786cc0d84da47ce8e6, 385ebe3d5bd22b6a5ae6314f33a7fa6aa24814005284c79edaa5bdcf98e28492, 2ebf051f6a61fa825c684f1d640bfb3bd79add0afcff698660f83f22e6544cba, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0

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
Rhadamanthys	Rhadamanthys is an information stealer with a diverse set of modules and a multilayered design. It is sold on the black market and frequently updated, making it a persistent threat. Its multi-layer architecture allows it to evade detection and perform a range of malicious activities, such as stealing sensitive information and exfiltrating data.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal Data	-
Info Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Stargazer Goblin			-
IOC TYPE	**VALUE**		
SHA256	060de3b4cf3056f24de882b4408020cee0510cb1ff0e5007c621bc98e5b4bdf3, 64a49ff6862b2c924280d5e906bc36168112c85d9acc2eb778b72ea1d4c17895		
IPv4:Port	147[.]45[.]44[.]73[:]1488, 89[.]23[.]98[.]116[:]1444, 147[.]78[.]103[.]199[:]2529		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RisePro	RisePro is a stealer written in C++ that spreads through downloaders like win.privateloader. It possesses similar functionality to the stealer malware “Vidar.” RisePro targets sensitive information on infected machines and attempts to exfiltrate it in the form of logs. It can steal credit card information, passwords, personal data, and other confidential information, posing a significant threat to affected systems.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal Data	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Stargazer Goblin			-
IOC TYPE	**VALUE**		
SHA1	52c071349a51f000c446acb9ba38194449a455ba3cff5be290ba336dab1176fd, 115aaa4fe6c3f309b03db57b4ce7e76ba8952cb240a22b6c35697cfe6352488f, B8d237fe35a52972a376a80721d5a97f9edc5da447502d3564185eaa6df07706		

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
RedLine	RedLine Stealer is a versatile malware that can be purchased either as a standalone product or on a subscription basis. It is designed to collect a wide range of information from browsers, including saved credentials, autocomplete data, and credit card details. RedLine Stealer have expanded their capabilities to include the theft of cryptocurrency.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal Data	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Stargazer Goblin			-
IOC TYPE	**VALUE**		
SHA256	d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54, 170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d, f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f, 9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53, ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two-factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	Exploiting Vulnerabilities	CVE-2024-21412
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	Microsoft Windows Internet Shortcut Files
ASSOCIATED ACTOR			**PATCH LINK**
Stargazer Goblin			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
IOC TYPE	**VALUE**		
SHA256	148c456e83e746a63e54ec5abda801731c42f3778e8eb0bf5a5c731b9a48c45d, 2f5624dcda1d58a45491028acc63ff3f1f89f564015813c52eebd80f51220383, 98b7488b1a18cb0c5e360c06f0c94d19a5230b7b15d0616856354fb64929b38, a484fa09be45608e23d8e67cd28675fa3e3c4111af396501385256ce34ff1d95		

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
Mint Stealer	Mint Stealer is a Python-based malware is designed to steal sensitive information, including browser data and cryptocurrency wallets. To evade detection, it employs encryption and obfuscation techniques, and it uploads the stolen data to file-sharing sites.	Phishing and compromised websites	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Stargazer Goblin			-
IOC TYPE	**VALUE**		
SHA256	1064ab9e734628e74c580c5aba71e4660ee3ed68db71f6aa81e30f148a5080fa, db47e673cccdbe2abb11cc07997aeabf4d2bdc9bec286674b58c6baafa09b82		
MD5	9f037593071344bc1354e5a619f914f4, e6e620e5cac01f73d0243dc9cf684193, afefdbd2bf7a6a622eaf09ab4a1adb3b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XDSpy.DSDownloader	XDSpy.DSDownloader is a malicious tool used by the cyber espionage group XDSpy. It's delivered through phishing emails containing a RAR archive with a malicious DLL. This DLL downloads the main malware payload while distracting the victim with a decoy document.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, System Compromise, Disruption of Operations	-
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
XDSpy			-
IOC TYPE	**VALUE**		
SHA256	65a953a80a0accd3b9a5b0f5c6978dad223273bd4d5ec892737e569c864fc73c, 01d092290e410617eb3369bf3682af186ae8da0937ee90acadba75ee5d4e17e, 78ba21a60241da65cf65e951773bbfd606402a3bf43acc5201e95220d13e8817		

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
Akira	Akira ransomware, first identified in March 2023, targets both Windows and Linux systems, employing a hybrid encryption method using ChaCha20 and RSA. This ransomware utilizes a double extortion tactic, encrypting files and exfiltrating sensitive data before demanding large ransoms, often in the millions.	Exploiting Vulnerabilities	CVE-2024-37085
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html
IOC TYPE	**VALUE**		
SHA256	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386		

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>Black Basta</td><td rowspan="5">Black Basta is a ransomware-as-a-service (RaaS) variant that was first identified in April 2022. They employ a double-extortion model, where they not only encrypt the victim's systems but also exfiltrate data. This dual approach increases the pressure on victims to pay the ransom, as they face the threat of data leaks in addition to system inaccessibility.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-37085</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt Data</td><td rowspan="2">Microsoft Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>-</td><td>PATCH LINK</td></tr>
<tr><td colspan="3"></td><td>https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">3d8713641264c41cd6784c5569c1447299fba88633070e40e70bb3ae2b4c5a4e, 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, 0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79</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>Babuk</td><td rowspan="6">Babuk is a ransomware strain that emerged in 2021, targeting large enterprises. Initially focusing on data encryption for ransom, the group later shifted to data theft and extortion. Known for its aggressive tactics and leaked source code,</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-37085</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="4">Encrypt Data</td><td>Microsoft Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">1da8156503645874c9647f6415362f9f1520b37b473490e742b3da6fe98eb493, 6b4c5947a0a37529e015d19b69ff46e701857afa020c414ce350b69a148e7cc6, 9596eab8ae29be0e3225e17a326610af6d79c90635f6cc226e55c0f8a0d4504c</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LockBit	LockBit is a prominent ransomware-as-a-service (RaaS) operation known for its aggressive tactics. It employs data encryption and exfiltration, demanding high ransoms. The group has evolved through multiple versions, each with enhanced capabilities, making it a persistent and sophisticated threat to organizations worldwide.	Exploiting Vulnerabilities	CVE-2024-37085
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

IOC TYPE	VALUE
SHA256	3b50796d11c0837412a2d9205f28604ef9c02ea436e33f9cb46ac3b99e1bbc37, 061ee3375dc3333d8c4266e773535e516206935d4f7dbbc3f0319d253840213d, f8c1925693a82d8a544bedcf975160a6cbd8a0d0e2a463e402402d8d28ad6ed, 1624a0e8f86cf5331ccf66fd830a96827fc0b3dd842abb268996d2387f2ed4be, 07a1258c5ef18d86c00f843408aa21667c7817b8e7d1ead1a5411856d0d21ed7

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
Kuiper	The Kuiper ransomware, developed in Golang, is compatible with Windows, Linux, and OSX systems, and is associated with a suspected intrusion at a government financial department in Africa.	Exploiting Vulnerabilities	CVE-2024-37085
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

IOC TYPE	VALUE
SHA1	90dd8718560a23faddf99e64b52175d1d765397c
MD5	84820f3eb491a2fde1f52435cd29646c
IPv4	91[.]92[.]251[.]25

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BeaverTail	BeaverTail is a JavaScript stealer malware that targets software developers through a supposed job interview process. It can steal sensitive information from web browsers, crypto wallets, and system data.	Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	6263b94884726751bf4de6f1a4dc309fb19f29b53cce0d5ec521a6c0f5119264, bc4a082e2b999d18ef2d7de1948b2bfd9758072f5945e08798f47827686621f2

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>InvisibleFerret</td><td rowspan="6">InvisibleFerret is a newly discovered, cross-platform Python backdoor malware that is part of a campaign targeting job seekers. It consists of various components for fingerprinting, remote control, keylogging, data exfiltration, browser stealing, and downloading the AnyDesk client for additional control.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Backdoor</td><td rowspan="4">Data theft</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">35434e903bc3be183fa07b9e99d49c0b0b3d8cf6cbd383518e9a9d753d25b672,
305de20b24e2662d47f06f16a5998ef933a5f8e92f9ecadf82129b484769bbac,
39e7f94684129efce4d070d89e27508709f95fa55d9721f7b5d52f8b66b95ceb,
ab198c5a79cd9dedb271bd8a56ab568fbd91984f269f075d8b65173e749a8fde,
444f56157dfcf9fc2347911a00fe9f3e3cb7971dccf67e1359d2f99a35aed88e</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	✓	Apache Log4j2	Andariel
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37085	✗	Microsoft Internet Explorer: 6 - 8	Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:internet_explorer:*:*:*:*:*:*:*:*	Akira Ransomware, Black Basta Ransomware, Babuk, Lockbit, and Kuiper
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Andariel (aka APT45, Onyx Sleet, formerly PLUTONIUM, DarkSeoul, Silent Chollima, and Stonefly)	North Korea	Critical Infrastructure, Defense, Aerospace, Government, Financial, Healthcare, Pharmaceutical, Engineering, Telecommunications, Transportation, Technology, Biotech, Chemicals, Education, Energy, Insurance, Legal, Medical Equipment, Nuclear Power, Retail, Utilities, and Agricultural	United States, Brazil, India, Japan, South Korea, United Kingdom, Germany, France, Nigeria
	MOTIVE		
	Espionage and Information theft, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-44228	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware	Apache Log4j2

TTPs

TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0042: Resource Development; TA0003: Persistence; TA0007: Discovery; TA0008: Lateral Movement; TA0043: Reconnaissance; TA0009: Collection; TA0011: Command and Control; TA0006: Credential Access; TA0010: Exfiltration; TA0005: Defense Evasion; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059.001: PowerShell; T1059.006: Python; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.003: Windows Command Shell; T1055.012: Process Hollowing; T1055: Process Injection; T1055.003: Thread Execution Hijacking; T1134: Access Token Manipulation; T1098: Account Manipulation; T1543.003: Windows Service; T1543: Create or Modify System Process; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1007: System Service Discovery; T1087: Account Discovery; T1591: Gather Victim Org Information; T1592: Gather Victim Host Information; T1595: Active Scanning; T1596: Search Open Technical Databases; T1003: OS Credential Dumping; T1048: Exfiltration Over Alternative Protocol; T1090: Proxy; T1560: Archive Collected Data; T1572: Protocol Tunneling; T1587.001: Malware; T1587.004: Exploits; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1039: Data from Network Shared Drive; T1567: Exfiltration Over Web Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Stargazer Goblin</td><td>-
MOTIVE
Information theft, Financial gain</td><td>All</td><td>Worldwide</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine</td><td>-</td></tr>
<tr><td colspan="3">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0042: Resource Development; T1204: User Execution; T1566: Phishing; T1189: Drive-by Compromise; T1059: Command and Scripting Interpreter; T1071: Application Layer Protocol; T1027: Obfuscated Files or Information; T1036: Masquerading; T1212: Exploitation for Credential Access; T1083: File and Directory Discovery; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1608: Stage Capabilities; T1608.001: Upload Malware</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Scattered Spider (aka Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, and Muddled Libra)	Unknown **MOTIVE** Financial gain	Commercial facilities, Telecommunications, Technology, and Business-Process Outsourcing (BPO)	Worldwide
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-37085	BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, and VIDAR Stealer	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

TTPs
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0040: Impact; T1657: Financial Theft; T1567: Exfiltration Over Web Service; T1585.001: Social Media Accounts; T1585: Establish Accounts; T1566: Phishing; T1660: Phishing; T1566.004: Spearphishing Voice; T1199: Trusted Relationship; T1078.002: Domain Accounts; T1078: Valid Accounts; T1648: Serverless Execution; T1204: User Execution; T1136: Create Account; T1556.006: Multi-Factor Authentication; T1556: Modify Authentication Process; T1484.002: Domain Trust Modification; T1484: Domain Policy Modification; T1578.002: Create Cloud Instance; T1578: Modify Cloud Compute Infrastructure; T1656: Impersonation; T1606: Forge Web Credentials; T1621: Multi-Factor Authentication Request Generation; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552: Unsecured Credentials; T1217: Browser Bookmark Discovery; T1538: Cloud Service Dashboard; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1539: Steal Web Session Cookie; T1021: Remote Services; T1021.007: Cloud Services; T1213.003: Code Repositories; T1213.002: Sharepoint; T1213: Data from Information Repositories; T1074: Data Staged; T1114:Email Collection; T1530: Data from Cloud Storage; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1567.002: Exfiltration to Cloud Storage

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Manatee Tempest (aka Indrik Spider, Gold Drake, Gold Winter, Evil Corp, UNC2165, DEV-0243, Blue Lelantos)	Russia	Financial, Government, Healthcare, Media	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-37085	-	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

TTPs
TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.007: JavaScript; T1584: Compromise Infrastructure; T1584.004: Compromise Infrastructure: Server; T1136: Create Account; T1486: Data Encrypted for Impact; T1074.001: Data Staged: Local Data Staging; T1587.001: Develop Capabilities: Malware; T1484.001: Domain or Tenant Policy Modification: Group Policy Modification; T1585.002: Establish Accounts: Email Accounts; T1562.001: Impair Defenses: Disable or Modify Tools; T1070: Indicator Removal: Clear Windows Event Logs; T1105: Ingress Tool Transfer; T1036.005: Masquerading: Match Legitimate Name or Location; T1003.001: OS Credential Dumping: LSASS Memory; T1018: Remote System Discovery; T1489: Service Stop; T1007: System Service Discovery; T1204.002: User Execution: Malicious File; T1078.002: Valid Accounts: Domain Accounts; T1047: Windows Management Instrumentation

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
XDSpy (aka UAC-0033)</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Russia and Moldova</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>XDSpy.DSDownloader</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; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1204: User Execution; T1204.001: Malicious Link; T1140: Deobfuscate/Decode Files or Information; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **Andariel, Stargazer Goblin, Scattered Spider, Manatee Tempest, XDSpy** and malware **Atlantida stealer, Rhadamanthys, RisePro, Lumma Stealer, RedLine, Akira, Black Basta, Babuk, Lockbit, Kuiper, BeaverTail, InvisibleFerret Backdoor, Mint Stealer, XDSpy.DSDownloader.**

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 **two exploited vulnerabilities.**

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Andariel, Stargazer Goblin, Scattered Spider, Manatee Tempest, XDSpy** and malware **Rhadamanthys, RisePro, Lumma Stealer, Red Line, Akira, Black Basta, Babuk, LockBit, Kuiper, Mint Stealer, BeaverTail** in Breach and Attack Simulation(BAS).

Threat Advisories

Andariel: North Korea's Evolving Cyber Threat Landscape

Stargazers Ghost Network: 3,000 Rogue GitHub Accounts Fuel Malware Spread

VMware ESXi's Fatal Flaw CVE-2024-37085 Opens Doors for Ransomware Havoc

DEV#POPPER the North Korean Cyber Threat Hiding in Job Offers

Mint Stealer: A New Python-Based Information Stealer

XDSpy Expands Arsenal with New Tool: XDSpy.DSDownloader

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
Atlantida Stealer	SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750, 2b6c8aa2ac917d978dfec53cef70eaca36764a93d01d93786cc0d84da47ce8e6, 385ebe3d5bd22b6a5ae6314f33a7fa6aa24814005284c79edaa5bdcf98e28492, 2ebf051f6a61fa825c684f1d640bfb3bd79add0afcff698660f83f22e6544cba, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0
	IPv4	185[.]172[.]128[.]95
Rhadamanthys	SHA256	060de3b4cf3056f24de882b4408020cee0510cb1ff0e5007c621bc98e5b4bdf3, 64a49ff6862b2c924280d5e906bc36168112c85d9acc2eb778b72ea1d4c17895
	IPv4:Port	147[.]45[.]44[.]73[:]1488, 89[.]23[.]98[.]116[:]1444, 147[.]78[.]103[.]199[:]2529
RisePro	SHA256	52c071349a51f000c446acb9ba38194449a455ba3cff5be290ba336dab1176fd 115aaa4fe6c3f309b03db57b4ce7e76ba8952cb240a22b6c35697cfe6352488f b8d237fe35a52972a376a80721d5a97f9edc5da447502d3564185eaa6df07706
RedLine	SHA256	8d8d7eb1180c13ed629dceac6c399c656692a6476c49047e0822bec6156a253a
	IPv4:Port	147[.]45[.]47[.]64[:]11837

Attack Name	TYPE	VALUE
Lumma	SHA256	B1B8EA15E6BBFC7C38EB394D7E81A99A93689464FAF991D77E28722E5B0E4681, D9F6408B67628D5618A4FBABA97404AC55988633CCB2A02A09C95B0B134BAFC9, DD5B52A63E8A774C058E558AA7E983D6AA51F560BA3F01829287C4B85081B884, D856A66EA554538D421ABCEB2D304200537F5A268CBFDE8F52F41A0C048EDFDC, 148c456e83e746a63e54ec5abda801731c42f3778e8eb0bf5a5c731b9a48c45d, 2f5624dcda1d58a45491028acc63ff3f1f89f564015813c52eebd80f51220383, 98b7488b1a18cb0c5e360c06f0c94d19a5230b7b15d0616856354fb64929b388, a484fa09be45608e23d8e67cd28675fa3e3c4111af396501385256ce34ff1d95
	URLs	hxxps[:]//considerrycurrentyws[.]shop, hxxps[:]//deprivedrinkyfaiir[.]shop, hxxps[:]//detailbaconroollyws[.]shop, hxxps[:]//distincttangyflippan[.]shop, hxxps[:]//greentastellesqwm[.]shop, hxxps[:]//horsedwollfedrwos[.]shop, hxxps[:]//innerverdanytiresw[.]shop, hxxps[:]//lamentablegapingkwaq[.]shop, hxxps[:]//macabrecondfucews[.]shop, hxxps[:]//messtimetabledkolvk[.]shop, hxxps[:]//patternapplauderw[.]shop, hxxps[:]//relaxtionflouwerwi[.]shop, hxxps[:]//sideindexfollowragelrew[.]pw, hxxps[:]//slamcopynammeks[.]shop, hxxps[:]//standingcomperewhitwo[.]shop, hxxps[:]//stickyyummyskiwffe[.]shop, hxxps[:]//sturdyregularrmsnhw[.]shop, hxxps[:]//understanndtytonyguw[.]shop, hxxps[:]//vivaciousdqugilew[.]shop
Akira	SHA256	049a593fd540d78840d000d2fa6046e8d28279376ef61e5ccc8f74dd49f1c498, 1ed8c04e2e91c9db7b88f818cc7d8f043f674d1898c182b6390acaa9fbb251aa, 1f188ed83c386c5b65036cd7afef8277d7c957a1b2b688977a6351312e16f307, 1fd9f2cdf2ee55d5d91e890c6a16e468f576a4e97747093204ffb122eacf2a27, 2bfe3fba2e94b1a4f8ae0ea767b64084390155bb4d57cc39e13c15b181f8d377, 2c10cc96f48839b84954e88cb6f85e5c15442f4d15c34213d008e859f87f7261, 5c0b974c49bb7963c5b65514666bedf5ade01405dcf2a282fd761bd40580fc30,

Attack Name	TYPE	VALUE
Akira	SHA256	5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5, 61bf0c07f2c51fda325d3b781f9d13a0bf304dff27814d78a3329728e92a92f2, 74fc20b6715fa1318455dca3a979afeb340c8fe03cdfa43dce8469fa36f7f78c, 77f13e2887ccd042e4303ed6dcc4c435097e14d2072025a9c089189850d91308, 86708db0f4c405c96b5ed10e7eb844528e0e0ec0a673d728b4ca46a3be306a52, b02e3e3a6f369a54edb85dfa82374f3d77707f4fdd0099fe206a6aa31ce55606, d07a2168892a73678da0869cc295cacaf12f0b1ffce337b957c0af7c5a802865, e74f3881764f0469ac6d67379fbcc837ddbc753d019a0ba35ce97abe550453ad, eb6dc793918d46556ea79531e49d5e12bb237802218abd8cdaa115752431b07a, f151257e38fc27b81eb3bdf694175d0872c9e0438fc5ea08844c912487290e75, d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386
Black Basta	SHA256	3d8713641264c41cd6784c5569c1447299fba88633070e40e70bb3ae2b4c5a4e, 7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, 0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79
Babuk	SHA256	1da8156503645874c9647f6415362f9f1520b37b473490e742b3da6fe98eb493, 6b4c5947a0a37529e015d19b69ff46e701857afa020c414ce350b69a148e7cc6, 9596eab8ae29be0e3225e17a326610af6d79c90635f6cc226e55c0f8a0d4504c

Attack Name	TYPE	VALUE
Lockbit	SHA256	0f178bc093b6b9d25924a85d9a7dde64592215599733e83e3bbc6df219564335, daff7ba0e08e663f81f9b13a759221cb626b0e5cf45a6b17bb4d65663023cf78, d526f8d4c268b96a76007f620e682f1fadfb3d1cc56656b63205d4d0311b97f0, 0f5d71496ab540c3395cfc024778a7ac5c6b5418f165cc753ea2b2befbd42d51, 19ca5aa4cd62929afb255d2b38e70fd3143e3b181889e84348a5c896e577d708, 0a937d4fe8aa6cb947b95841c490d73e452a3cafcd92645afc353006786aba76, 9a0f32eb9da6cd8f3f4db8c49c87999374c5f045f51f8011ca29713743ec4cff, de04ab70799c9f7ad348ea1ea7adbad53204bcff69e70107e8910c168d134af1, 3b50796d11c0837412a2d9205f28604ef9c02ea436e33f9cb46ac3b99e1bbc37, 061ee3375dc3333d8c4266e773535e516206935d4f7dbbc3f0319d253840213d, f8c1925693a82d8a544bedcf975160a6cbd8a0d0e2a463e402402d8d28ad6ed, 1624a0e8f86cf5331ccf66fd830a96827fc0b3dd842abb268996d2387f2ed4be, 07a1258c5ef18d86c00f843408aa21667c7817b8e7d1ead1a5411856d0d21ed7
Kuiper	SHA256	c66590a2ffbe53667be147c4e74e626764aff9eb31017dd8b8f161279fd0f4f6, ee0372abd3681b07517d0c5a5406257e4e2abd53224227fe04c077963dd36189, ec92a82fa5596eb4fb3c0c39cbbc7c7ab839fdb64d782822662f25e76086760d, d6c1d2e77ce21d5a026e7abf99c9fffe55d87b282f460dc737da231211a12a0d, 998347d4ba21661688169337ca4ea2a6118c2fad2005d39d8bf46c0bcf46af5a, 4e153342189a55ffed34a91f2a3f4440af1acbf7dc58135a165a06b4e657556a, 0162641163a30a2edff787eeecc733ab1de46f03e213743dc768d39eb3075985
	SHA1	90dd8718560a23faddf99e64b52175d1d765397c
	MD5	84820f3eb491a2fde1f52435cd29646c
	IPv4	91[.]92[.]251[.]25
BeaverTail	SHA256	6263b94884726751bf4de6f1a4dc309fb19f29b53cce0d5ec521a6c0f5119264, bc4a082e2b999d18ef2d7de1948b2bfd9758072f5945e08798f47827686621f2

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

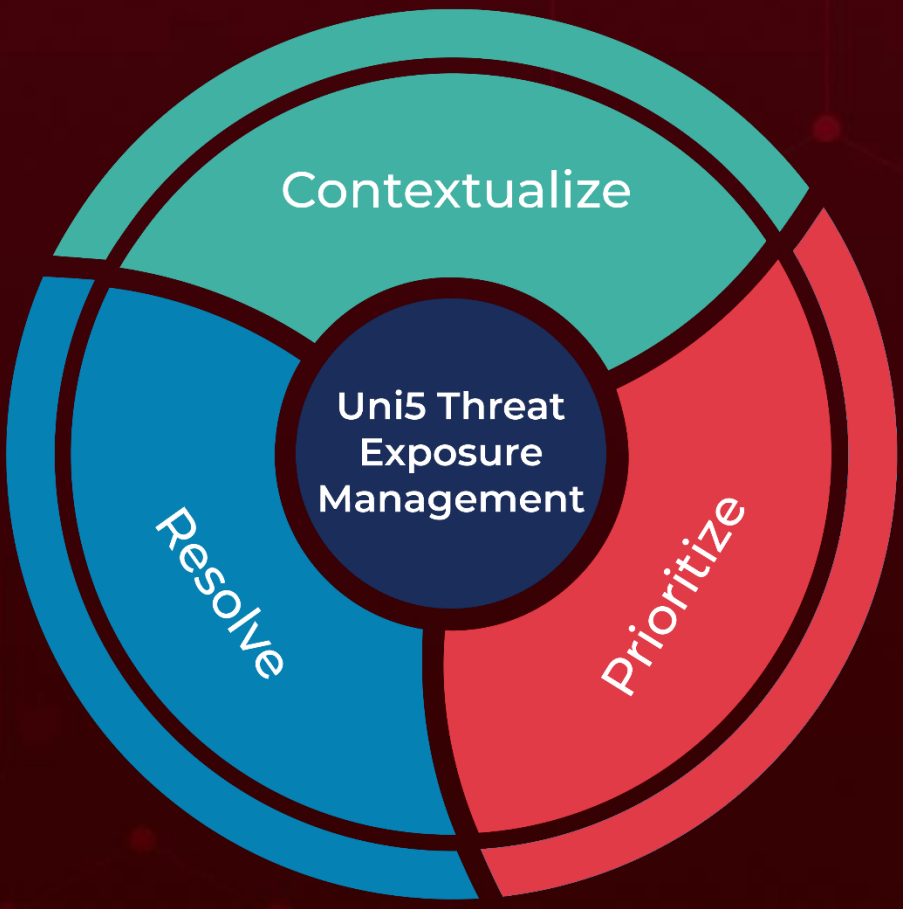
Attack Name	TYPE	VALUE
InvisibleFerret	SHA256	35434e903bc3be183fa07b9e99d49c0b0b3d8cf6cbd383518e9a9d753d25b672, 305de20b24e2662d47f06f16a5998ef933a5f8e92f9ecadf82129b484769bbac, 39e7f94684129efce4d070d89e27508709f95fa55d9721f7b5d52f8b66b95ceb, ab198c5a79cd9dedb271bd8a56ab568fbd91984f269f075d8b65173e749a8fde, 444f56157dfcf9fc2347911a00fe9f3e3cb7971dccf67e1359d2f99a35aed88e, 4f50051ae3cb57f10506c6d69d7c9739c90ef21bfb82b14da6f4b407b6febac0, 276863ee7b250419411b39c8539c31857752e54b53b072dffd0d3669f2914216, 617c62da1c228ec6d264f89e375e9a594a72a714a9701ed3268aa4742925112b, c547b80e1026d562ac851be007792ae98ddc1f3f8776741a72035aca3f18d277, 03185038cad7126663550d2290a14a166494fdd7ab0978b98667d64bda6e27cc, 2d300410a3edb77b5f1f0ff2aa2d378425d984f15028c35dfad20fc750a6671a, 92aeea4c32013b935cd8550a082aff1014d0cd2c2b7d861b43a344de83b68129
Mint Stealer	SHA256	1064ab9e734628e74c580c5aba71e4660ee3ed68db71f6aa81e30f148a5080fa, db47e673cccdbe2abb11cc07997aeabf4d2bdc9bec286674b58c6baafa09b82
	MD5	9f037593071344bc1354e5a619f914f4, e6e620e5cac01f73d0243dc9cf684193, afefdbd2bf7a6a622eaf09ab4a1adb3b
XDSpy.DSDownloader	SHA256	65a953a80a0accd3b9a5b0f5c6978dad223273bd4d5ec892737e569c864fc73c, 01d092290e410617eb3369bf3682af186ae8da0937ee90acadba75ee5d4e17e4, 78ba21a60241da65cf65e951773bbfd606402a3bf43acc5201e95220d13e8817
	SHA1	00bde6ad42ef3cbef9f0f0cc054014435432b17c, 02760b55fa69392d9 9633c271e43108c64c21807, 68d83a5d25d62f0b15912fb70474dd371db1947d
	MD5	2982ac131e49354ec51e645f9db53b40, 0fd1128bc81eca818909d50f9806fd85, 3bd819440fbc91a530c3c659d99564e3

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

What Next?

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

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



REPORT GENERATED ON

August 5, 2024 . 10:30 PM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com