Date of Publication
July 1, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

24 to 30 JUNE 2024

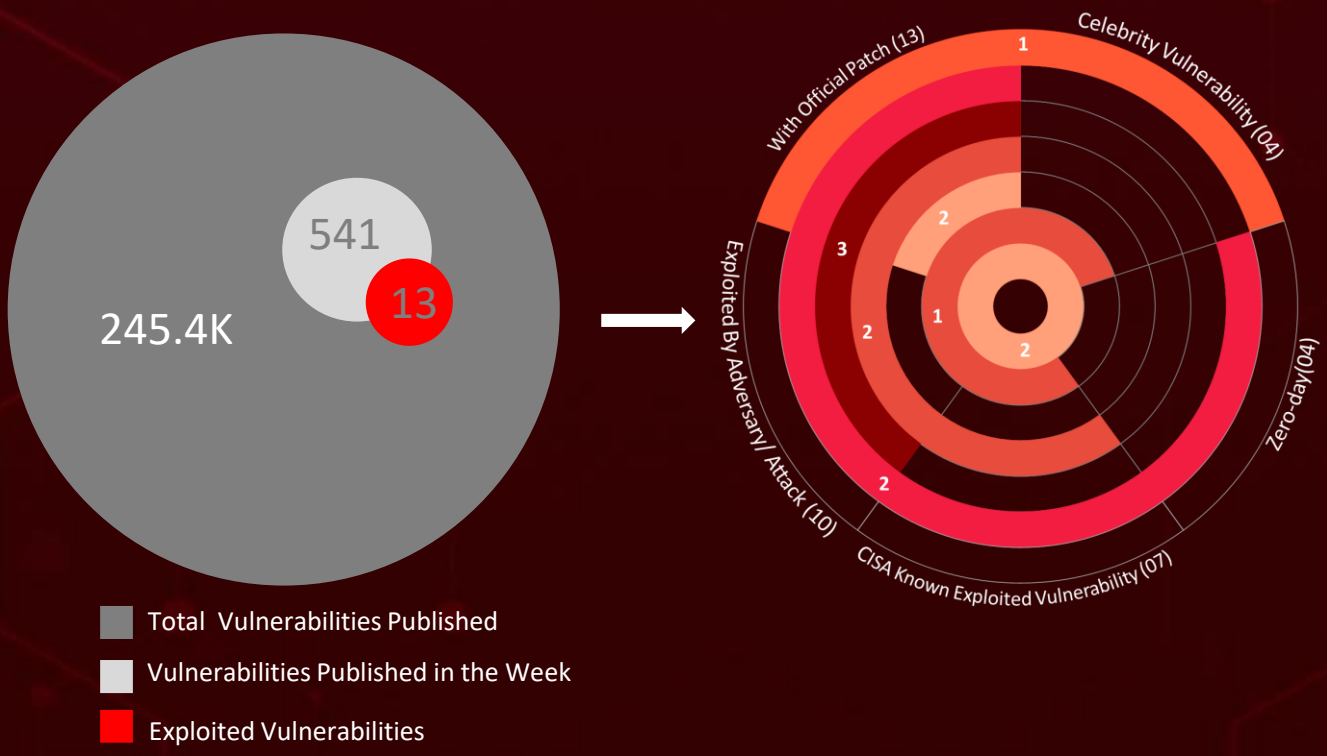
Table Of Contents

Summary

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

Additionally, **DragonForce ransomware** is using a leaked Lockbit Black builder to customize and execute their operations, potentially increasing the scale and impact of their malicious activities.

Furthermore, the espionage group **SneakyChef** has launched a new campaign targeting government agencies with two innovative Remote Access Trojans (RATs) named **SugarGh0st and SpiceRAT.** These rising threats pose significant and immediate danger to users worldwide.



High Level Statistics

8
Attacks Executed

13
Vulnerabilities Exploited

5
Adversaries in Action

- SugarGh0st
- SpiceRAT
- DragonForce
- XWorm RAT
- CatB Ransomware
- InnoLoader
- BMANAGER
- GoRed Backdoor

- CVE-2022-2586
- CVE-2024-5805
- CVE-2024-5806
- CVE-2021-3156
- CVE-2021-4034
- CVE-2019-13272
- CVE-2022-27228
- CVE-2021-44228
- CVE-2021-40438
- CVE-2023-3519
- CVE-2019-12725
- CVE-2022-40691
- CVE-2024-0762

- SneakyChef
- ExCobalt
- UAC-0184
- Boolka
- ChamelGang

Insights

Boolka, a threat actor, has shifted its tactics from scripting to sophisticated malware attacks

Progress MOVEit Software has critical vulnerabilities involving authentication bypass issues within its SFTP modules

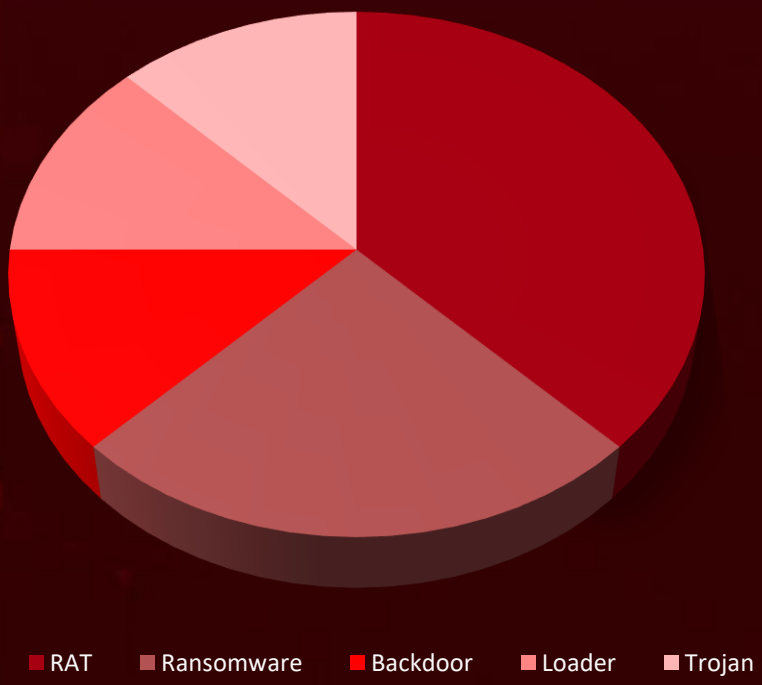
UAC-0184
launched an advanced malware campaign against Ukraine, deploying Xworm RAT

ExCobalt, a cyber espionage group, has been targeting Russian organizations with an advanced Golang-based backdoor named GoRed

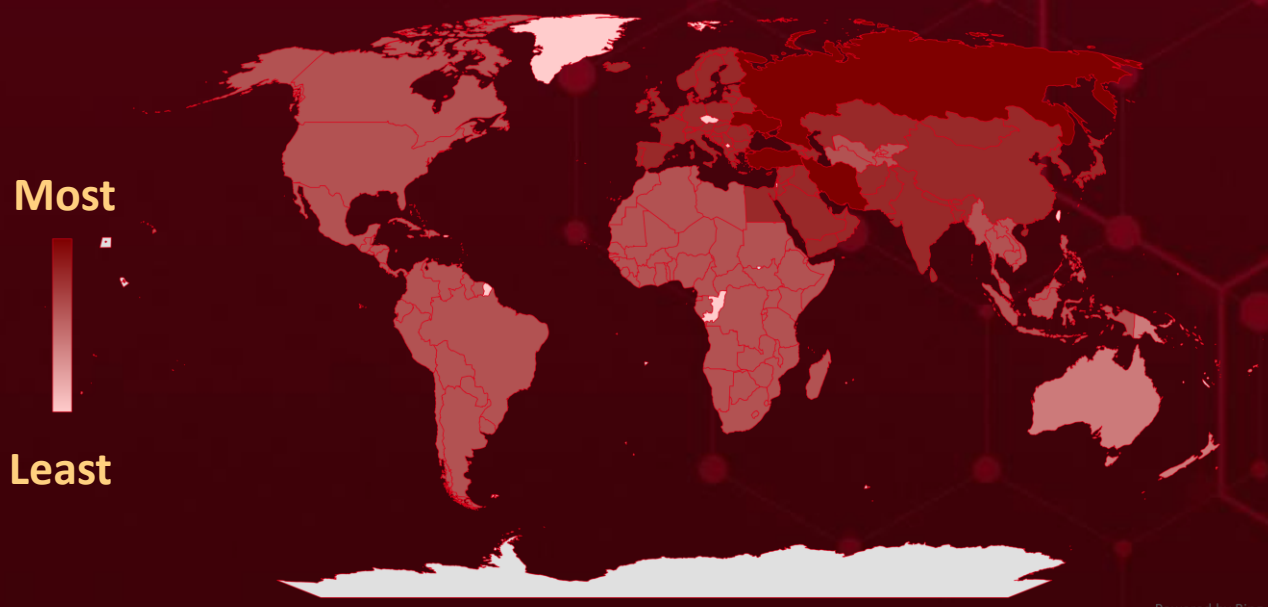
UEFIcanhazbufferoverflow
The CVE-2024-0762 vulnerability in Phoenix SecureCore UEFI firmware allows local attackers to execute code and escalate privileges on many Intel Core processors

SneakyChef Group
targeting Government sector using SugarGh0st and SpiceRAT

Threat Distribution

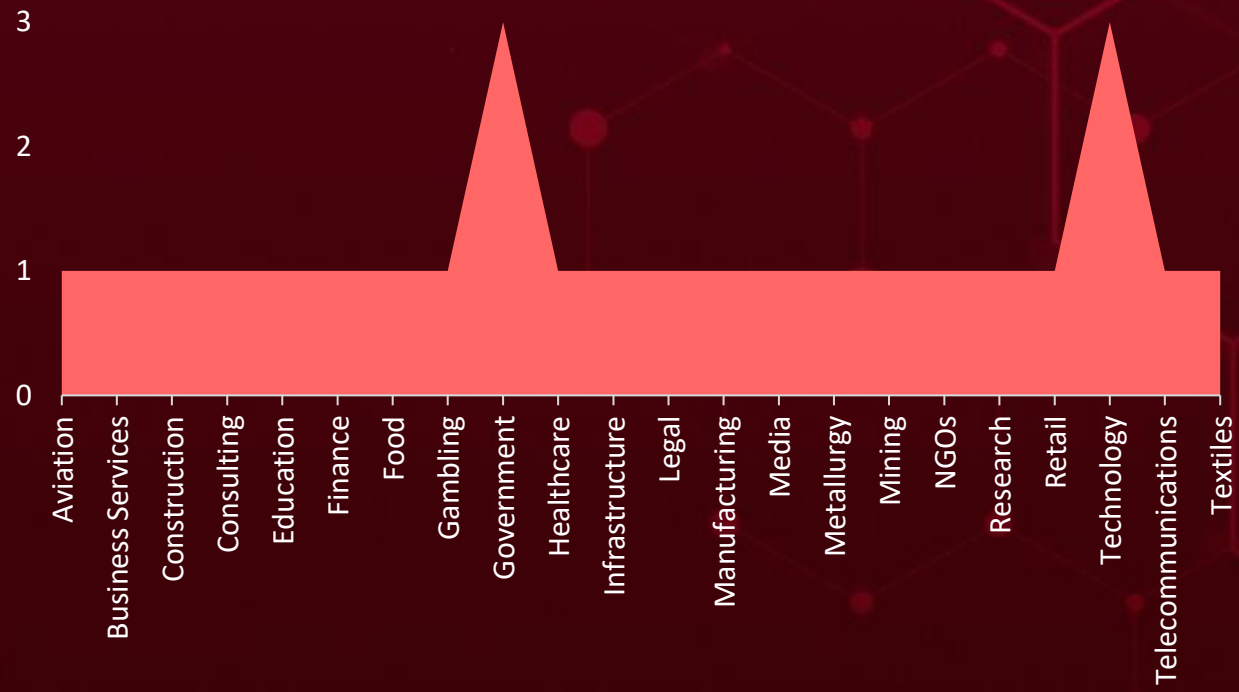


Targeted Countries



Countries	Countries	Countries	Countries
Ukraine	China	Albania	Bahamas
Iran	North Macedonia	Portugal	Indonesia
Russia	Croatia	Iraq	Somalia
Cyprus	Poland	Romania	Cabo Verde
Turkey	Afghanistan	Ireland	Togo
Switzerland	Armenia	San Marino	Cambodia
Oman	Denmark	Israel	Burkina Faso
Monaco	Slovakia	Serbia	Cameroon
Azerbaijan	Egypt	Italy	Rwanda
Saudi Arabia	Sri Lanka	Slovenia	Canada
Bahrain	Estonia	Japan	Sierra Leone
Luxembourg	Lebanon	Spain	Central African Republic
Bangladesh	Finland	Syria	
Netherlands	Lithuania	Sweden	Brunei
Belarus	France	Andorra	Jamaica
Qatar	Maldives	Austria	Tajikistan
Belgium	Georgia	United Kingdom	Chad
South Korea	Moldova	Jordan	Turkmenistan
Bhutan	Germany	United Arab Emirates	Chile
Liechtenstein	Mongolia	Kazakhstan	Venezuela
Bosnia and Herzegovina	Greece	Yemen	Barbados
Malta	Nepal	Latvia	Philippines
Bulgaria	Hungary	Kuwait	Kenya
Montenegro	North Korea	Gabon	Ethiopia
Bahrain	Iceland	Honduras	Zimbabwe
	Norway	Suriname	Argentina
	India	Burundi	Kyrgyzstan
	Pakistan		Gambia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1068 Exploitation for Privilege Escalation

T1059 Command and Scripting Interpreter

T1204 User Execution

T1588 Obtain Capabilities

T1055 Process Injection

T1082 System Information Discovery

T1027 Obfuscated Files or Information

T1190 Exploit Public-Facing Application

T1105 Ingress Tool Transfer

T1588.006 Vulnerabilities

T1566 Phishing

T1036 Masquerading

T1498 Network Denial of Service

T1204.002 Malicious File

T1486 Data Encrypted for Impact

T1070 Indicator Removal

T1057 Process Discovery

T1212 Exploitation for Credential Access

T1056 Input Capture

T1547 Boot or Logon Autostart Execution

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SugarGh0st	SugarGh0st RAT is a remote access trojan and a customized variant of Gh0stRAT. It features customized commands to facilitate remote administration tasks as directed by the C2 server and a modified communication protocol, based on the similarity of the command structure and the strings used in the code.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
SneakyChef			-
IOC TYPE	**VALUE**		
SHA256	8a563b3091b56eb0562f5442c90b4d28d4be2946a3dc4a225b4b96134f7e447b, d6bffa45aa2448b2fb584713395b742e02ef77c1d54f125cd501240e0dd91a13, 951a54d2c61c3257447c4ff5fd451ee581c76d3d4d88fa482b99f5410d7b7b6f, 8db5a7efe1a83e43cb4acdc596b0413b4beb54f9f8e13f978c07a6eeee6b8435, 31b7e97770ffe74dad914a37a78c8f9a7286c75b62b5fae1c4ec722837ad457e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SpiceRAT	SpiceRAT employs the DLL sideloading technique, exploiting a legitimate signed executable to load a malicious DLL loader binary. This advanced malware collects reconnaissance data from the victim's machine, including operating system details, hostname, username, and network information.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal Information	-
ASSOCIATED ACTOR			**PATCH LINK**
SneakyChef			-
IOC TYPE	**VALUE**		
SHA256	6ca2415aabb806a871889c2ab48ad05b1ba444b5867ceadbcea3ab7f23de72f4, b84ebbe57151844ac7ac9fc5d488e4696f37f98779d13dceafe6c5a7f2219a4c, 0374a9812c7e43db1bde605cc3decff3d77c8b041b959a5422e4da0b60e0f6dc, 48c65bb99ce954df0ee492b92e634d602d621295be2ff87e57fcb07c8b33db8b		

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
DragonForce Ransomware	DragonForce has been observed using a leaked ransomware builder from the LockBit ransomware group. DragonForce ransomware targets victims with the intent of extortion. The threat actor typically employs a double extortion tactic: first, they lock the victims out of their infected machines and exfiltrate data before encryption.	Phishing, Exploiting Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	d54bae930b038950c2947f5397c13f84		
SHA1	e164bbaf848fa5d46fa42f62402a1c55330ef562		
SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XWorm RAT	XWorm allows to gain unauthorized access to devices, facilitating the theft of sensitive information such as login credentials and passwords. Additionally, it includes features for clipboard monitoring, installing ransomware, and launching Distributed Denial of Service (DDoS) attacks.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0184			-
IOC TYPE	**VALUE**		
SHA256	0d16de10ce708b990d1b0ae26ac12792c91864426c88a8c73a475f7f33db014b, dd8377e9c3620d0732bedecd0d219f77f7bcffbc49470a9b7ff22db33fe4a185		

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
CatB Ransomware	CatB is a ransomware that uses DLL hijacking to evade detection. It injects itself into the Microsoft Distributed Transaction Coordinator (MSDTC) service, a legitimate Windows process, and uses that process to encrypt the victim's files. This makes it harder for security scanners to identify the ransomware, as it is not running as a standalone process and may not show the typical behavior of ransomware.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
ChamelGang			-
IOC TYPE	**VALUE**		
SHA256	35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b, 512587a73cd03c6324ade468689510472c6b9e54074f3cf115aa54393b14f037, 9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2, 83129ed45151a706dff8f4e7a3b0736557f7284769016c2fb00018d0d3932cfa, 3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
InnoLoader	InnoLoader is a new unique malware that generates a distinct version with each download, complicating detection. It disguises itself as an installer, executing malicious actions and downloading additional payloads. The malware adapts its behavior based on C2 server instructions to evade detection.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Execute Commands	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
Domains	valuescent[.]website, caretouch[.]hair, whipunit[.]hair		

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>BMANAGER</td><td rowspan="5">The BMANAGER Trojan is a sophisticated malware providing remote access to attackers. It disguises itself as legitimate software, avoids detection, and can disable security features. Its primary functions include log keystrokes, data theft and system manipulation, posing significant cybersecurity threats.</td><td>custom malware delivery platform</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Trojan</td><td rowspan="3">System Compromise</td><td>Windows</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Boolka</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">7266f20123edcb2e0b92ac0b63225b8db2c5ff349818b339ef1553bff06719e4</td></tr>
<tr><td>Domains</td><td colspan="3">mainnode[.]beonlineboo[.]com,
node[.]beonlineboo[.]com</td></tr>
<tr><td>URL</td><td colspan="3">hxxp[:]//updatebrower.com/download/bmanager[.]txt</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>GoRed Backdoor</td><td rowspan="5">GoRed Backdoor uses the RPC protocol to communicate with its command and control (C2) server. This malware can obtain credentials from compromised systems. Operators utilize DNS/ICMP tunneling, WSS, and QUIC to communicate with GoRed. It gathers various types of information from compromised systems, including details of active processes, host names, lists of network interfaces, and file system structures. GoRed serializes, encrypts, archives, and sends the collected data to a specialized server dedicated to storing compromised information.</td><td>Exploiting Vulnerabilities</td><td>CVE-2022-2586
CVE-2021-3156
CVE-2021-4034
CVE-2019-13272
CVE-2022-27228
CVE-2021-44228
CVE-2021-40438
CVE-2023-3519
CVE-2019-12725
CVE-2022-40691</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Backdoor</td><td rowspan="3">Data Theft, Encrypt Data</td><td>Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>ExCobalt</td><td>https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t , https://www.sudo.ws/releases/stable/#1.9.5p2 , https://bugzilla.redhat.com/show_bug.cgi?id=2025869 , https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17 , https://helpdesk.bitrix24.com/open/15536776/ , https://logging.apache.org/log4j/2.x/security.html , https://httpd.apache.org/security/vulnerabilities_24.html , https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467 , https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">67b7a8fad28dcc40c0889e5c4e40aef9348441c64bba74bd6db885d88ce6d246</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-2022-2586	✗	Linux kernel	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	GoRed Backdoor
Linux Kernel nft_object Use-After-Free Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5805	✗	MOVEit Gateway 2024.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_gateway:*:*:*:*:*:*:*:*	-
Progress MOVEit Gateway Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5806	✗	Progress MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	-
Progress MOVEit Transfer Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3156	✓	Sudo before 1.9.5p2	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sudo_project:sudo:*:*:*:*:*:*:*:*:*	GoRed Backdoor
Baron Samedit (Sudo Heap-Based Buffer Overflow Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-193	T1068: Exploitation for Privilege Escalation	https://www.sudo.ws/releases/stable/#1.9.5p2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0762	ZERO-DAY	Phoenix SecureCore for Intel Kaby Lake: from 4.0.1.1 before 4.0.1.998; Phoenix SecureCore for Intel Coffee Lake: from 4.1.0.1 before 4.1.0.562; Phoenix SecureCore for Intel Ice Lake: from 4.2.0.1 before 4.2.0.323; Phoenix SecureCore for Intel Comet Lake: from 4.2.1.1 before 4.2.1.287; Phoenix SecureCore for Intel Tiger Lake: from 4.3.0.1 before 4.3.0.236; Phoenix SecureCore for Intel Jasper Lake: from 4.3.1.1 before 4.3.1.184; Phoenix SecureCore for Intel Alder Lake: from 4.4.0.1 before 4.4.0.269; Phoenix SecureCore for Intel Raptor Lake: from 4.5.0.1 before 4.5.0.218; Phoenix SecureCore for Intel Meteor Lake: from 4.5.1.1 before 4.5.1.15	-

NAME	CISA KEV	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
UEFIcanhazbufferoverflow (Phoenix SecureCore UEFI firmware Buffer Overflow Vulnerability)		cpe:2.3:a:phoenix:securecore_for_intel_kaby_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_coffee_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_ice_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_comet_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_tiger_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_jasper_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_raptor_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_alder_lake:*:*:*:*:*:*:*:* cpe:2.3:a:phoenix:securecore_for_intel_meteor_lake:*:*:*:*:*:*:*:*	-

CWE ID	ASSOCIATED TTPs	PATCH DETAILS
CWE-120	T1068: Exploitation for Privilege Escalation, T1542: Pre-OS Boot	https://www.phoenix.com/security-notifications/cve-2024-0762/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4034		Red Hat Polkit	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	GoRed Backdoor
Pwnkit (Red Hat Polkit Out-of-Bounds Read and Write Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1068: Exploitation for Privilege Escalation T1059: Command and Scripting Interpreter	https://bugzilla.redhat.com/show_bug.cgi?id=2025869

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-13272		Linux kernel before 5.1.17	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	GoRed Backdoor
Linux Kernel Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.17

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-27228		Bitrix before 21.0.100	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:bitrix24:bitrix24:*:*:*:*:*:*:*:*	GoRed Backdoor
Bitrix Arbitrary Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://helpdesk.bitrix24.com/open/15536776/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228		Apache Log4j2	ExCobalt
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	GoRed Backdoor
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40438	✗ ZERO-DAY	Apache HTTP Server 2.4.48 and earlier	ExCobalt
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*:*	GoRed Backdoor
Apache HTTP Server-Side Request Forgery	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy T1005: Data from Local System	https://httpd.apache.org/security/vulnerabilities_24.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519	✗ ZERO-DAY	Citrix NetScaler ADC and NetScaler Gateway	ExCobalt
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:-:*:*:*	GoRed Backdoor
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-12725	✗	Zeroshell 3.9.0	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zeroshell:zeroshell:3.9.0:*:*:*:*:*:*:*	GoRed Backdoor
Zeroshell Remote Command Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	Reached EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40691	✗	Moxa SDS-3008: 2.1	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:moxa:sds-3008_firmware:*:*:*:*:*:*:*:*	GoRed Backdoor
Moxa Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1588.006: Vulnerabilities, T1190: Exploit Public-Facing Application	https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SneakyChef	China	Government	Europe, Middle East, Africa and Asia
	MOTIVE		
	Espionage and Information theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	SugarGh0st, SpiceRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003:Persistence; TA0004: Privilege Escalation; TA0005:Defense Evasion; TA0009:Collection; TA0006: Credential Access; T1053.005: Scheduled Task; T1566: Phishing; T1027: Obfuscated Files or Information; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1036: Masqueradin;g T1204: User Execution; T1204.002: Malicious File; T1059.005: Visual Basic; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1547.001: Registry Run Keys /Startup Folder; T1547: Boot or Logon Autostart Execution; T1056.001: Keylogging; T1056: Input Capture; T1218.010: Regsvr32; T1218: System Binary Proxy Execution

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ExCobalt	-	Metallurgy, Telecommunications, Mining, Information Technology, Government, Software development	Russia
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-2586 CVE-2021-3156 CVE-2021-4034 CVE-2019-13272 CVE-2022-27228 CVE-2021-44228 CVE-2021-40438 CVE-2023-3519 CVE-2019-12725 CVE-2022-40691	GoRed Backdoor	Linux kernel, Sudo, Red Hat Polkit, Bitrix, Apache Log4j2, Apache HTTP Server, Citrix NetScaler ADC and NetScaler Gateway, Zeroshell, Moxa-SDS

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control;TA0040: Impact; TA0043: Reconnaissance; TA0042: Resource Development; T1595.002; Vulnerability Scanning; T1583.001: Domains; T1583.002: DNS Server; T1587.003: Digital Certificates; T1199: Trusted Relationship; T1195.001: Compromise Software Dependencies and Development Tools; T1059.003: Windows Command Shell; T1059.004: Unix Shell; T1059.006: Python; T1106: Native API; T1053.003: Cron; T1505.003: Web Shell; T1136.001: Local Account; T1068: Exploitation for Privilege Escalation; T1140: Deobfuscate/Decode Files or Information; T1027.002: Software Packing; T1027: Obfuscated Files or Information; T1601.001: Patch System Image; T1070.004: File Deletion; T1003.008: /etc/passwd and /etc/shadow; T1003.001: LSASS Memory; T1082: System Information Discovery; T1614.001: System Language Discovery; T1033: System Owner/User Discovery; T1087.001: Local Account; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1021.004: SSH; T1021.002: SMB/Windows Admin Shares; T1021.001: Remote Desktop Protocol; T1563.001: SSH Hijacking; T1560.001: Archive via Utility; T1560.002: Archive via Library; T1074: Data Staged; T1071.001: Web Protocols; T1132.001: Standard Encoding; T1071.004: DNS; T1572: Protocol Tunneling; T1132.002: Non-Standard Encoding; T1573.001: Symmetric Cryptography; T1090.001: Internal Proxy; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol; T1020: Automated Exfiltration; T1567: Exfiltration Over Web Service; T1485: Data Destruction; T1486: Data Encrypted for Impact

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UAC-0184</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Ukraine, Finland</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Information theft</td><td rowspan="2">ASSOCIATED ATTACKS/RANSOMWARE</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>TARGETED CVEs</td></tr>
<tr><td>-</td><td>XWorm RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1547.001: Registry Run Keys / Startup Folder; T1574.002: DLL Side-Loading; T1055: Process Injection; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1057: Process Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer; T1059.005: Visual Basic; T1566: Phishing; T1566.001: Spearphishing Attachment</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Boolka</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage, Information theft</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>BMANAGER</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0006: Credential Access; TA0001: Initial Access; TA0010: Exfiltration; TA0040: Impact; TA0007: Discovery; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1204:User Execution; T1204.002: Malicious File; T1583.004: Server; T1584.003: Virtual Private Server; T1584: Compromise Infrastructure; T1588.002: Tool; T1588: Obtain Capabilities; T1056.001: Keylogging; T1056:Input Capture; T1583.001: Domains; T1583: Acquire Infrastructure; T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1203: Exploitation for Client Execution; T1569: System Services; T1569.002: Service Execution; T1543: Create or Modify System Process; T1543.003: Windows Service; T1001: Data Obfuscation; T1657:Financial Theft; T1082: System Information Discovery; T1083: File and Directory Discovery; T1210: Exploitation of Remote Services; T1005: Data from Local System; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1565.002: Transmitted Data Manipulation; T1608: Stage Capabilities; T1608.001: Upload Malware</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
ChamelGang (aka CamoFei)</td><td>China</td><td rowspan="3">East Asia, South Asia, North America, South America, and Europe</td><td rowspan="3">Aviation, Business Services, Construction, Consulting, Critical Infrastructure, Education, Finance, Food, Gambling, Government, Healthcare, Legal, Manufacturing, Media, Non-Profit, Research, Retail, Software, Textiles</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>CatB Ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1003: OS Credential Dumping; T1016: System Network Configuration Discovery; T1068: Exploitation for Privilege Escalation; T1046: Network Service Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1082: System Information Discovery; T1482: Domain Trust Discovery; T1078: Valid Accounts; T1018: Remote System Discovery; T1069.002: Domain Groups; T1560.001: Archive via Utility; T1136.002: Domain Account; T1069.001: Local Groups; T1219: Remote Access Software; T1657: Financial Theft; T1490: Inhibit System Recovery; T1562.001: Disable or Modify Tools; T1486: Data Encrypted for Impact; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **thirteen exploited vulnerabilities** and block the indicators related to the threat actors **SneakyChef, ExCobalt, UAC-0184, Boolka, ChamelGang,** and malware **SugarGh0st, SpiceRAT, DragonForce, XWorm RAT, CatB Ransomware, InnoLoader, BMANAGER, GoRed Backdoor.**

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 **thirteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **SneakyChef, ExCobalt, UAC-0184, Boolka, ChamelGang,** and malware **SpiceRAT, DragonForce,** and **InnoLoader,** in Breach and Attack Simulation(BAS).

Threat Advisories

Phoenix UEFI Firmware Flaw Exposes Multiple Intel CPUs to Risk

SneakyChef Group Hits Governments Using SugarGh0st and SpiceRAT

DragonForce Unleashes Chaos with Leaked Lockbit Builder

ExCobalt's GoRed the Silent Infiltrator of Russian Sectors

UAC-0184 Strikes Ukraine with XWorm RAT

Boolka: From Scripting to Sophisticated Malware Attacks

Critical Vulnerabilities Patched in Progress Software's MOVEit

ChamelGang's Double Play: Strategy Beyond Encryption

InnoLoader Malware Stealth Mastery, Unique Instances per Download

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
SugarGh0st	Domains	account[.]drive-google-com[.]tk, account[.]gommask[.]online
	SHA256	8a563b3091b56eb0562f5442c90b4d28d4be2946a3dc4a225b4b96134f7e447b, d6bffa45aa2448b2fb584713395b742e02ef77c1d54f125cd501240e0dd91a13, 951a54d2c61c3257447c4ff5fd451ee581c76d3d4d88fa482b99f5410d7b7b6f, 8db5a7efe1a83e43cb4acdc596b0413b4beb54f9f8e13f978c07a6eeee6b8435, 31b7e97770ffe74dad914a37a78c8f9a7286c75b62b5fae1c4ec722837ad457e, e56537d09156bb77f4821d5ce005c7840ec41890de233d88a1152f68110098cf, 06056f83e93849124dc435166c1b463bf34bbf99ea5671221ddaf6641e3db4f4, 81ded17e368abc280db4d9f83fb0aebe1ec58eb7e4103f98f0fb5269c8696551, 8190e8990bb7bc860691ce2d3ff6015d7f9a0339e77aa7c6e5e3ae5209bd6f4c, 727bcb28eb0282a389bd2c82e3fac57a9c348aedee23d18c8d136bbd8803b642, 0b6dcf9ba14096c631bd9a3f90180c5f6ad9177a8283724146425b2f08b53e02, 653c3ea0ce07880ffe3a2acd735770cc2cbedb137cb5a29d4b059af5a569f98f, 2547f1a874c552da17abf6d5f88e626ed4bda71ca0bb39b2bc13b2d748a05409,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	862f6f60d6c145d99fb01476708c93e72f0b905ee54aba03904e92eaf3d8b2d9, 99ab797804684699925b70bdf2ecbbb878f4a86e7b971349036700c72ad15fb1, 653281c876250878eb503e4377c3f79bdfec31e94b27e5413a1b9f8f0f84a6a4, c8bfebff63e5f227aacb3a0aebcf40c973a4fbde6d37895c76498798e925cfb6, cac8c35fd03cc8698e53cafa64941be59870380ecedd2f4998e110787224241c, 18270dd537c3e2f02513b51c3a89814f4c34aa994aa8d823bc534fa39d95dde2, 4509575df3a0a791838f13405122def4eae7f5d2d8142f4830f6944ecd913f03, 823d23f1bcc76b08773e988be209b4a2f1cf99b094732cde395bc40f0729948e, 70359e4ce398ad356fd36f1f9306a570b36c552b83310332e5bf257f21cb1e9a, e2a8ffe20d91720516b242d0053ae58474be4205b9926993eab13e6662cb9a91, 267eec9cd5ff136364e0346d62df0cbb0294e0fb8f672685e785bf3ffddfb76e, 7ccb9b8964391360d6e122343d714301851c2332f0d50e037fe08591bd7c139d, 7caca38b67f9f629912f21bc0d76f8a5782fc62cccb93f53d2d07fd21fd30c33, 66f2712d989950e3b6c1f56a08b2e8689ea8a48bf84c7cee93583c7e78591f3c, b9a60ea9b1ac73e333b403f8471b5111a0ba67b60c9f0d7e44e2e290fccf6f42, 837164909df9b37bc31edcdb1207954337bad59a630b44f8ea06a594bcbe4035, 4cdc33e535d07e6519b1be0520349dedaefcc464734b24d1e656414100680efe, d31b5dd937655c14caff1cca6da88dc81f9cc523e119d43a9ac38dbb302eebbd, 21123d5bf92e763c4ef34fd4f9ddcb1b3a4a2c9ab0fd5657f4f30b0964979274, 75b39e923c69b488ae6981d314075f7e423ba2236150c20d41112db8f80a4827, 6071f84650b3226f60068f5f7a1dc7c7ec819ab7b6e8dcf34163838b966fda44b0, 510acd67d4c5fb45d6721283ed0eb4128347458ccb2b00feda9787f138c35278, 4f98dc3df220f41bce3c3a2714392279e68dd24a53c7c2f22a0a9850eb5d8476,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	2e2aef8948f5e2d93df7f4412fadc31500feb9035ceff18cce85393c6e230088, c0230704e1ee34666c40b2a3898666ba3929283ad0a86b63ab0fad6f4a0555ec, f7de8e94f280f9b943950a75ae78032c6501261a12650a6f757107bc8df6c3c2, bc73528b391f30acdd3c3a1674bc7973d3026c367142d72684facd68915851f6, e11908adf04627812cfa721189dfa06f884ceedff2dfa3b18578494995561716, 0fcc045db0d07ea4909a487273d313f796fa19ee8095a5272dfc5d6f3484f4ec, bdcc0bc3f5d022f99a1599c7cbed3aa2b6839e1e1d05ed2448dbd8b7ab34c784, 065f10e2a92b433a779c508e4add9c096b2891f5417fa183e58c8b8f7f9f8524, 87bda94d6b5ad0170c07abe540f530e797c6fec7410b30796e265cc21997d735, 401720fa24dc03cce8640b00d00c57676a8369ee49f456bd771a6ecbd81b82b6, 84572497f7022163bbb2e9885c942b1bcfa1793305c116ac898ee1b52ab6f898, 2f32e99c182f0f7cf6ff54d9d1a9d9f7e59823030d2a89e15890c2c8b1612caf, 57e3c92639027738e5a867d2f66d30a9509a96573d7a5eeee1c2a710faf9321c, 7528cf4daa8f0b4108ff220bc98f6046faf446653a3f98edc1d58350490d9fc8, b89ebfdfa9abb0ab618ebf2baf66b6cf27929d1e6599b3cb174c12e0a4c71d96, 6f8ccda88e0ff98c781ad6e027f4294eb54bff27a3ca1cd72aa83e4082013860, 162594cdb38526300af0db4acd13dd7a5a4ac07004bf32f887b6f1492361 60b7, f46b2a57ee2904ded87f6db77ed4373bfd71de12879bd939348ccb8fa8cc1403, a77789f32058b879d7e3831d2d20a885996b8f07694a954e1e717f0483660ccb, 984e8b3dda2c87bc8e3d21a05b07a8f52799c99aa45584aa2671efe62b5184c2, 3f23d9ffc16c5f455f7bd02bf57667efb3d0a645ffa13fa38e0a6f5022208dd4, 4e18b57c586b3bfb6bd825ecbee2bdfcce91c8414e40c0a7655edc327d62ac0f, f4ffced2a4c7f3e48f2a43e17e58f8feb0ad6cb2ad98fafc87d9a159230810fa,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	9483bccb2b0964d11b13ca01fba7ba6a21a531807d48eb3182ceaf7ed240ef2b, 26f92ea9f5eb220d9e544af757c57e5672971b9cd43b166e65c055b6978d6031, 2c8116dce38993762cdb687eab69786b9ccd1bd8c569dee8bef5a226579224bb, 4bcf097c19e18e3b3bfa4c45ebb4e67d565a0984211edf9e2fdc042b43141317, 67b648a7f0d24e5b56e83f73f9494be6a63f4d7372c960a2134054352c9c3490, 9ce558dc6af9c183d15012a5012a36184586e40f8a461a948192c3f055201766, b5953319cb28a0db7a70dff03949f1d98487456a273ac3cfb1f70f8cb3b07c18, e4b8fe0b0a87e5844deee4668d7638acd3ab9ea60a947eb1b32a4bd0691e5411, 7fffe1969dee2b4c72b4c5d0c75e493ecf6f3598a89d8538be3e7c53b898bbff, 6cb99d0073d2e6b7e15b22a74b98901dccb3c328d88f6e1c38b0af0379dd388c, 5a3811aee5156d928b2b634b512d382d89f8203cb883cab743a54cbc4f3f41f1, bfcfa5e291b0c9201344a73c8ef25c2912561e32c48af0ae0d30ad8199ffc8c4, c4a912f776579aa0126bbadd9261a4cd6efb3bcb5f5c7d64e96b11f3bdbc214b, f92c275dfd051481cb03557213195647dd7c68edf9f7beddcff0aadf298f371b, 1b14de17a12cdb92210b8543e3418c16f9fe00db3394fa74ab3a8f1c5904ecf0, c4e2301615cbab9abf2d94327bb7839df64d88fc5c508a2f33c3f0fc881be7c3, 066b3631682f63b4a44ecfa5b6dfb100d8052429a7e1c5b1ba8cab4832529f26, fb76bc19e177372d210bcfe9b1f35fb296b0b7cb64f0ad5075a64d06a3c85159, 2c4356614ddeb8085367167b301a8e437166142e738adb27bf26c09da3acae56, 4b1b7257fd376286501043eb27debc850300a674962068e044a34e697381d694, 0618b63352d0ae02d0f02ce8adf02d1c16fd56b18e903622bc95e520388743e0, 792ca7508ce158e20eff7b838fafb6120afc81b3677a84eb066810544ccf1577, 49fa747eee1bebed9bbb74b7b555f8018fb4e0e11f74349c2f7ac89a225d27f8,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	1b9604b50e8c0c6cf2496855a3c367d72fc447839fab708b20d649cf276f572a, 698c73f004e7f46bc371e0476193456071d9f7df9662cca7aa0e010b4fcedf57, 0986b26fcc87723d73e80c280f1bbc221fdb188ab8666f098caac6d896f1c4d1, 27ace9002f5bc7b3474ec3ec7ac72ed094fa2d29d9b2e8b5b1a787b50afd4f05, e498efd08ced0eccaebc4721cee807858d40fde428fd5ea61ce06272a25282a0, 26dfb13aea6f55e01f4dc54bb91ea7d9afd3bd73bd0c95b63345364ed149ff80, aa58e1b322877ff660961e18558488c49491a523a12373f95c41a1dfe60ad477, 43c40fe84b53b2573564331db15f5fea8cdf599d6c9c2f361dd154a9b78cd6aa, 3df795503a11b3c1a7ce3aeaf72f436ec9d7704c8189f9aa4abbc4f6db69d155, f0f587aa4eac787e4caf5f4b8795b7cc8a4c33fbb518ec2d616516076570f393, bae38315e5a6622d01b66db561efa206e698f3cb6157645dabd4f0267b8d2c91, 5779a2234b0531171625983798997847d56cdcd421cacf0a1860bbe4ba70b79, 35a9c2e8d911c8793a4b464633beaa2c6772601d6d58bf12c456e694a4adcf46, 220dd9d5ba1c6e087c8294eb01b7e0dfeb39b3a9c99567da102df44b2f04dbd7, dd4fc4760401b8dc37b0a823af19d0f7b5c2039704caf5327f8f8c6d00bd148c, d18cf366f549a8828dc02e6540a191b3625da36995806dab559d6b020fe74695, db6a8b9988ab1b83d8c1e6b5bd0a4bbf2baacf1ed84220026f9ae8a867e5eec2, e121a6c8cccecbe1a27c2003c255096f04c23f13b24a1f035775348f2aae53d0, daed820a32723e146e762343d0a32f041d21bd2e603b355b2f91d0bc7d98927c, 41bb112c6d4c609d53111ad1bb7cc687ec8ab848b6039c7a8eb64fee311b0822, 1c1499485254acb0d94ec6b4ffcb0c33d1dc154b5d95cc433a44c8bbb66c718f, f87c6b520253d9d6b14a443ea2096baeb8cf532e9cc8843f39e6168cd873669d, 4f02b04252b268bffdc6584ced29254209fcac4ba7388527efa43786cad17aaa,

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	33dc74a86e72a353412da885e5e07fe64b65f1769fe7ef17aa79b6bd6b36d0dc, f7cbe4349d4f95bbf08e1d649490fffe85e345976467bd1e0a066acfd3c2bb35, 88c6525924bf306dc21aada7898084622bf6a224465123025a53b1c187ff8ae9, 3edc38bb3ad101f6e56d99e4c9f173c16346315ec7bb36e3d7f327dbcbdcd606, 502a08fa74475ad5affeaac4a0f9e491df59a20c97796ce88284e79821ac8483, e71d4f329b7353f95f5f13f3fd33c4727f9f06f96083e199c18ad3cf1a2351fa, 6af30df6ee33ee44e93e34aed5fbe80bef0e7d1832d96f60c61e3eace5df315e, 65d96b763572ad2a7a03ab964225414de9fc7f4b820a603ef3f94f9203fbe4b2, d3da04c58d81445754a4a837f3784e5fa7ec54ceeb8e595a836e9b87dc0c39cd, 44bab852fa3bbaec1a03c900a8dace3c3553bf3c8289e5ffe9457633af0ea74a, b02bc37b60170d53ff9d17ae0f75e6df5cde7287cede634bcb0042545585dd90, 948ce1b8169805870338a59415ef470029323fc824a84bed9a760b2d78affb44, adfdf33b7f14b4509d1d1ec5155bb57ae381b6a04ebc97281a58d3246d7abaa3, 1a11ba0de41e053025e98f64d4b6ac044f6afd0db00fb91f97c447a4e63a5e78, 17c6aaa3efc51678cf4c269ba99e62859967c5d2a6da0303e66d60c1e04b20b6, 638ef4333b1b2993e945dbbc57f8a2a2ee0ab84bf02ef11a6a343a07f673784a, 40bd419635471cf6c8df65142cb1cadfc1ed88bb6f9f921abbdaf5041503bc96, bf30f0045791417fa1e691b4974d5651ffd4310a536f30df325fe89365f1fd70, 15929ca0bf26f189592cc6f2ba7fae8d10b0d84d86ecce2f74f583f7ebf849ed, 832225013088d9619cca1bfc3192652fb434a2442ec33316342969c330b46825, 1cd45dac19c6d340f604546504393060d9b313d5b16a85f947e19daebc41dee5, 1073bf25ac3af08cf3f48c2cbaed489ef43671387211d6e63f96aa7fcf1ec0b3, 543a1c4db82edce36ae07e4836b4d4a7640355bdf728d5ed41370892bf97d8a8, e39a3ceb034e425f4554df867871bb7c5df43ba116dea05b173c4bd444789aea

Attack Name	TYPE	VALUE
SugarGh0st	SHA256	4b1f3cc69e905137263ec8c39bbdcbccd5e33c3abffe54d77de847a998fcf17a, 48cc1d2df6ea2a04201e74ce59983a0bf0964d59a0e5c5647068b653a0ec66d5, 05758a568e30b3f35092b8d43bf4f29a3e5e9b988dc541d51fc8233ebbec2874, a22e16fad2d88de1a625201408b2262d8335bef3d944f4f696ad825973af124d, 7684296728c10249f671cf80b58e04633031e1b74a88e8b4f7d31776fc643d10, 375e0b117c7e45266e9544c23e226dd791ac32d094e60b858ff823577be43acb, 944cd95eaf496ad6dd8859032c4577ad6917dec3a4c300eeca762e08a97243f5, 6b327a15877528e5e5b0891fd587cb2fc932d94404c756401af628195eb94831, 8cd0026ba4f0c8984bdb6daaddb6fa17088e3b9272859cc2c03195d36f47f334, 06ac9bcbc1d026fbe9a261afe62a1b5704dc64b89a28dae47441fa6ef6230eb9, 2432f192511fb377d69619fc7eb0612570e22e3ba88fc42e841552a66fe2dc8f, 53e7e7fce0d8fde3be0d6679193f924555df217b696f6dc201e1966e9f4efabd, ac5342050b0ec85a122846510e06f861960c45613ecc05e3951c57d7d02aa716, 21cf0efec4def4a95af75a7bfdef915bf103a9a6cd03593b4f665f49cdbe4a02, 58754bf9701a39bf13959157db5761d19a562264ac79a8ae47b82589d17a1a07, 5f40142782f5e13334caf25f3038be324b3f47a3ee465f6da4442ec6e7920d5b,
SpiceRAT	IPv4	45[.]144[.]31[.]57, 94[.]198[.]40[.]4
	Domains	stock[.]adobe-service[.]net, app[.]turkmensk[.]org
	URL	http://94.198.40.4/homepage/index.aspx, http://stock.adobe-service.net/homepage/index.aspx, http://app.turkmensk.org/homepage/index.aspx

Attack Name	TYPE	VALUE
SpiceRAT	SHA256	6ca2415aabb806a871889c2ab48ad05b1ba444b5867ceadbcea3ab7f23de72f4, b84ebbe57151844ac7ac9fc5d488e4696f37f98779d13dceafe6c5a7f2219a4c, 0374a9812c7e43db1bde605cc3decff3d77c8b041b959a5422e4da0b60e0f6dc, 48c65bb99ce954df0ee492b92e634d602d621295be2ff87e57fcb07c8b33db8b, bd3d9bad4d460da08a4a3ae655e7c49b8435efd39ea4faa19ed052c7f65423ab, 598c2b0b15b7b35b93f7435aecbd377de66ac3ccc4b7af8edce1ce3bc6d773cd, e2330f64c92a49927098f8a07de9da8fc54c87a89dc549f6ebdcf3bc78732db2, 9d4283c05417c0b49a00c6e5159eb5bcb52142036f94fcdfb9712b231d020955, 197f3be195767142f1a4da0ad9e108c23993361d1a180b62749a9b84ed0b1a45, 4d4d8f9941fa5e378f6019d1a4e20bb70bce31db23720724ec35a373eb7ecf75, 9f1cd725116114ab72c772c99a4809f5870dfceebb1f47f24c68025e34e714f9, 427b6dc489cbfad36413fce6f71e82e158a6632c9986c1dee1af7676a129f048, dde3e5dca9e0498db558dd8e83f27143ad86cd0fcca1a33964ee4f3100682db8
DragonForce Ransomware	MD5	d54bae930b038950c2947f5397c13f84
	SHA1	e164bbaf848fa5d46fa42f62402a1c55330ef562
	SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b
	Tor Address	Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion, 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion

Attack Name	TYPE	VALUE
GoRed Backdoor	MD5	6ea3feb1888ce02e3d0d2857b5ef71c4, 64db61efc8acf370b91110b6f93d4dce, 63f6de3c86de55172b147b947f29c808, d3cd9d9bad6450e8fd4fd2e972639c69, cad5cb82baccd1f28e381e5c924f204a, 6f6e7fe49a8d5696f389e202d3b8c7e2, b5dc9a67f76fa18784b51fd3c5b9607c, caf68b393d56548074b9434564cb0625, b747c05888caf380edf6b2baab142272, 0385b0f83dbfc99c243ff066e3fe3cb2, 7dc1e49f1664af70d85d31af70f29071, fc3b7f47958f6c1c6a93a2f2f970734c, c02bee46d6a7a46f54e6abe003fec897, ad5c0363e7e28c69007f891fbc3dd030
	SHA1	c5540ec2ec79a21f07b0d793cc36b024a0db64cc, a81373d92d798418109552fb91d4c407d4c37a89, 5a504869350a4bdbcda22b09dbe7b05a7551a860, a190448a0c01a6e58610de27d022ccba0e755f79, 81861a853216f78219dd8cb0b4717d5d63260e7d 1d784e6c7d12fb7730895f21e4bfd3cde4b3900f, de243b57b087f5d1cde50db1949aa3744f1f6b5e, 680cb0a25e4a5148f5a1f7d3b75fad4fd345cdb0, ef50067027e27bea188023fa6a8ce9054c7d4ce9, 4f6164321d10c7a54a54398ccc7b11c1e7390e38, 1981f9a1d885c0ccb2d1f5910765a52d1989bc37, 8030f2430234426ab3bdc8cdd995be7c4805d7d2, 58d03630792f287184177660d9fd846fbde5416c, 3dd9bd38a8f8166b1af25cb523a9a6f25b1791df
	SHA256	67b7a8fad28dcc40c0889e5c4e40aef9348441c64bba74bd6d b885d88ce6d246, f43c99ef85166774ed47cad96c70b8273aa82c313e55bb08d9 c74e2b3f59b000, f91c9fd27bf0e3a7e82998721946ee70735ec46ee672ca80e3 062aa2d5195447, be246cdf932aa5b1c2ada0d74c8d1eca4028538b28fb61d7a8 d930b4266fd55c, ec36fcd64432843292d16f601a758ba4091ada906c5c4c4e54 0e326676911141, 41d35016c78f86eee8972808c7de8c200ff24625639adff5b9d 0ab8773fff6b4, aca34d7c3832879f6f7ebe8f7c59160896909574c94d1d12d7 c71b6f7918bc50, 8d055f3ad4d01f601df24a7c20ded981005adef7e6d2675041 5d1f95a471c2e3, 17e57c5e71b99a386b18728eac4a27e83415756071c9e8585 9940da41e94976b,

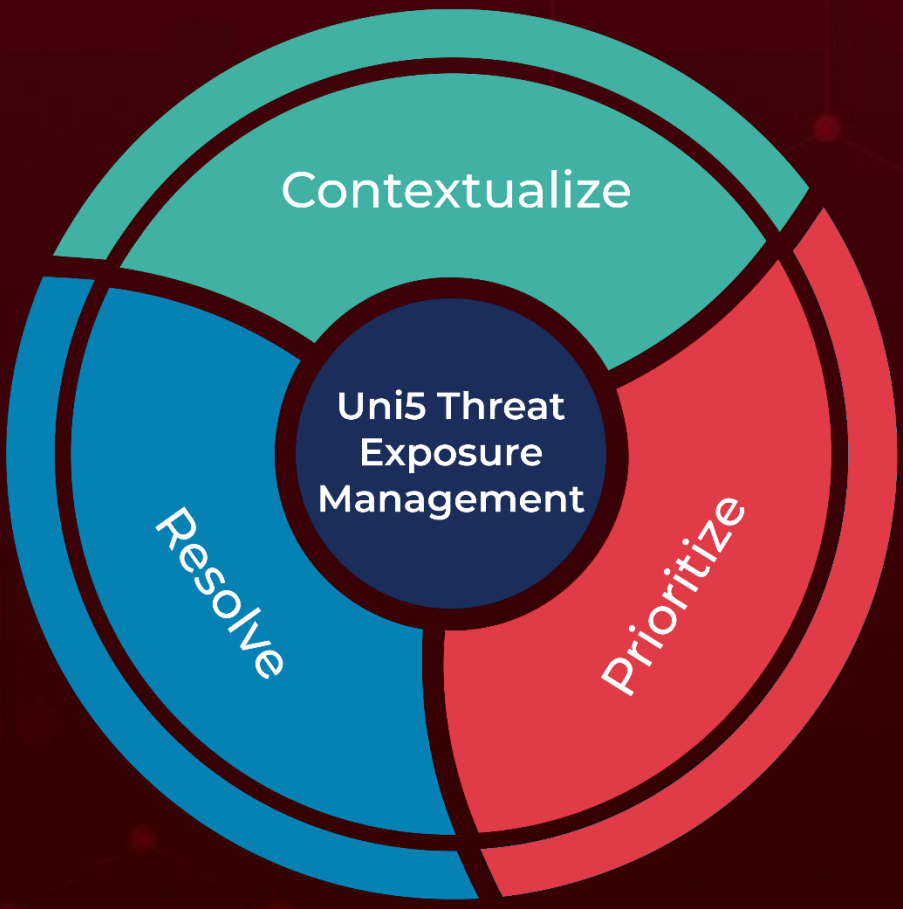
Attack Name	TYPE	VALUE
GoRed Backdoor	SHA256	32d76f2fe1188a131cb3219356639e83c60d47a703e40b8801a364d98e37128f, f3bb44d52e43477ce43c91eb8d9830e356fc105b96377edd6b190fcccda61e2f, ab801eaa9ad11199e1382a124d6024f9551a5a33ca1b9e5cafc0098621abb91f, e2b2ebe1b82d1c122dc2750f318f2484fe5361fcd964bfdcdcae631cf32f8d37, 4561a38ff34cc71cc73d54e2adfbd378f58d54596b012ff1841fdd7fc42063c3, f56b7fbc5dda7e46aff1b7753a1edb1f6fad5c8953dd3dbff30b3d8675b1dbd3
XWorm RAT	SHA256	0d16de10ce708b990d1b0ae26ac12792c91864426c88a8c73a475f7f33db014b, dd8377e9c3620d0732bededcd0d219f77f7bcffbc49470a9b7ff22db33fe4a185
BMANAGER	SHA256	7266f20123edcb2e0b92ac0b63225b8db2c5ff349818b339ef1553bff06719e4
	URL	hxxp[:]//updatebrower.com/download/bmanager[.]txt
	Domains	mainnode[.]beonlineboo[.]com, node[.]beonlineboo[.]com
CatB Ransomware	Bitcoin Address	bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
	SHA256	35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b, 512587a73cd03c6324ade468689510472c6b9e54074f3cf115aa54393b14f037, 9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2, 83129ed45151a706dff8f4e7a3b0736557f7284769016c2fb00018d0d3932cfa, 3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642, c8e0aa3b859ac505c2811eaa7e2004d6e3b351d004739e2a00a7a96f3d12430c
InnoLoader	Domains	valuescent[.]website, caretouch[.]hair, whipunit[.]hair, eyesnose[.]hair, nightauthority[.]xyz, cattlebusiness[.]icu, monkeyagreement[.]fun, laughvein[.]hair, brotherpopcorn[.]website, selectionword[.]xyz

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

July 1, 2024 • 5:30 AM

More at www.hivepro.com