Date of Publication
December 11, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

04 DECEMBER to 10 DECEMBER 2023

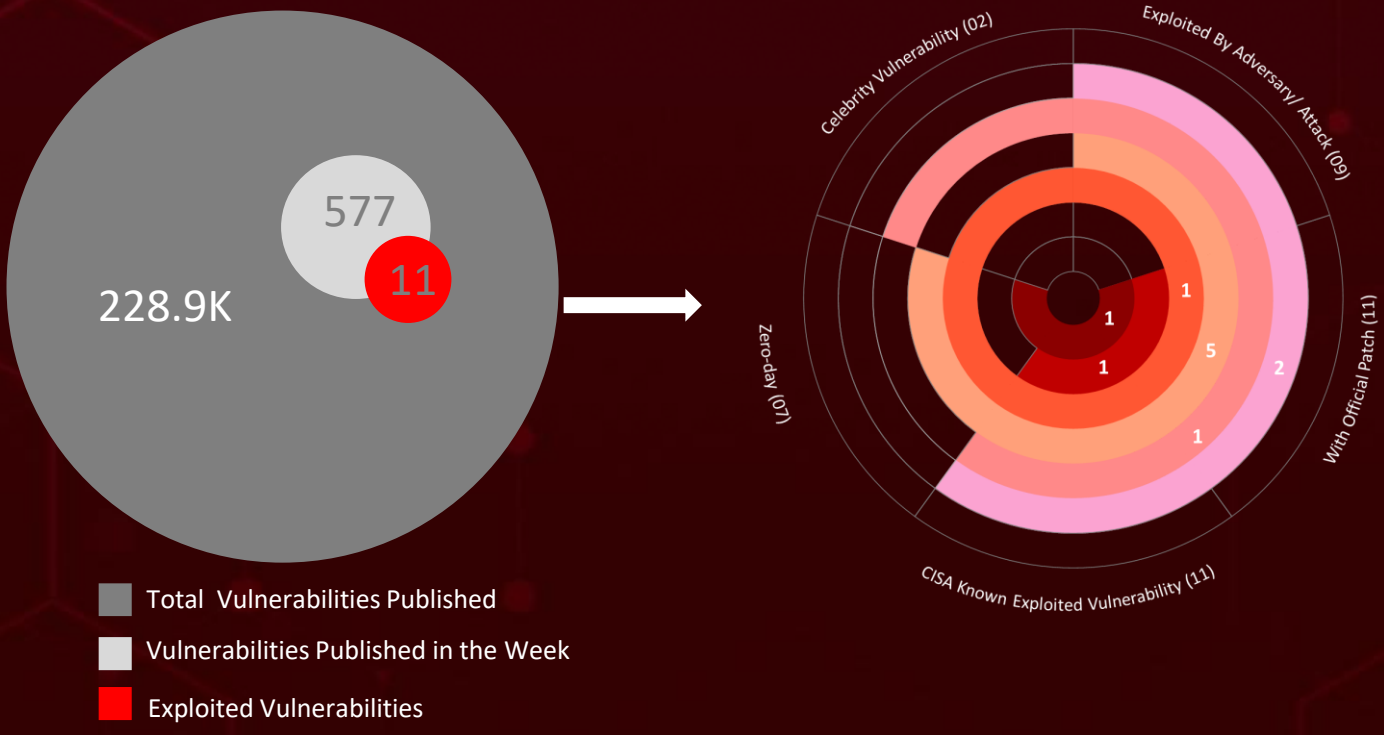
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **eleven** attacks were executed, **eleven** vulnerabilities were uncovered, and **four** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs revealed that among the seven zero-day vulnerabilities, one in WinRAR is being consistently exploited by Threat Actors including **APT28**, an APT group with Information theft and Espionage motivations. Additionally, a vulnerability was identified in **Adobe ColdFusion**, zero-day flaw exploited by attackers widely.

The **Crucio Ransomware** is actively used by CyberAv3ngers group with the goal of disrupting systems and networks. These attacks are on the rise, posing a significant threat to users in United States of America and Israel.



High Level Statistics

11
Attacks Executed

11
Vulnerabilities Exploited

4
Adversaries in Action

- SugarGh0st RAT
- Gh0st RAT
- Crucio Ransomware
- Agent Racoon
- Ntospy
- BlueSky Ransomware
- Tor2Mine
- DanaBot
- AsyncRAT
- KrasueRAT
- XorDdos Trojan

- CVE-2023-26360
- CVE-2023-27350
- CVE-2022-30190
- CVE-2023-23397
- CVE-2023-38831
- CVE-2021-40444
- CVE-2021-42292
- CVE-2021-42321
- CVE-2021-34473
- CVE-2020-17144
- CVE-2020-0688

- CyberAv3ngers
- AeroBlade
- Star Blizzard
- APT28

Insights

KrasueRAT
A new Linux Remote Access Trojan, targets Thai organizations

BlueSky Ransomware
Deployed worldwide by exploiting **CVE-2023-27350**

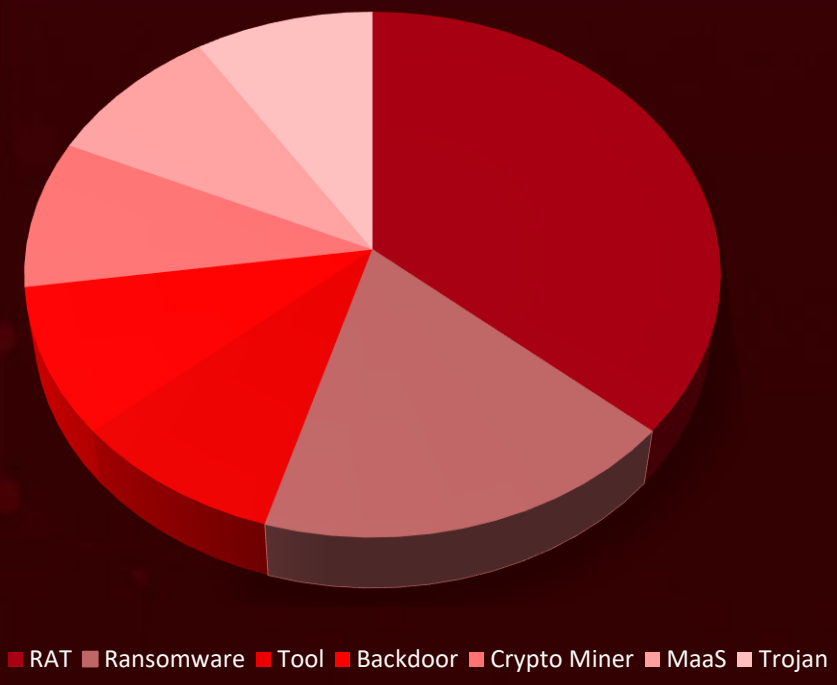
SugarGh0st RAT
A variant of Gh0st RAT, exhibits advanced features for remote control

DanaBot
Multistage MaaS Malware, distributed through phishing campaigns

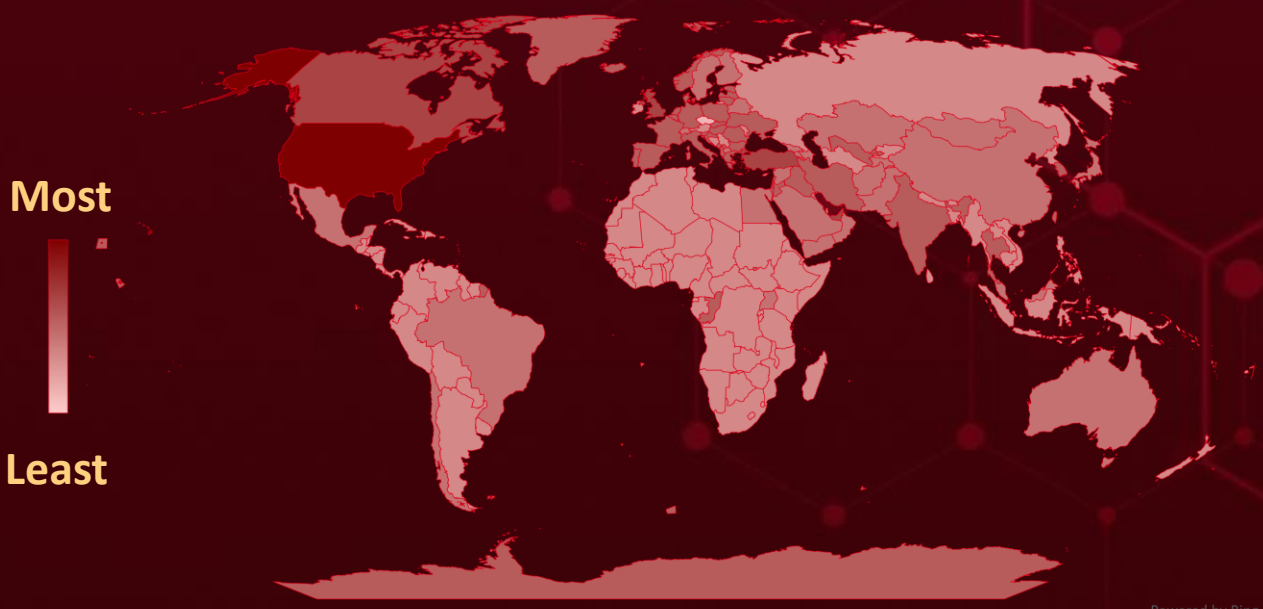
CVE-2023-26360 Zero-Day
Targets government servers, leading to potential unauthorized code execution

APT28
Consistently exploiting number of vulnerabilities for initial access

Threat Distribution



Targeted Countries



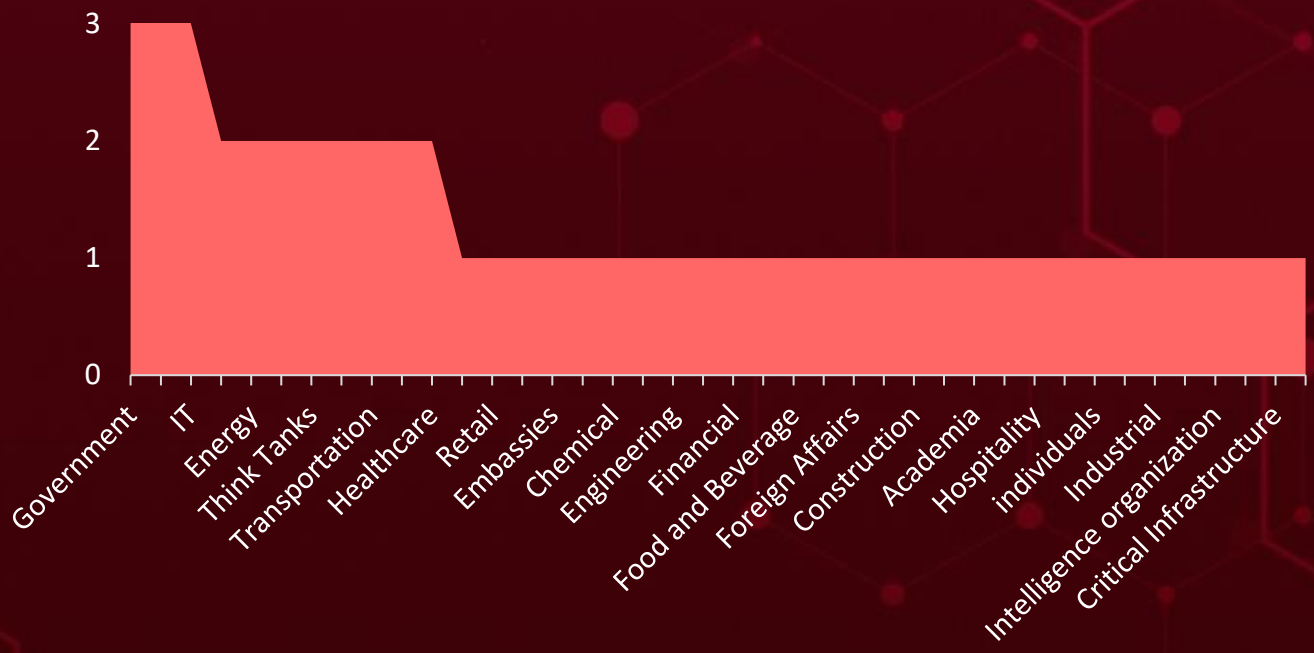
Countries
USA
Turkey
UK
Canada
UAE
Latvia
Portugal
Montenegro
Denmark
South Korea
Estonia
Lithuania
France
Norway
Germany
Slovakia
Greece
Thailand
Hungary
Lebanon
Iceland
Luxembourg
India
Netherlands
Iran
Poland
Iraq

Countries
Romania
Israel
Slovenia
Belgium
Spain
Bulgaria
Croatia
Albania
Italy
Ukraine
Jordan
Uzbekistan
Finland
Australia
Switzerland
Mexico
Chile
Mongolia
Brazil
China
Tajikistan
Bahrain
Uganda
North Macedonia
Japan
Cyprus
Kazakhstan

Countries
Oman
Sweden
Pakistan
Syria
Belarus
Georgia
Egypt
Afghanistan
Qatar
Azerbaijan
Armenia
Malaysia
Saudi Arabia
Kuwait
Yemen
Palau
St. Vincent & Grenadines
Sao Tome & Principe
Guinea-Bissau
Turkmenistan
Guyana
Ecuador
Haiti
Eritrea
Holy See
Tanzania

Countries
Honduras
Guatemala
Andorra
Peru
Brunei
Saint Kitts & Nevis
Austria
Seychelles
Indonesia
Belize
Burkina Faso
Ethiopia
Burundi
Tonga
Ireland
Ghana
Cabo Verde
Djibouti
Cambodia
Papua New Guinea
Jamaica
Dominican Republic
Cameroon
Russia
Angola
Samoa

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/ Decode Files or Information	**T1071.001** Web Protocols	**T1053.005** Scheduled Task
T1059.003 Windows Command Shell	**T1110** Brute Force	**T1055** Process Injection	**T1560** Archive Collected Data	**T1564** Hide Artifacts
T1583 Acquire Infrastructure	**T1566** Phishing	**T1036** Masquerading	**T1070.004** File Deletion	**T1059.001** PowerShell
T1071 Application Layer Protocol	**T1566.001** Spearphishing Attachment	**T1070** Indicator Removal	**T1078** Valid Accounts	**T1566.002** Spearphishing Link

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SugarGh0st RAT	SugarGh0st is a customized variant of the Gh0st RAT. SugarGh0st is equipped with some customized features in its reconnaissance capability in looking for specific ODBC registry keys, loading library files with specific file extensions and function name, customized commands to facilitate the remote administration tasks directed by the C2, and to evade earlier detections.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	-
RAT			PATCH LINK
ASSOCIATED ACTOR			
-			-

IOC TYPE	VALUE
Hostname	account[.]drive-google-com[.]tk, login[.]drive-google-com[.]tk
IP	103[.]148[.]245[.]235, 103[.]108[.]67[.]191
SHA256	8584094f79fce97321ee82ca5da41b6830ecc6a0921bcaddb8dd337827cd7d1a, 3436135bb3839521e7712882f0f6548aff78db66a1064408c49f820a0b85d980

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gh0st RAT	Gh0st Rat is a Windows malware that can remotely control a computer to log keystrokes, take screenshots, execute arbitrary commands, download and install additional malware.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6

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
Crucio Ransomware	It is a customized Ransomware designed to infiltrate and exfiltrate data from key Israeli targets.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		infiltrate and exfiltrate data	-
ASSOCIATED ACTOR			PATCH LINK
CyberAv3ngers			-
IOC TYPE	**VALUE**		
MD5	BA284A4B508A7ABD8070A427386E93E0		
SHA1	66AE21571FAEE1E258549078144325DC9DD60303		
SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agent Racoon	Agent Racoon is a malicious program written using the .NET framework. This malware creates a communication channel with its C&C server by leveraging the DNS protocol.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Execute commands and exfiltrate data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	**VALUE**		
SHA256	4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, e0748ce315037253f278f7f8f2820c7dd8827a93b6d22d37dafc287c934083c4, baed169ce874f6fe721e0d32128484b3048e9bf58b2c75db88d1a8b7d6bb938d		
File Path	c:/windows/temp/onedriveupdater.exe, c:/windows/system32/msmdlb.exe		

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
Ntospy	This malware is a Network Provider DLL module designed to steal user credentials.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Tool		Steal Credentials	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e30f8596f1beda8254cbe1ac7a75839f5fe6c332f45ebabff88aadbce3938a19, 1a4301019bdf42e7b2df801e04066a738d184deb22afcad9542127b0a31d5cf, e7682a61b6c5b0487593f880a09d6123f18f8c6da9c13ed43b43866960b7aa8e, 58e87c0d9c9b190d1e6e44eae64e9a66de93d8de6cbd005e2562798462d05b45, 7eb901a6dbf41bcb2e0cdcbb67c53ab722604d6c985317cb2b479f4c4de7cf90		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlueSky Ransomware	BlueSky Ransomware is a modern malware using advanced techniques to evade security defenses. It predominantly targets Windows hosts and utilizes the Windows multi-threading model for fast encryption.	Phishing emails, phishing websites, and trojanized downloads	CVE-2023-27350
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data	PaperCut MF and NG
ASSOCIATED ACTOR			PATCH LINK
-			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219
IOC TYPE	VALUE		
MD5	7b68bc3dd393c2e5273f180e361f178a		
SHA1	07610f11d3b8ccb7b60cc8ad033dda6c7d3940c4		
SHA256	e6b413c8b8b2dfc4d8879acf85981a64020f094dcff27aa95f500f4be600bc67, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24, 5cda02a670505a523a18df8cbb216b77dc3f69f3ec22d7ee90f1d1dae1eddf10		

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
Tor2Mine	Tor2Mine is based on XMRigCC and uses a script that attempts to disable malware protection, execute a miner payload, and harvest Windows credentials.	Exploiting Vulnerability	CVE-2023-27350
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Crypto Miner		Harvest Credentials	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

IOC TYPE	VALUE
MD5	9e88c287eb376f3c319a5cb13f980d36, 08bdf000031bbad1a836381f73adace5
SHA1	3dff4ae3c421c9143978f8fc9499dca4aed0eac5, 501af977080d56a55ff0aeba66b58e7f3d1404ea
SHA256	f955eeb3a464685eaac96744964134e49e849a03fc910454faaff2109c378b0b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DanaBot	DanaBot is written in Delphi programming language, capable of stealing credentials and hijacking infected systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
MaaS		Data theft for financial gain	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	8ffd4fd0e29d6888e9eaf78a6f698436f8a4477cdba8b6271015f7b012d1f8e0, 67540a00b6fa011944ba222eb8b83f877aa75328204dbd02b242ad9a678d1a83, e7351978a0011be925a7831e37a82750c51b2ef5e913b42d69b3d509fe8e6b8a, 2cf2d35802c12f09cc2700baf30816c6155a6095651dad6bfff440d1c772e0d9, 7a3996fdfa138ac0d4692820c82e1ae23fd5874c8c7bd89c11b56d5cd31480dd

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a malware known for stealing credentials and executing various malicious activities since 2019. Its recent variant, distributed through WSF script files, employs sophisticated fileless techniques. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system.	distributed through WSF script files	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal Credentials	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IP	185[.]81[.]157[.]242		
MD5	0a80a592d407a2a8b8b318286dc30769, 61b7507a6814e81cda6b57850f9f31da, 750dc2354b0454eafd66900687a0f7d6		
SHA1	316b99a2bf664ccd94eb050005975c52806d2163		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KrasueRAT	The Krasue rootkit is a Linux Kernel Module (LKM) and targets Linux Kernel versions 2.6x/3.10.x. The rootkit masquerades as a VMware driver and does not contain a valid digital signature.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft for financial gain	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IP	128.199.226[.]11		
MD5	100a5f3875e430f6de03d99752fbb6a7, 5055925b5bcd715d5b70b57fdbeda66b		
SHA1	051bc3273a20a53d730a3beaff2fadcd38d6bb85, eddb4476ca610f3c5e895f4811c9744704552d2f		

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
XorDdos Trojan	XOR DDoS is a Linux Trojan malware with rootkit capabilities that was used to launch large-scale DDoS attacks. Its name stems from the heavy usage of XOR encryption in both malware and network communication to the C&Cs. It is built for multiple Linux architectures like ARM, x86 and x64.	Launch brute force attack	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Collect data, execute commands, launch DDoS	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	ce0f1914e0f0748f85ecc18d8470de2a0b2b60be7eaab7a459899f77993e82e6, 664fd170b1d07e372b3daa91aab78a8151d3f0b0361a2b3157b405314dd219a2, c0b0225201fd3a4c08245e58bbb4b844e0d3426e89b9ac3fc34db37d994fb182, 44046ce4a3a47b4d22ac7697817bfc16e18d835a33f0898c3e4df359c33d158c, 2154547c69bf8bee7f296bd8ce56ffa4115da65c2308e9fc6d5079b2eb9dec93		

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26360	✗	ColdFusion: 2016 update 15 and earlier versions ColdFusion: 2021 Update 5 and earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:2021:Update 5:*:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities	https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350	✗	PaperCut MF: before22.0.9 PaperCut NG: before22.0.9	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*:*	BlueSky Ransomware, Tor2Mine
PaperCut MF/NG Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190		Windows Server: 2008 – 2022, Windows: 7 – 11 21H2	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
FOLLINA (Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23397		Microsoft Windows	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps::*:*:*:enterprise:*:*:*	-
Microsoft Office Outlook Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-294	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	 ZERO-DAY	WinRAR version 6.22 and older versions	APT28
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	-
RARLAB WinRAR Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40444	 ZERO-DAY	Windows Server & Microsoft Internet Explorer	APT28
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
Microsoft MSHTML Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42292	✗	Microsoft Office & Excel	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:excel:2013:sp1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:*	-
Microsoft Excel Security Feature Bypass	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42292

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42321	✗	Microsoft Exchange Server	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_21:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_22:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_10:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_11:*:*:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42321

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473		Microsoft Exchange Server	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	-
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-17144		Microsoft Exchange Server	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_31:*:*:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-17144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-0688		Microsoft Exchange Server	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_30:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_14:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_15:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_3:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_4:*:*:*:*:*:*	-
Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers)</td><td>Iran</td><td rowspan="3">Critical Infrastructure (specifically Water and Wastewater Systems), Energy, Food, Beverage, Manufacturing, Healthcare, and Shipping</td><td rowspan="3">United States of America and Israel</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>Crucio Ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0006: Credential Access; TA0007: Discovery; TA0001: Initial Access; TA0040: Impact; T1110: Brute Force; T1584: Compromise Infrastructure; T1552: Unsecured Credentials; T1190:Exploit Public-Facing Application; T1057: Process Discovery; T1486: Data Encrypted for Impact</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 AeroBlade	Unknown	Aerospace	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1001: Data Obfuscation; T1016: System Network Configuration Discovery; T1027: Obfuscated Files or Information; T1598.002: Spearphishing Attachment; T1029: Scheduled Transfer; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1071.001: Web Protocols; T1082: System Information Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1106: Native API; T1137.001: Office Template Macros; T1140: Deobfuscate/Decode Files or Information; T1203: Exploitation for Client Execution; T1204.002: Malicious File; T1221: Template Injection; T1559.002: Dynamic Data Exchange			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto)</td><td>Russia</td><td rowspan="2">Academia, Defense, Governmental Organizations, NGOs, Think Tanks and Politicians</td><td rowspan="2">Canada, India, Lebanon, UAE, Ukraine, USA, NATO, UK</td></tr>
<tr><td>MOTIVE
Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs
-</td><td>ASSOCIATED ATTACKS/RANSOMWARE
-</td><td>AFFECTED PRODUCTS
-</td></tr>
<tr><td colspan="4">TTPs
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; T1593: Search Open Websites/Domains; T1078: Valid Accounts; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.002: Email Accounts; T1583: Acquire Infrastructure; T1583.001: Domains; T1586: Compromise Accounts; T1586.002: Email Accounts; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1550: Use Alternate Authentication Material; T1550.004: Web Session Cookie; T1539: Steal Web Session Cookie; T1114: Email Collection; T1114.002: Remote Email Collection; T1114.003: Email Forwarding Rule</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Diplomatic, Education, Electrical, Embassies, Energy, Engineering, Financial, Foreign Affairs, Government, Healthcare, Industrial, Information Technology, Intelligence organization, IT, Logistics, Media, NGOs, Oil and gas, Telecommunications, Think Tanks, Transit Pipeline, Transportation, Utilities	Afghanistan, Albania, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, North Macedonia, Norway, Pakistan, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, SouthAfrica, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, United Arab Emirates, Uganda, United Kingdom, Ukraine, United States, Uzbekistan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-30190 CVE-2023-23397 CVE-2023-38831 CVE-2021-40444 CVE-2021-42292 CVE-2021-42321 CVE-2021-34473 CVE-2020-17144 CVE-2020-0688	-	Microsoft Windows, RARLAB WinRAR, Windows Server & Microsoft Internet Explorer, Microsoft Office & Excel, Microsoft Exchange Server

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; T1134: Access TokenManipulation; T1098: Account Manipulation; T1583: Acquire Infrastructure; T1588.006: Vulnerabilities; T1588.005: Exploits; T1560: Archive Collected Data; T1110: Brute Force; T1059: Command and Scripting Interpreter; T1586.002: Email Accounts: T1005: Data from Local System; T1140: Deobfuscate/Decode Files or Information: T1114: Email Collection; T1203: Exploitation for Client Execution; T1068: Exploitation for Privilege Escalation; T1498: Network Denial of Service; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1057: Process Discovery; T1221: Template Injection; T1204.001:Malicious Link; T1078:Valid Accounts; T1588: Obtain Capabilities

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eleven exploited vulnerabilities** and block the indicators related to the threat actors **CyberAv3ngers, AeroBlade, Star Blizzard, APT28** and malware **SugarGh0st RAT, Gh0st RAT, Crucio Ransomware, Agent Racoon, Ntospy, BlueSky Ransomware,, Tor2Mine, DanaBot, AsyncRAT, KrasueRAT, XorDdos Trojan**.

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 **eleven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the malware **SugarGh0st RAT, Gh0st RAT, Agent Racoon, Ntospy, BlueSky Ransomware, Tor2Mine, DanaBot, KrasueRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

SugarGh0st RAT A Customized Gh0st Variant in Cyber Espionage

Iranian APT Group ‘CyberAv3ngers’ Target U.S. Critical Infrastructure

Novel Tool Set Targeting Entities in the Middle East, Africa, and U.S.

AeroBlade Swoops Down on U.S. Aerospace Giants

Adobe ColdFusion Vulnerability Leads to Federal Agency Breach

From Brute-Force to BlueSky Ransomware

DanaBot Stealer: Multistage MaaS Malware Resurfaces

A New Face of AsyncRAT Utilizes WSF Scripts to Spread

Atlassian Addresses Critical RCE Flaws

Star Blizzard Continues to Refine Their Tradecraft for Evasion and Stealth

New Linux Krasue RAT Targeting Telecom Companies in Thailand

APT28's Tactical Exploitation of Critical Vulnerabilities

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 malicious 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 RAT	IP	103[.]148[.]245[.]235, 103[.]108[.]67[.]191
	Hostname	account[.]drive-google-com[.]tk, login[.]drive-google-com[.]tk
	SHA256	8584094f79fce97321ee82ca5da41b6830ecc6a0921bcaddb8dd337827cd7d1a, 3436135bb3839521e7712882f0f6548aff78db66a1064408c49f820a0b85d980, c758eed6660786097b63ac6748236b5b6084783703ea7ee2111e8f0bcaa3652e, 6dff111b6adc9e33bed20eae99bec779f1c29dd55895a71125cfbe3c90950eb2, 7c87451261dfce64fda987eb395694b5330fd958466c46c931440cd9dc227505, ddac61f918ed87b49ef15d05873e7f52b919758aef713145f6a7d538c714fa2e, f3ea4611c72d57eabf381d5639c3c8d1840cb005ed811f3038410fb2e04978c1, 9d9a0af09fc9065bacabf1a193cad4386b5e8e5101639e07efa82992b723f3b0, 5ad182c913f0b5cb6a34126137c335110d4c9472f5c745cb7a438d108b03b27c, 38c815729f34aef6af531edf3f0c3f09635686dbe7e5db5cb97eca5b2b5b7712, adb4eb33213fa81c8b6cc013a6f4a43fa8b70eb8027433cf4339b532cb6e84cf,

Attack Name	TYPE	VALUE
SugarGh0st RAT	SHA256	2e543adb701afd40affcb4c51bd8246398b0210bee641ca9aeffcca893c9e4a5, 7cacdc84a0d690564c8471a4f58ab192ef7d9091ab0809933f616010bbf6846a, 66982ebd5ebb75633723c7057a1e948ac3aafe3ff808397eb0c55c853c82f9e6, 21f19d87d2169c82efd76ddb1baa024a1e59b93f82d28f276de853fc3ef8b20e, 362fde3362e307af3787b9bf0b5c71f87b659a3217e054c4d0acea8b9e6d74b0, ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e, 9783c0eee31ce6c5f795ecf387025af5d55208ff2713c470af2042721ab38606, 410d7dc973d188cd0d962a59f48deb1cfc73adf37857765e90194f6e878d4488, bd0a1efe07fcb4af4bec1b2881a0711f0be34044680ad8cff958a68a70d4a914, ff0f28f96bbb6c80fc3823fe71d5e07e1a05b06986e82a2fbe324d68ba5ab2ea
Gh0st RAT	SHA256	83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6
Crucio Ransomware	MD5	BA284A4B508A7ABD8070A427386E93E0
	SHA1	66AE21571FAEE1E258549078144325DC9DD60303
	SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
Agent Racoon	SHA256	4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, e0748ce315037253f278f7f8f2820c7dd8827a93b6d22d37dafc287c934083c4, baed169ce874f6fe721e0d32128484b3048e9bf58b2c75db88d1a8b7d6bb938d, 3a2d0e5e4bfd6db9c45f094a638d1f1b9d07110b9f6eb8874b75d968401ad69c, 4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, 354048e6006ec9625e3e5e3056790afe018e70da916c2c1a9cb4499f83888a47, dee7321085737da53646b1f2d58838ece97c81e3f2319a29f7629d62395dbfd1
	File Path	c:/windows/temp/onedriveupdater.exe, c:/windows/system32/msmdlb.exe, c:/windows/temp/onedriveupdater.exe, c:/program files (x86)/google/update/googleupdate.exe, c:\windows\temp\mslb.ps1

Attack Name	TYPE	VALUE
Ntospy	SHA256	e30f8596f1beda8254cbe1ac7a75839f5fe6c332f45ebabff88aadbce3938a19, 1a4301019bdf42e7b2df801e04066a738d184deb22afcad9542127b0a31d5cfa, e7682a61b6c5b0487593f880a09d6123f18f8c6da9c13ed43b43866960b7aa8e, 58e87c0d9c9b190d1e6e44eae64e9a66de93d8de6cbd005e2562798462d05b45, 7eb901a6dbf41bcb2e0cdcbb67c53ab722604d6c985317cb2b479f4c4de7cf90, f45ea12579f636026d29009190221864f432dbc3e26e73d8f3ab7835fa595b86, bcd2bdea2bfecd09e258b8777e3825c4a1d98af220e7b045ee7b6c30bf19d6df
BlueSky Ransomware	MD5	7b68bc3dd393c2e5273f180e361f178a
	SHA1	07610f11d3b8ccb7b60cc8ad033dda6c7d3940c4
	SHA256	e6b413c8b8b2dfc4d8879acf85981a64020f094dcff27aa95f500f4be600bc67, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24, 5cda02a670505a523a18df8cbb216b77dc3f69f3ec22d7ee90f1d1dae1eddf10, 40bf3b2f344995352d9a9703c4e0fb12a752c105b9fb133d6cce7e9e5e99df4a, 2ee6dfbfb2afd7442c9f2212eb142876698851c3ffb552ee420c0281e35a836e, e32fc8ad818d2ef217aaa4f467c7a8af1dad88fdd5166186f732b2e233c90148, 11e409f8b0799cd64c53d40ff10cbc639a1f85cd5ba6544fe42689a96302cc2e, c72e5ff7858844e335fafdd54395be85d708cfb9a91ade6f398fc0f1c9b50919, 38478119e3344e735cf60442e7528db63046a543a5f422db8f946b2c2693d19a, 4fd0c22d92f8bf7a062497867a802bdbab4c802ac10c8b529fe7f896e7517492, 1b44b3e401f26547ee820bc0fe90904c55ec59d74e4385fe5bdd1826738fa9e6, 22a020af0e4be83dea45c0700d065d9ae64630748c02b58397f6c6d91c3efb0d, 4c752131e47710d47dd0084a22ac03cd5924eb617e97cf895159ae03d86f561e, 6e1057e52d296655f932b8a9da7302b31379ce5b9ba4cc32ed3af4c15c7adcf0, 905de085d2a9ebf553e3325eb9c878b9855f85c10f77e80c46519056658d6bab, d401be3ec0699cfdc1a16a9243ebc25181385e428122b0b1a283b7a8d47dd0bc,

Attack Name	TYPE	VALUE
BlueSky Ransomware	SHA256	99828018b3af892707985f6a3f8c3d34ae1d1575fdefd7a05f1e6861181ec1b2, afccc93c4122d7e63543fc342a4ba9319c4969797c0c3ed32b944b07c83aea16, 2176a3cdf5db56f5dcab475f362d459d4b2b3dafc3c146caaf3100009d0c8a5f, 11ae63b3a7caac549374aaa3c7fea9cba7f23ae83118745fee0a4157f61156f2, 18329783ad51783d679aec6111ca171eb1176f8fa866949a5267009c14605aa6, 9e302bb7d1031c0b2a4ad6ec955e7d2c0ab9c0d18d56132029c4c6198b91384f, 8dfd7ee796dd98daefbc1458a34f0460ebd8508df319d44ab48f4cbc579a7f09, baaa0e49398ef681ef71e84a7a86dd2b78f36ac83785e0d9a061067ebaf8b006, c0514cd580275b54f5b1d69086c9f415e7afb805479bfea50251e82dc2e60e12, 376fdb43699c90fd6cca2706c14827791137b3a753c7368a202de63f588fdb2f, 94733075d7ccdc9d770f71200e11f84c00b8a529182b504fb997e9b331470f9a, c3d5248230230e33565c04019801892174a6e5d8f688d61002e369b0b9e441ff, 311dc38f619f40f06bee5157119ab4b93684924f53e4ff2da34412f9dac111a4, 3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb, 840af927adbfdeb7070e1cf73ed195cf48c8d5f35b6de12f58b73898d7056d3d, 47971a5a44f487f341d482fdcb91271a2aea4d3eee7191c69568690d2fe9f251, 91795d3e8925e647444eb383e52cdc5046db10fa320afc817fab29b085e7d76f, 06ad123df8f3fcc6ca4785c0b52fc57e6e54f44e403fca2fdbd339580d3c53b0, d6386b2747335f7b0d13b1f69d995944ad8e9b71e09b036dbc0b907e583d857a, c75748dc544629a8a5d08c0d8ba7fda3508a3efdaed905ad800ffddbc8d3b8df, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec, 2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef, e75717be1633b5e3602827dc3b5788ff691dd325b0eddd2d0d9ddcee29de364f, 1c99798c7aaabba3c0af8e75b7af7bfde290448b7570c7fac43e02f2690e1248, b39fcf37d9019cc92127ee82c03df5e37aa8238cd76cc6eca2e3d1e7e977fc26, d4f4069b1c40a5b27ba0bc15c09dceb7035d054a022bb5d558850edfba0b9534

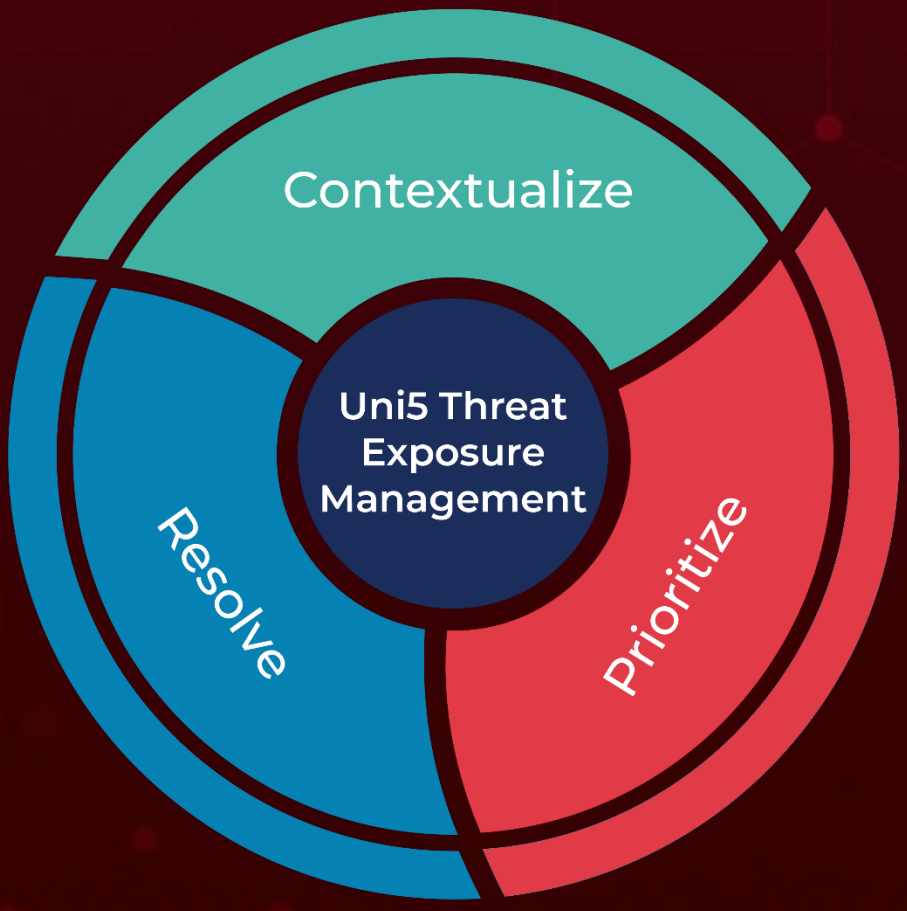
Attack Name	TYPE	VALUE
Tor2Mine	MD5	9e88c287eb376f3c319a5cb13f980d36, 08bdf000031bbad1a836381f73adace5
	SHA1	3dff4ae3c421c9143978f8fc9499dca4aed0eac5, 501af977080d56a55ff0aeba66b58e7f3d1404ea
	SHA256	f955eeb3a464685eaac96744964134e49e849a03fc910454faaff2109c378b0b, 74b6d14e35ff51fe47e169e76b4732b9f157cd7e537a2ca587c58dbdb15c624f
DanaBot	SHA256	8ffd4fd0e29d6888e9eaf78a6f698436f8a4477cdba8b6271015f7b012d1f8e0, 67540a00b6fa011944ba222eb8b83f877aa75328204dbd02b242ad9a678d1a83, e7351978a0011be925a7831e37a82750c51b2ef5e913b42d69b3d509fe8e6b8a, 2cf2d35802c12f09cc2700baf30816c6155a6095651dad6bfff440d1c772e0d9, 7a3996fdfa138ac0d4692820c82e1ae23fd5874c8c7bd89c11b56d5cd31480dd, a41d5274599dfe60823b477ea0dc20b9c8e9b398d8b287701f8cb02ea605ad84, 6eba004a9ea73c873bd66739431db34ebc3eb3928b9ecf0b89132ad473ef20b3
AsyncRAT	IP	185[.]81[.]157[.]242
	MD5	0a80a592d407a2a8b8b318286dc30769, 61b7507a6814e81cda6b57850f9f31da, 750dc2354b0454eafd66900687a0f7d6, 790562cefbb2c6b9d890b6d2b4adc548, a31191ca8fe50b0a70eb48b82c4d6f39, ac12d457d3ee177af8824cdc1de47f2a, b98e76816350a6a527fc311dae62b85e, c09266666ee71ade24e0e5f889cc8199
	SHA1	316b99a2bf664ccd94eb050005975c52806d2163, 3b10e9a10fc90e2a0a28f13a84c9b58eeb382dfc, 921bd5cb08b5c6a77a28e2864417bb8cdefafbf0
	SHA256	621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c, 70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75, a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387
	Hostname	drippmedsot[.]mywire[.]org
	URL	hxxp://drippmedsot[.]mywire[.]org:6606, hxxp://drippmedsot[.]mywire[.]org:7707, hxxp://drippmedsot[.]mywire[.]org:8808, hxxp://za[.]com/Order_ed333c91f0fd[.]zip

Attack Name	TYPE	VALUE
AsyncRAT	Hostname	drippmedsot[.]mywire[.]org
KrasueRAT	IP	128.199.226[.]11
	MD5	100a5f3875e430f6de03d99752fbb6a7, 5055925b5bcd715d5b70b57fdbeda66b
	SHA1	051bc3273a20a53d730a3beaff2fadcd38d6bb85, eddb4476ca610f3c5e895f4811c9744704552d2f
	SHA256	38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353, 3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59, 4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1, 8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831, 902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc, 97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772, afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4, b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d, c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5, e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632, ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f
XorDdos Trojan	SHA256	ce0f1914e0f0748f85ecc18d8470de2a0b2b60be7eaab7a459899f77993e82e6, 664fd170b1d07e372b3daa91aab78a8151d3f0b0361a2b3157b405314dd219a2, c0b0225201fd3a4c08245e58bbb4b844e0d3426e89b9ac3fc34db37d994fb182, 44046ce4a3a47b4d22ac7697817bfc16e18d835a33f0898c3e4df359c33d158c, 2154547c69bf8bee7f296bd8ce56ffa4115da65c2308e9fc6d5079b2eb9dec93, c9bd6d01eb7258fef88ec5c9276431c1db45f063b316f83943e45b6a40a76783, 4616bc3ba5c245946819c55db573b552ba1c0cc5e0c54c433ffb1824452fc609, a40d947d6a1d92c2789968ce0d2e6eb1734e248e2d30828c61a41f4ac840e8a0, 311c93575efd4eeeb9c6674d0ab8de263b72a8fb060d04450daccc78ec095151

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

December 11, 2023 . 6:20 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com