Date of Publication
April 23, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

15 to 21 APRIL 2024

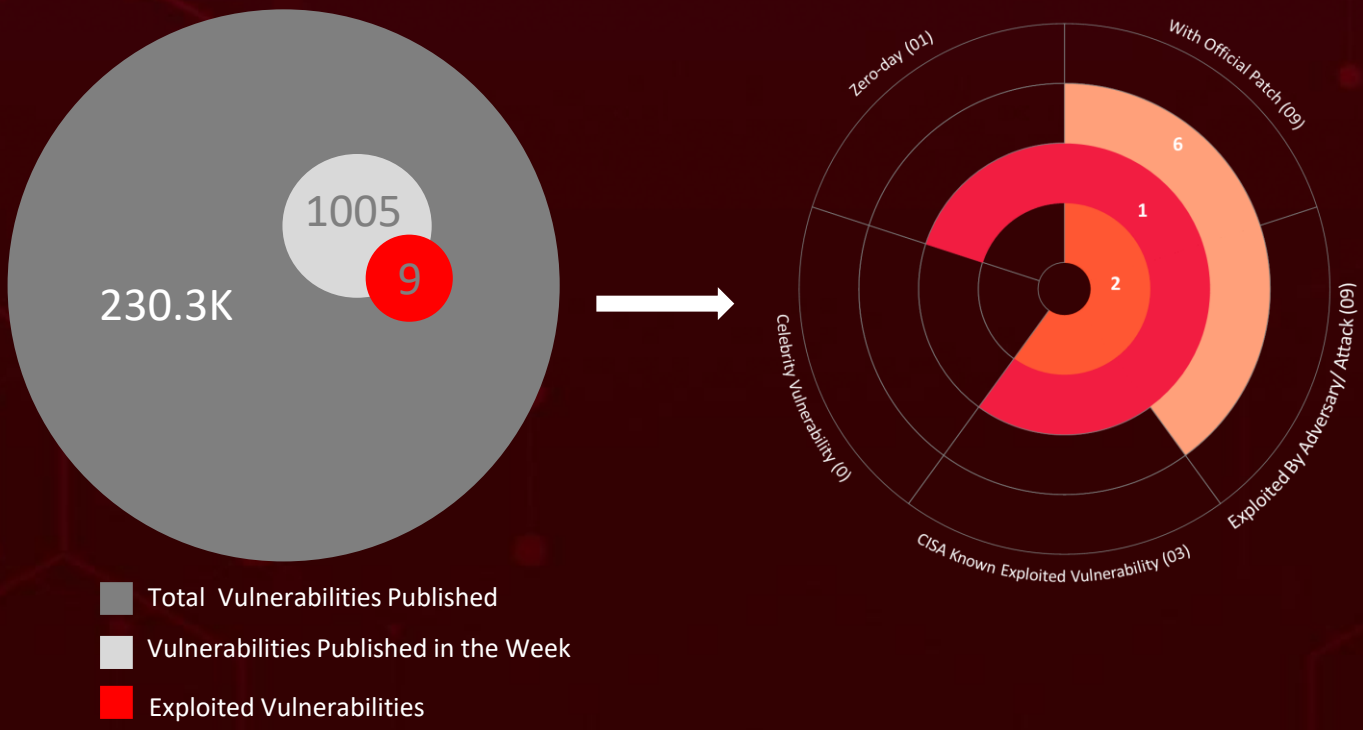
Table Of Contents

Summary

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

Furthermore, HiveForce Labs discovered that **UTA0218** threat actors are exploiting **CVE-2024-3400**. **CVE-2024-3400** is a critical vulnerability in Palo Alto Networks PAN-OS software's GlobalProtect feature, allowing unauthenticated attackers to execute code with root privileges, potentially leading to full device control.

FIN7 has been orchestrating a spear-phishing campaign targeting the U.S. automotive sector. Their method involved enticing victims with a complimentary IP scanning tool, which was a conduit for installing the notorious **Carbanak backdoor**. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

13
Attacks Executed

9
Vulnerabilities Exploited

4
Adversaries in Action

- DarkBeatC2
- UPSTYLE
- LockBit 3.0
- AgentTesla
- FormBook
- Remcos
- LokiBot
- Guloader
- SnakeKeylogger
- Xworm
- JsOutProx
- FatalRAT
- Carbanak

- CVE-2024-3400
- CVE-2023-48788
- CVE-2017-11882
- CVE-2024-28255
- CVE-2024-28847
- CVE-2024-28253
- CVE-2024-28848
- CVE-2024-28254
- CVE-2024-20295

- MuddyWater
- SOLAR SPIDER
- TA558
- FIN7

Insights

CVE-2023-48788

Fortinet FortiClientEMS Vulnerability exploited in **Connect:fun** campaign

Zero-Day in Palo Alto Networks PAN-OS

CVE-2024-3400 is a critical flaw in Palo Alto Networks PAN-OS, allowing unauthenticated attackers to execute code with root privileges, leading to full device control

FatalRAT's

Targeted phishing campaign primarily targeting cryptocurrency

Solar Spider

Is conducting a cyberattack campaign, employing JSOutProx RAT, targeting Financial sectors in APAC and MENA regions

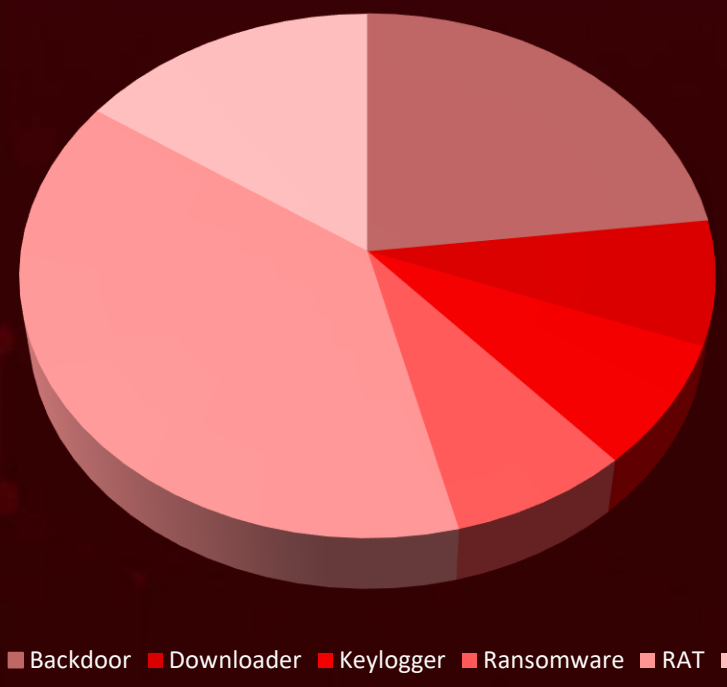
TA558 hacking group

In their recent campaign named SteganoAmor, is employing steganography to hide malicious code within images

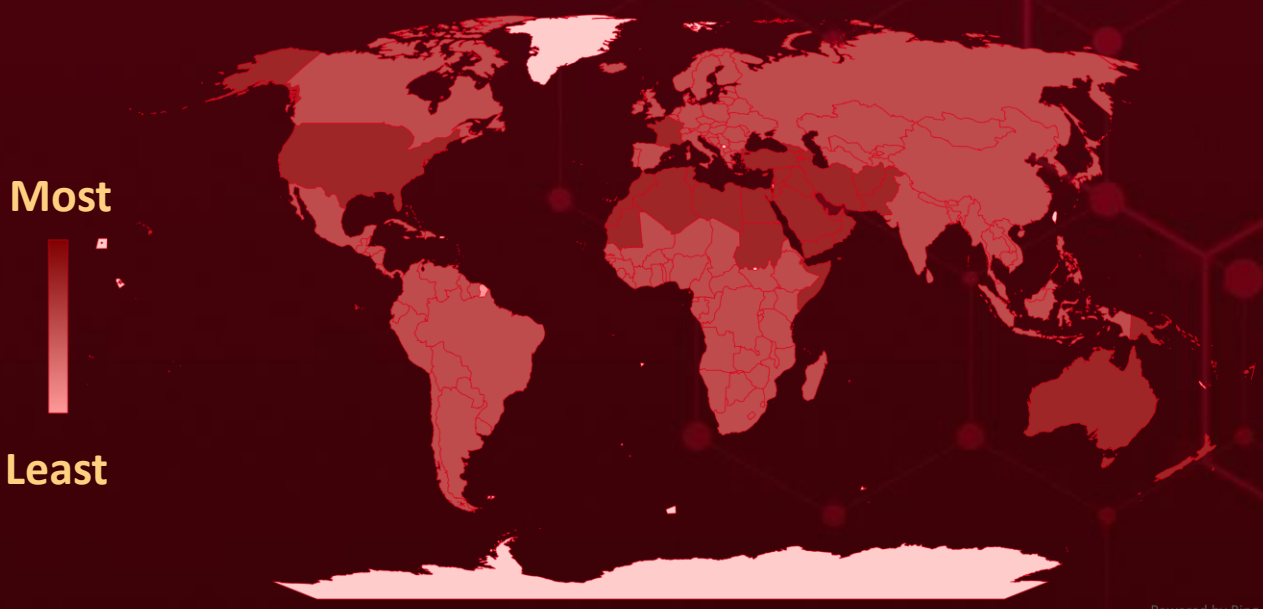
MuddyWater

The Iranian threat actor, has added a new C2 infrastructure named DarkBeatC2 to its arsenal

Threat Distribution

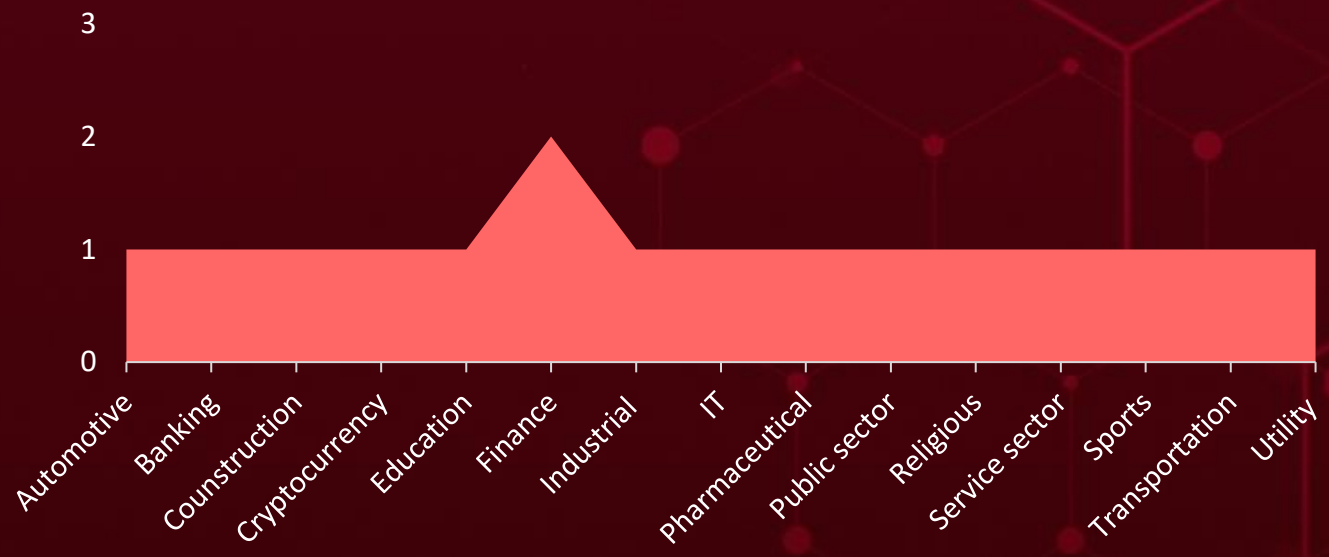


Targeted Countries



Countries	Countries	Countries	Countries
Israel	Oman	Brunei	South Africa
Saudi Arabia	Iraq	Czech Republic	Eswatini
Morocco	Palau	Slovakia	Suriname
Tuvalu	Papua New Guinea	Denmark	Ethiopia
Armenia	Qatar	Uzbekistan	Togo
Pakistan	Samoa	Argentina	Finland
Australia	Jordan	Burkina Faso	Costa Rica
Syria	Solomon Islands	Dominica	Austria
Azerbaijan	Kiribati	San Marino	Cuba
Yemen	Sudan	Dominican Republic	Gabon
Bahrain	Kuwait	Sri Lanka	Nepal
New Zealand	Tonga	DR Congo	Gambia
Cyprus	Lebanon	Congo	Niger
Algeria	Turkey	Ecuador	Andorra
Djibouti	Afghanistan	Namibia	Norway
Somalia	United Arab Emirates	Albania	Germany
Egypt	Malta	North Korea	Panama
Tunisia	Vanuatu	El Salvador	Ghana
Fiji	Marshall Islands	Paraguay	Philippines
United States	Mauritania	Equatorial Guinea	Greece
France	Libya	Rwanda	Romania
Micronesia	Tajikistan	Eritrea	Grenada
Georgia	Portugal	Serbia	Saint Lucia
Nauru		Estonia	Guatemala
Iran			Canada

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1566** Phishing
T1204 User Execution	**T1218** System Binary Proxy Execution	**T1083** File and Directory Discovery	**T1027** Obfuscated Files or Information	**T1204.002** Malicious File
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel	**T1555** Credentials from Password Stores	**T1588.005** Exploits	**T1068** Exploitation for Privilege Escalation
T1203 Exploitation for Client Execution	**T1566.001** Spearphishing Attachment	**T1574.002** DLL Side-Loading	**T1082** System Information Discovery	**T1055** Process Injection

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkBeatC2	DarkBeatC2, a malicious backdoor by Iranian hackers MuddyWater, infects systems through social engineering. It uses PowerShell scripts to silently load a hidden component (DLL) that grants remote access. This technique leverages legitimate functions for stealthy control of compromised devices.	Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Control and Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
MD5	3dd1f91f89dc70e90f7bc001ed50c9e7, Bede9522ff7d2bf7daff04392659b8a8, 32bfe46efceae5813b75b40852fde3c2, b7d15723d7ef47497c6efb270065ed84		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
UPSTYLE	Upstyle, a custom Python-based backdoor. Designed to grant attackers remote control, it facilitates additional commands and potentially establishes persistence on the compromised firewall.	Exploiting vulnerabilities	CVE-2024-3400
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	Palo Alto Networks PAN-OS
ASSOCIATED ACTOR			**PATCH LINK**
UTA0218			https://security.paloaltonetworks.com/CVE-2024-3400
IOC TYPE	**VALUE**		
SHA256	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078		
SHA1	988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9		
MD5	0c1554888ce9ed0da1583dbdf7b31651		

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
JsOutProx RAT	JsOutProx RAT is a Windows Trojan. Deceptive emails with attachments or website links trick users into downloading it. Once installed, attackers can steal your data, mess with your system, or install even worse malware. It's especially fond of targeting banks and financial institutions.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data breaches, financial losses, and data theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
SOLAR SPIDER			-
IOC TYPE	**VALUE**		
MD5	118b6673bd06c8eb082296a7b35f8fa5, 1bd7ce64f1a7cf7dc94b912ceb9533d0, 3a2104953478d1e60927aa6def17e8e7, 3d46a462f262818cada6899634354138, 66514548cdffab50d1ea75772a08df3d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agent Tesla	The Agent Tesla malware, classified as a remote access trojan (RAT), demonstrates remarkable proficiency in infiltrating systems to extract sensitive information like keystrokes and login credentials from web browsers and email clients.	Phishing	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	C54A3C60BC528E8594C813C61A2F929666E0F22A3CA837612B9CD48442721853, 97A6F1686F456A126C4FD823B01DF49814C71DBF4E2F3458CE9C62F89DE17719, D86EAA75FDBC0D2DE5B239974B02038200247B981ECC99074E86B5AD51A5906A, 02A2A2779ECD2CD887B97930A56FA5C8977A0D8FEC04D06BF3FB65ACB418FE9F, CA528EB30885238A7E594075C68AFE244602E2438DA103C98DDD81CBDEAFFA2E		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos, a legitimate remote access tool, is misused by attackers for total system control. It hides, escalates privileges, and persists on reboot. Phishing emails, exploit kits, and watering hole attacks are common delivery methods.	Phishing emails, exploit kits, and watering hole attacks	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Remote Control and Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	6FF46BDE6F6AB139C685F220E33230D1C064A6E62F68047F3E97BC8F04727E1E, 2E5B8A1ED53E25C5DDD9B7CD97B86627BAF197A7E3893909BCF33360BEDA2F7, D72B9F4910CBE10F8D1B3EEB7096F26412FCE2B735C9929C354D8F20265ABA50, 593CF342A669FCB1BFF594BD8CE85FC112BC19D42F7FCB0932C9AC5CDF70D0D9, D0947156CDD5831F8F4CEDE0B54E7A0B0D43EEAFC4F85532032A406F65736A69		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LokiBot	LokiBot, an information-stealing Android malware, targets your bank accounts. It lurks in seemingly harmless apps, stealing login details and bypassing two-factor authentication. Once LokiBot infiltrates your device, it can steal messages, spy on calls, and even grab your contacts.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss and Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	40B9D6C7BD8BBDC15EF53C7067C6282A37B1AFE5796F721ADEB42E2E606521FF, 6255A5B13CA4D4C4CA7A43EADA557F7F248B124690BA49E11535E1C6496EFFD8, 861AC33701D696AA03435C2A6A6985C76EE1A38AB86CAD1C21CDBD15237A35D, 5DB6A8DFAFD6956BEAF4127500CD5232D78D70165A1775FA1DA58277A43327D, A5748DCF451F0661BDB05C9075327BD7EA6CB654B05140F4F2DD0B169AC26BC8		

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
FormBook	FormBook, identified in 2016, is an infostealer malware. It infiltrates systems to pilfer diverse data like browser-cached credentials, screenshots, and keystrokes. Moreover, it functions as a downloader, facilitating the retrieval and execution of further malicious files.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	50413921860A4F9DB3C3AB95C68154E9FFD12726C64A4A46D141499FCF448288, C4333322E47F6528C43A77936DEA4BCF9230A3EC68C527D931D3C1C8F6232BAF, 2EA01DEF771F0E57B541D4819DD9A543C5ADB3A4452C6F5C03EAC2C49C542BF, 7C614154B6EC07D9D05E17100DA1B4223A07A5BE73F8002D0290B722B4C379C9, AA48EAF5253F8378F5E6DB8325D90E229E3D836080083C6269DE0969AF2854BA		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Guloader	Guloader malware acts like a secret agent, dropping off harmful payloads on your device. This sophisticated downloader, first spotted in late 2019, uses a variety of tricks to evade detection. It encrypts its malicious code, disguises itself within legitimate processes, and even alters its behavior if it suspects it's being analyzed.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Deploys other malware and Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	40B9D6C7BD8BBDC15EF53C7067C6282A37B1AFE5796F721ADEB42E2E606521FF, 6255A5B13CA4D4C4CA7A43EADA557F7F248B124690BA49E11535E1C6496EFFD8, 861AC33701D696AA03435C2A6A6985C76EE1A38AB86CAD1C21CDBD15237A35D, 5DB6A8DFAFD6956BEAF4127500CD5232D78D70165A1775FA1DA58277A43327D, A5748DCF451F0661BDB05C9075327BD7EA6CB654B05140F4F2DD0B169AC26BC8		

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
SnakeKeylogger	SnakeKeylogger, a sly keylogger and data thief, slithers past defenses, stealing your keystrokes, screenshots, and clipboard data. It uses email, FTP, and even Telegram to send this intel to attackers, putting your online accounts, privacy, and finances at risk.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Keylogger		Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	3B50796D11C0837412A2D9205F28604EF9C02EA436E33F9CB46AC3B99E1BBC37, 061EE3375DC3333D8C4266E773535E516206935D4F7DBBC3F0319D253840213D, F8C1925693A82D8A544BEDCF975160A6CBD8A0D0E2A463E402402D8D28AD6ED, 1624A0E8F86CF5331CCF66FD830A96827FC0B3DD842ABB268996D2387F2ED4BE, 07A1258C5EF18D86C00F843408AA21667C7817B8E7D1EAD1A5411856D0D21ED7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Xworm	XWorm, marketed as a malware-as-a-service, operates as a remote access trojan (RAT) with a comprehensive toolkit for hacking. It can extract sensitive information and files from compromised computers, seize control of MetaMask and Telegram accounts, and monitor user actions.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data breaches, financial losses, and identity theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	C0BD1EBDF30196EFE9F0F562DCCCC143ECE619994CA14170E88F87AD402CDFFA, CD9CA4735E5100ABF0163B9E2E7F63B35CD3DC0BA791E0540E15C94A13470289, F9D7569C8A07239001E8EB6E8915D922821F53A37328C67F390D64B8D594623D, E1DE5491FBADA68CDBFF98F68ED645BF8FDF62F21CF792FCA7CC556EF2D30A9F, AC009DA131ECC35C95B484248FCD3091F607D71F26F7421699B2A8C907B1EE04		

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 3.0	LockBit 3.0 ransomware also known as LockBit Black, that encrypts your data and might steal it too, threatening to leak it if you don't pay. Known for its evasive tactics, it targets enterprises and operates as a RaaS service.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	3B50796D11C0837412A2D9205F28604EF9C02EA436E33F9CB46AC3B99E1BBC37, 061EE3375DC3333D8C4266E773535E516206935D4F7DBBC3F0319D253840213D, F8C1925693A82D8A544BEDCF975160A6CBD8A0D0E2A463E402402D8D28AD6ED, 1624A0E8F86CF5331CCF66FD830A96827FC0B3DD842ABB268996D2387F2ED4BE, 07A1258C5EF18D86C00F843408AA21667C7817B8E7D1EAD1A5411856D0D21ED7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FatalRAT	FatalRAT, a Remote Access Trojan, initiated a targeted phishing campaign primarily targeting cryptocurrency enthusiasts, especially those utilizing the Exodus platform. This campaign strategically deploys FatalRAT alongside additional malware such as Clipper and Keylogger, specifically focusing on Chinese-speaking individuals and organizations.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data breaches, financial losses, and data theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d		

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
Carbanak	Carbanak Backdoor also known as Anunak, is a sophisticated backdoor equipped with data theft functionalities and a modular design. Its capabilities encompass keylogging, desktop video recording, VNC access, HTTP form interception, file system manipulation, file transfer, TCP tunneling, HTTP proxying, OS sabotage, theft of POS and Outlook data, and reverse shell functionality.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7			-

IOC TYPE	VALUE
SHA256	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
MD5	87aa5f3f514af2b9ef28db9f092f3249

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400	✗	Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 <11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	UTA0218
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	UPSTYLE
Palo Alto Networks PAN-OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48788	✗	FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*:*:*	Connect:fun Campaign
Fortinet FortiClientEMS SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882		Microsoft Office: 2007 SP3 2010 SP2 2013 SP1 2016	TA558
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*:*	AgentTesla, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203 : Exploitation for Client Execution, T1059 : Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28254		OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-j86m-rrpr-g8gw

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28255	✗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190 : Exploit Public-Facing Application, T1068 : Exploitation for Privilege Escalation	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-6wx7-qw5p-wh84

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28847	✗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-8p5r-6mvv-2435

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28253	✗	OpenMetadata versions prior to 1.3.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-7vf4-x5m2-r6gr

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28848	✗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-5xv3-fm7g-865r

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2024-20295</td><td>  </td><td rowspan="2">Cisco Integrated Management Controller: 3.2.6 - 4.12
Enterprise NFV Infrastructure Software: 3.12 - 3.13
Cisco 5000 Series Enterprise Network
Compute System: All versions
Catalyst 8300 Series Edge Universal CPE:
All versions
UCS C-Series Rack Servers in standalone
mode: All versions
UCS E-Series Servers: All versions</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:cisco:integrated_management_controller:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Cisco Integrated Management Controller CLI Command Injection Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-78</td><td>T1059.008: Network Device CLI, T1059 : Command and Scripting Interpreter</td><td>https://www.cisco.com/c/en/us/support/index.html</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)	Iran	-	Israel
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	DarkBeatC2	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1036: Masquerading; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1071: Application Layer Protocol			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
SOLAR SPIDER</td><td>-</td><td rowspan="3">Financial Services, Banking</td><td rowspan="3">APAC and MENA regions</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>JsOutProx RAT</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and: Control; TA0010: Exfiltration; T1036: Masquerading; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1055: Process Injection; T1027: Obfuscated Files or Information; T1212: Exploitation for Credential Access; T1056: Input Capture; T1082: System Information Discovery; T1567: Exfiltration Over Web Service; T1657: Financial Theft; T1566: Phishing; T1567.001: Exfiltration to Code Repository</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
TA558</td><td>-</td><td rowspan="3">Industrial sector, service sector, public sector, electric power industry, counstruction, Transportation companies, Sports, Information Technology, Education, Religious organizations, Finance, Pharmaceutical industry</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2017-11882</td><td>AgentTesla, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1132: Data Encoding; T1132.001: Standard Encoding; T1071: Application Layer Protocol; T1071.002: File Transfer Protocols; T1217: Browser Information Discovery; T1056: Input Capture; T1125: Video Capture; T1123: Audio Capture; T1033: System Owner/User Discovery; T1555: Credentials from Password Stores; T1204: User Execution; T1204.003: Malicious Image</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)</td><td>Russia</td><td rowspan="3">Automotive</td><td rowspan="3">USA</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td></td><td>-</td><td>Carbanak Backdoor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1027: Obfuscated Files or Information; T1021.004: SSH; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1057: Process Discovery; T1059.001: PowerShell; T1069.002: Domain Groups; T1082: System Information Discovery; T1087.002: Domain Account; T1090: Proxy; T1124: System Time: Discovery; T1204.002: Malicious File; T1222.001: Windows File and Directory Permissions Modification; T1543.003: Windows Service; T1562.004: Disable or Modify: System Firewall; T1564.001: Hidden Files and: Directories; T1566.002: Spearphishing Link; T1566: Phishing; T1571: Non-Standard Port; T1583.001: Domains; T1608.005: Link Target; T1569.002: Service Execution</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **MuddyWater, SOLAR SPIDER, TA558, FIN7** and malware **DarkBeatC2, UPSTYLE, LockBit 3.0, AgentTesla, FormBook, Remcos, LokiBot, Guloader, SnakeKeylogger, Xworm, JsOutProx, FatalRAT, Carbanak.**

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 **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **MuddyWater, SOLAR SPIDER, TA558, FIN7** and malware **DarkBeatC2, UPSTYLE, LockBit 3.0, JsOutProx, FatalRAT, Carbanak** in Breach and Attack Simulation(BAS).

Threat Advisories

MuddyWater Enhances Its Arsenal with DarkBeatC2 Framework

Zero-Day Flaw in Palo Alto Networks PAN-OS Patched After Active Exploitation

JSOutProx's Latest Incarnation Strikes Fear in Financial Circles

FortiClient EMS Vulnerability Exploited in Connect:fun Campaign

TA558's SteganoAmor Campaign Targets Organizations Worldwide

Vulnerability in PuTTY Client Allows Recovery of Private Key

LockBit 3.0 Builder Unleashed Custom Ransomware on the Rise

LeakyCLI Vulnerability in Cloud Tools Puts Credentials at Risk

Cisco IMC Flaw Enables Attackers to Escalate Privileges to Root

FatalRAT's Calculated Cryptocurrency Carnage

OpenMetadata Flaws Exploited for Cryptojacking on Kubernetes

FIN7 Takes Aim at the U.S. Auto Industry

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
DarkBeatC2	MD5	3dd1f91f89dc70e90f7bc001ed50c9e7, Bede9522ff7d2bf7daff04392659b8a8, 32bfe46efceae5813b75b40852fde3c2, b7d15723d7ef47497c6efb270065ed84
	IPv4	45.66.249[.]226, 137.74.131[.]19, 164.132.237[.]68, 95.164.61[.]64, 95.164.46[.]54, 91.225.218[.]210, 95.164.38[.]68, 45.140.147[.]81, 80.71.157[.]130, 103.35.190[.]203, 95.164.46[.]253
UPSTYLE	SHA256	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
	MD5	0c1554888ce9ed0da1583dbdf7b31651
	SHA1	988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9

Attack Name	TYPE	VALUE
LockBit 3.0	SHA256	07926e060b7083bbe639b36e9c79cce23404ba9dcaa58c190ee40d7d415ff96f, 707bb3b958fbf4728d8a39b043e8df083e0fce1178dac60c0d984604ec23c881, 5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226, c9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794, 72a18c1e65869e5fce28667ce2b9069f9c180f4af3437193a12566fa1aa9d1a1, f7d05c0e9430ba0621020caad12fa1e8e62acb3bda349cd03240c1938ce7a887, 4dfa2dcbcfe39550255fcf5daaa4ee3b74e7ea3a32666c91c100fb6b8508544b, b2c3beda4b000a3d9af0a457d6d942ec81696f3ed485f7cf723b18008a5f3d10, e81d18241b9af3d08b7a8e98148d690489eaf8891ec7b00e932d9efccbc41860, 2d2a9923c2676d5950473cb9ecb0d4c0db55035ca7540ef5717d8cae2733ac5e, be05716fd6f750c771974985de80d71892e1842c8a760038888ff5008cb6f3e0, 988f9936c4990bc9769bade8353ce321983afb83026295a6b70537e5f1151040, 54e75fae8ee8ffbbee075c7694a7fbb1ed838030d36e9e9c4e454010229e230d, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24
AgentTesla	SHA256	C54A3C60BC528E8594C813C61A2F929666E0F22A3CA837612B9CD48442721853, 97A6F1686F456A126C4FD823B01DF49814C71DBF4E2F3458CE9C62F89DE17719, D86EAA75FDBC0D2DE5B239974B02038200247B981ECC99074E86B5AD51A5906A, 02A2A2779ECD2CD887B97930A56FA5C8977A0D8FEC04D06BF3FB65ACB418FE9F, CA528EB30885238A7E594075C68AFE244602E2438DA103C98DDD81CBDEAFFA2E, 091982DE7843B6D35B392A9526B3ABF94B6A89A0455FA3F1FF1A18AB823C307D, CBA91CA10CE9EC62E5785A3F2004655540054A281CB76A4FCE46B56441B2A119, 1B01030333E0A08D7D9E66C2D57C34DEB54704E8769C52149D543100A5BF86B8,

Attack Name	TYPE	VALUE
AgentTesla	SHA256	2091183DB00054D0DC8504468CDF15C10F9A4172DD36AFA1D18123E59155DCDC, CD4F4252279410BC08AB3F37CB032A87C0C98077C4FC9981266A9964C37274A9, 34DD266B2EC7F77DAE04BDCD14E82B0CF977E0C6CC689A1C8A49737BB18A86BE, 8694E70E25489684DD115CACC569DCEC2D1AACF86D97C395B7475DB75F7C711F, D85278C4099B913C69779C4B69A0C85CBB0D7CBE72AE9A324B798A0FD2E02FB7, F36D42A5E7745D82D8ABC396CF0B91784B3C0ED6B82CFCAC3B77D1D8F61BCF2B, C1BF99CC27B4632A1916CA5AF4D8946A38E1D29CA0CF5AF7EAB237C5DAC930FB, 308BBA46BFCB12039B06105BEF71AFCCD82ACB7DF7658A8A4497C1955C67EE5D, 8AD61CAE616332A206292501D56A552330901422E52FC09EB6FD7D85820C3E15, 9E2F5BAD6ACB0454F71026526CB9D5D78985EF6E566B433B04BA7ABA5B277DDB, A830EABA9888A6FA0A3CBF85DA3636F1C41AE7A0372CBC5CFAB0EFD197894FC9, F74C6A3DEF1CED2A6E4BC81FEC1B4F062EBA67CE271CA4A47271631986A6D1C3
Formbook	SHA256	50413921860A4F9DB3C3AB95C68154E9FFD12726C64A4A46D141499FCF448288, C4333322E47F6528C43A77936DEA4BCF9230A3EC68C527D931D3C1C8F6232BAF, 2EA01DEF771F0E57B541D4819DD9A543C5ADB3A4452C6F5C03EAC2C49C542BFA, 7C614154B6EC07D9D05E17100DA1B4223A07A5BE73F8002D0290B722B4C379C9, AA48EAF5253F8378F5E6DB8325D90E229E3D836080083C6269DE0969AF2854BA, 4E538F7F6D63185FC67C4DF0B3697709F3D420821C2E7B423FBE62C684C7F9AF, 26EE13CEB4C1B409A14DE72D0CF8E1F3B0CB4D92A416B8618CFF800DF7762FB1, C892E597C34DB8FD7F3B96CD87A613F34AC3CDC710BF8F82A86E7D98AEB90C25, 27B3F0E015EDCC476C4A71A0AEEDFB5E1FC711E56CA0027C4AA2B13D4078036C, 0948B592B85131C65EE3FA422E8E05BB2AF509B5BE7F59FA88AC6D0E5AD0743C,

Attack Name	TYPE	VALUE
Formbook	SHA256	609E38239C20A1B1A2A1D773E18E467FB8097DCB2F398580C8780FC27D1DF443, 0A8CE026714E03E72C619307BD598ADD5F9B639CFD91437CB8D9C847BF9F6894, 37AE91A0976D913BC1A194207829DC5460AFD7B12D4EE22A69129772D151F156, 8AEE0E7501795514AB18F454EB754FBA95090A590A7F1128EB1EA52DBABAB134, D79A768E106B5C09D20E48704AEB15F5ACCEA32C5E05D1693FF26F0D3A45374D, D4D5A21A5EA9100F99E0D037AF48B705F809C571D6F444C94715D0204EA7A8EF, 2423D7CB2BE18902BCDB5C9C5AE88B32F9F4D97C920A429AAF4AE1FF70D70B01, B780B2FB9E38BCC285F93125E548C0E7B896FB20A26400F20293C3C6634EBE2D, 3FED057E15C7C7AD6539672E9DAD14FC272B22C7DC21AB6BA73544A50EB2E5D6, 571114066B38641901A6A70CF10FC8C0D64167B09C220C19ACAD7D15505455C0
Ramcos	SHA256	6FF46BDE6F6AB139C685F220E33230D1C064A6E62F68047F3E97BC8F04727E1E, 2E5B8A1ED53E25C5DDD9B7CD97B86627BAF197A7E3893909BCF33360BEDA2F71, D72B9F4910CBE10F8D1B3EEB7096F26412FCE2B735C9929C354D8F20265ABA50, 593CF342A669FCB1BFF594BD8CE85FC112BC19D42F7FCB0932C9AC5CDF70D0D9, D0947156CDD5831F8F4CEDE0B54E7A0B0D43EEAFC4F85532032A406F65736A69, 9E6406269FE3E1F7A309E3EE01E4770D6F5C7ABD2DEAD9AFC7EDDFEDCDB04295, 16ED067E08AF1F57D826FC97D438A03DD9E69FBD191F64B241654635ACAE3277, 4143A027AF3C078D252C462F6101CC1B4B849402280371D9279E6FA62EE6CF75, 91741818480B13EAAC1D5547B488142FE2DF86B8EB51B62B31ACBFD5FEF53F47, 1035DBC121B350176C06F72311379B230AAF791B01C7091B45E4C902E9ABA3F4, B2D5E15268CB130C995118E17AFA1198CA19604A20B91F1907A7EF18210DB30F, 1EC10BE5E16B3BF64560B88F44D02A4BD759E6F7D19F1BDFC6AA8AD2015371AB,

Attack Name	TYPE	VALUE
Ramcos	SHA256	B201D9C6A3A0C85ACBF87DF1BDC9D1377F389867E7807B7CECE516B9AD6EFA7B, 9137A41DDF1827FBC839DD16CF40CEEC512BEC3465CBA4A691D0FC543686A03A, BAD6DC695EC91155FBF548D43E3039C1B694DB28C1A713B81ECC2D59674635CB, BDAEB27128A9D6DBCD93B0844D57E6DE8A03EC3B53B1380F41523EC35AD6AF18, 4F138CD5C06D63316037E0622FA6C9E91A6798C78A457307772796C332DC4B98C, 45E734BC929BDEFEAA6F09BA766B8EF86CA2AF2B8534CA756420E6C5A39413F3, 7BCDC2E607ABC65EF93AFD009C3048970D9E8D1C2A18FC571562396B13EBB301
LokiBot	SHA256	40B9D6C7BD8BBDC15EF53C7067C6282A37B1AFE5796F721ADEB42E2E606521FF, 6255A5B13CA4D4C4CA7A43EADA557F7F248B124690BA49E11535E1C6496EFFD8, 861AC33701D696AA03435C2A6A6985C76EE1A38AB86CAD1C21CDBD15237A35DD, 5DB6A8DFAFD6956BEAF4127500CD5232D78D70165A1775FA1DA58277A43327ED, A5748DCF451F0661BDB05C9075327BD7EA6CB654B05140F4F2DD0B169AC26BC8, 3DDAE440455EE0723B4035FD75927DB44A82F22056C2657FADC125BFF94172BA, C16A14B36E6F0FDD1D74867149808CEBBDA3D2BC713359C98A781BA856FA8246, A725AC3C18D2E27DC053DFCA8284030D4280DEBFE9EA66523CC7AEAC491A4C48, A4B40080FE1EE2FA7A916BE8D7738DAB8F934F1D0367AF6462FA1F0DDD1BAB40, 130B3179FAF1683E10847BCF542AF95829A6509C99B409FEC11B5B040C345094, 237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D, 63F63156E794305B1847F85AEA00C20690BBFE942A27ACF718F5DA3B51EFCA37, 5929347CDE36BD71909DFC96BF2278A424054A21466C3DA91B58467B2D7D6D91, 677094197476508F5E6D59632ACE2106FC0A07435850F1541FF69BE9E939C7BF, A66799C33360147031E8A33775C723CC426256FA2BEC9773B8802FFB33D32AA5,

Attack Name	TYPE	VALUE
LokiBot	SHA256	5E0A6BF1CB4D379D238D51CDAB8BD64B47C10C2921F3F2CB1F6DA2B33C8AC332, 93A26C45838C0147B6227526EF8ABAD9CFABB115300E703C0C169CA7D3A7D77E, B744BAE65129D2D9980029A4D55B4552C79A28A5AFA89B48E0A383B96078231A, 630821BFAE07B41945A9EBF48D20EABDB4AD0E7B74CC58606E45597287A48738, A1CDE47A700A9372C2DE3C0566C895812DC3D9B7DD77E14C282C2E00611B436C
Guloader	SHA256	2582A3D44619CF80599337232301B2A1C06B706B397CB45718F15A0311871578, A50C71D12A6C7DEA4F7B1494A592FF459A42EA2511F82328ACB04DEB65E0861B, C637A1D9397AED930B59ED64B88233432B601BF7F2A2934AD2DE0A243DB30983, C3F62B8F93B8EA82168EB60074369A55855D637798D246182A3FE0E40F70DCC7, 6EEEB05646DC1C6DB8F8FB818A3148548100334EC73108506E5434E5F18B8888, C21E99F913EF55751C39FF7A605335CC0C3598D70CAEE0D40193C70A8DA2B9DB, 89ED1483ADE890ADA1D088CA1C76A378ED83043FE2DFC877B69788A5857B375C, EA7EED758FFF9ABB8044BFFA0BF0A0FE8865A10EA1124D245A9F1B39725429AC, 8596299CDDDE8AA075B0CE5CCA5AF805BBBD1CFA1FC6D54319060369FFAB275D, 2C92015C742474E9A12B6AF28085F85A0DD10F76E4882F8B51693253291A8B23, 7B53347CFFA39B9146236CBCDCBF2C40BE98CA5CB360BBE07E1F10B20E391B49, 3C6D1AEAC47CA58D37C43AF7C826E5D5727B33F0171D15708A3B9D602D2B5A10, 920E040D64758438D2BA1514B29A497C8D7C0822D19C8B9F9DF24D1A03583983, 676146162491E834C2F073B6B5499416C93141AE4D6B817D0F2D5E41EBBB581F, 75DCA4592067755F34E2ECA369ECA24BFBDE194A2F870FB79CD26B42046AAD98, F8A1D6FC26EE5CFEC7E2BB4FA4AAC2A4F4FA57DDF10589D60202E89A592223F0, 504A1971A4AD0A3006F67DF485B92EF5F0BEF5510ADF777E24DE9437C28CAB48,

Attack Name	TYPE	VALUE
Guloader	SHA256	C8E32720B969178C753329B176A0CC34AF8ED2317DCE003CFE52E55D3E07E81E, 4365FF3C93EE1FAA413AB7CF6838884C449053479D3039E995A6CDFE590125E4, 26D95099636E212FCCB35C4865A6AAEE393079698B6C3A6F0A07EF2960A845B0
SnakeKeylogger	SHA256	3B50796D11C0837412A2D9205F28604EF9C02EA436E33F9CB46AC3B99E1BBC37, 061EE3375DC3333D8C4266E773535E516206935D4F7DBBC3F0319D253840213D, F8C1925693A82D8A544BEDCF975160A6CBD8A0D0E2A463E402402D8D28AD6E8D, 1624A0E8F86CF5331CCF66FD830A96827FC0B3DD842ABB268996D2387F2ED4BE, 07A1258C5EF18D86C00F843408AA21667C7817B8E7D1EAD1A5411856D0D21ED7, 36E9496A87CA35BF4D8D4D8E800BC82371D6DB67B8B19ED0C0C37FBC66EF8A5B, B932E7EC61F1CC9B3C858A55EB883ACCF378580572077C2676ADCF2A0AA8DDE1, E417867AC84D86D4B244788731D9C840FF0537640665083D293D077633F0628E, 53F9DACF7CCBE8AF215F3CB912F7C2ABB468505D5C1430137C82C4B60997C424, 2D00AFFF6535A1FAFD100B518B45019EC4645AFB3C105670F71CEB6CDF552814, 4ADA7E83E7FFA97F90588475D5C9356A9F1003E1CC7721D227CA0609EF23E9DC, D156D6626E85584270B990B2B53C325A53BE473E21C6FD32E1AC4E50301EE165, 7DB30520CDE8D37F8875299B1182C0E56A0A47D995117C1BE330D08B4DE86666, 2F320096233E8420996FF654C26C078472BBE2BC115FD5D4D6139E0819A58457, 225C1D3377CFF7773455E55202057E9E95C537C33016D26BB832333797277E49, F315D7D883A82CE0B007F7F2B899047B781FA2CB5B05952E146AB679C8C64717, 9A327BC3EF2E083620C9AE2E7A6363E720D8ABB5A4FC3C4EAFA91A34D1C5E2F4, 82452545022D3ACA5B5453B044F6E1A5C0837DBF340E42B1E75C047B555F9BC4,

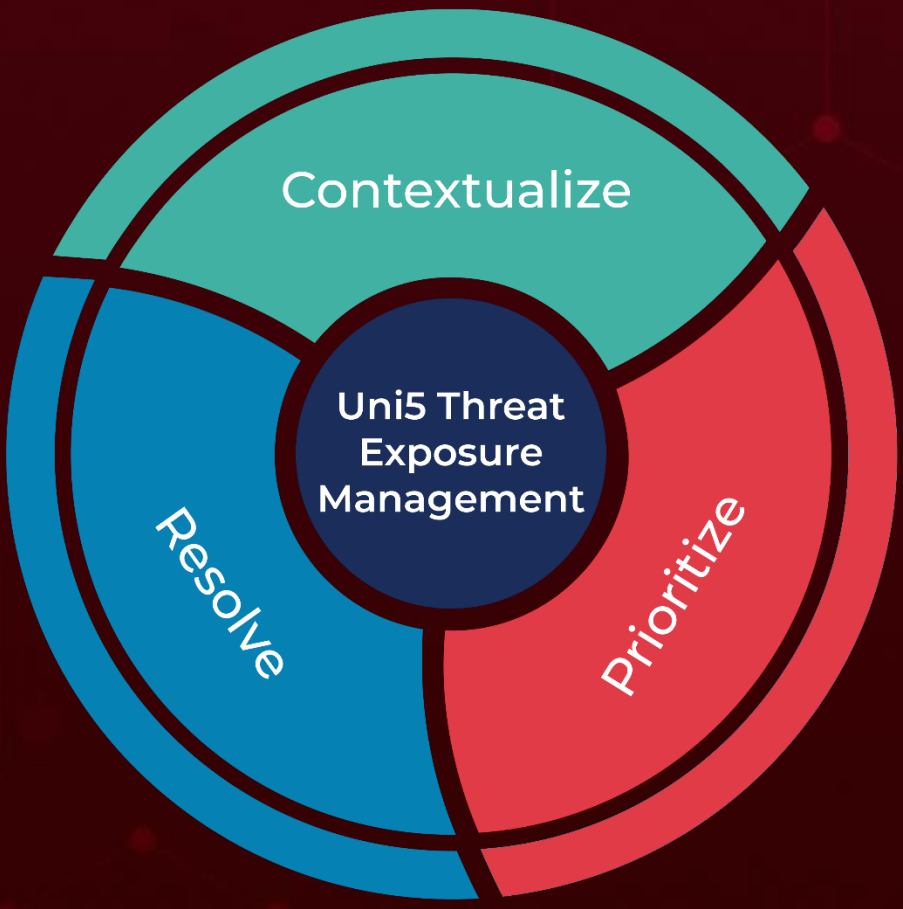
Attack Name	TYPE	VALUE
SnakeKeylogger	SHA256	EBD92BDD8BEAFB2436B1B084EBFA7686BD53F73E305AA368D9EAA53A7C96C78F, 3D499CCCCF5F8EC92BE049BB72964B0762B5DA99FF7E0280F77284DF6E042B4E
Xworm	SHA256	C0BD1EBDF30196EFE9F0F562DCCCC143ECE619994CA14170E88F87AD402CDFFA, CD9CA4735E5100ABF0163B9E2E7F63B35CD3DC0BA791E0540E15C94A13470289, F9D7569C8A07239001E8EB6E8915D922821F53A37328C67F390D64B8D594623D, E1DE5491FBADA68CDBFF98F68ED645BF8FDF62F21CF792FCA7CC556EF2D30A9F, AC009DA131ECC35C95B484248FCD3091F607D71F26F7421699B2A8C907B1EE04, B6F7B52A5A37CDC6A4EF74557EA182E006CDDBFD81CAA55FF0154F032C643B16, FB6030901766855BD7C744C8B3718248014F53C72562191FE6BAC6468D48B476, 096E33B9B0B4F843A7EA0259F75B4370F00AB90F3807EB89D5F0117DA762900D, C39365657B596C0E0D5599D177EC383659D23D24D1E529FCF2EEEF2C8F82E5F0, B6D964C8820A2827075248FB5F78E6D108E86CED610F854B7BF79BA0511B0E6D, D2AE6FC3637DAE75AA818C5EAAE687AF4989CD9B2312D6375A182AC1E3DE8FD5, 820BB1A31F421B90EA51EFC3E71CC720C8C2784FB1E882E732E8FAFB8631A389, F79EA17E2928C9D73D8733366AB1DFFA64F3B26275219EACA2E83C2F76C96161, 87B77954F60BEA9EEBAC32548459D1024998C92B6606E6CE9CBAB0FACC746751, EEF14366A8910998A21B02BBC3180C87A110D6900897E918EE5810A0DBA6FDF0, B079DD50E4CD9788F984A1F1018984D71D03990C44FBE3089EBE0A595DA4E98A, D22FAFFE39DE72108CB34407C0F6555069AE9E5D7D0C26F839370558F44BCA9A, 70BA57FB0BF2F34B86426D21559F5F6D05C1268193904DE8E959D7B06CE964CE, C9A766B2570F5F059A4A1222AF829AA099CB7E5E47F3CC6A6DFDA9A80611E3A0, CD829068822B91CC8BA0CB929CC82FC8CA94897A87C73A154D4469983CCB7643

Attack Name	TYPE	VALUE
JsOutProx	MD5	118b6673bd06c8eb082296a7b35f8fa5, 1bd7ce64f1a7cf7dc94b912ceb9533d0, 3a2104953478d1e60927aa6def17e8e7, 3d46a462f262818cada6899634354138, 66514548cdffab50d1ea75772a08df3d, 6764dbc4df70e559b2a59e913d940d4b, 72461c94bd27e5b001265bbccc931534, 81b9e7deb17e3371d417ad94776b2a26, 89a088cd92b7ed59fd3bcc7786075130, 9c9df8fbcef8acd1a5265be5fd8fdce9, bea8cf1f983120b68204f2fa9448526e, d22f76e60a786f0c92fa20af1a1619b2, efad51e48d585b639d974fcf39f7ee07, f1858438a353d38e3e19109bf0a5e1be
FatalRAT	SHA256	8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d
Carbanak	SHA256	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
	MD5	87aa5f3f514af2b9ef28db9f092f3249

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

April 23, 2024 • 12:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com