Date of Publication
September 11, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

4 to 10 SEPTEMBER 2023

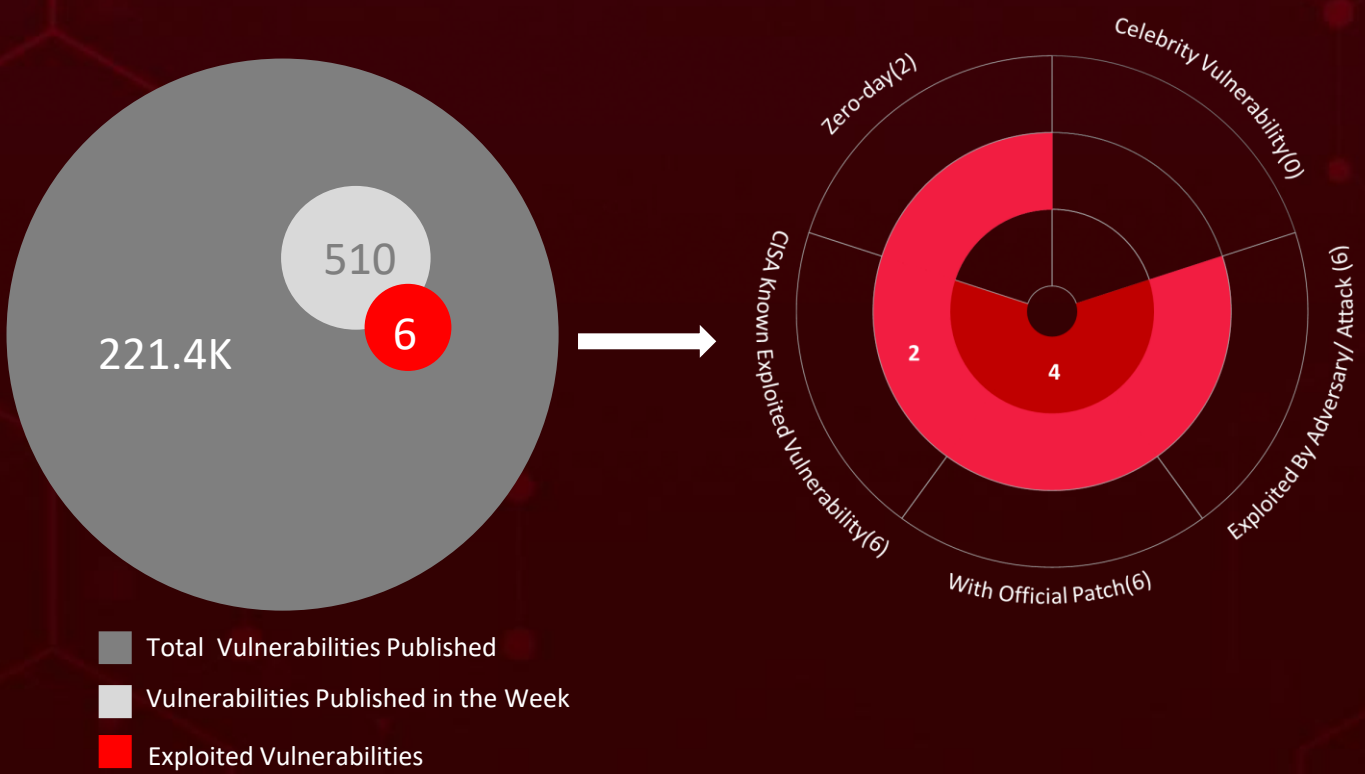
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **ten** executed attacks, **one** instance of adversary activity, and **six** vulnerabilities including two zero-day vulnerabilities highlighting the ever-present danger of cyber attacks.

Furthermore, HiveForce Labs uncovered a modular Linux-based botnet '**DreamBus**' exploiting a critical remote code execution vulnerability in RocketMQ servers, tracked as **CVE-2023-33246**, to infect devices.

Meanwhile, **Smishing Triad**, a China-based threat actor, has been conducting a large-scale smishing campaign targeting US citizens and other countries, impersonating various postal and delivery services, such as USPS, Royal Mail, PostNord, and others, to steal payment data and other sensitive information. These observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

10
Attacks Executed

6
Vulnerabilities Exploited

1
Adversaries in Action

- IDAT Loader
- StealC
- Lumma
- Amadey
- SuperBear RAT
- FreeWorld Ransomware
- Chae$ 4
- DreamBus
- DuckTail
- Agent Tesla

- CVE-2023-28432
- CVE-2023-33246
- CVE-2018-0802
- CVE-2017-11882
- CVE-2022-47966
- CVE-2022-42475

- Smishing Triad

Insights

Chae$ 4

is new variant of Chaes Malware targeting Financial and Logistics sectors

FreeWorld

is a new ransomware that targets Microsoft SQL servers using brute-force attacks

DreamBus

Botnet exploiting critical vulnerability (CVE-2023-33246) in Apache RocketMQ

Agent Tesla New variant

spreads through crafted Excel files, exploiting Office vulnerabilities CVE-2017-11882 and CVE-2018-0802

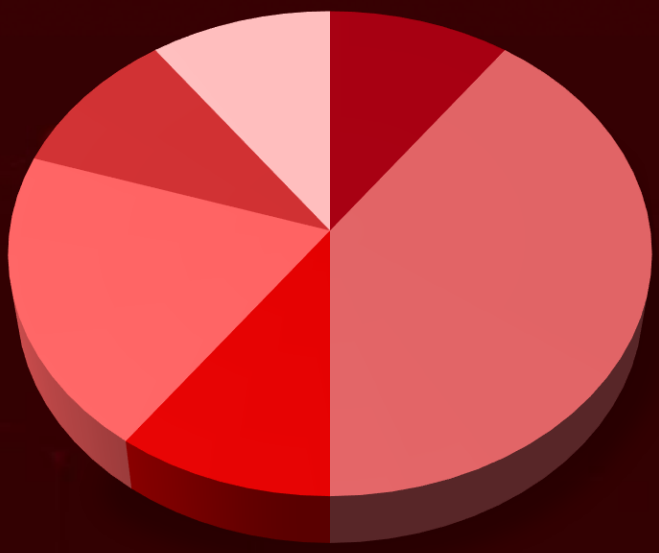
Smishing Triad

China-based actor conducting a large-scale smishing campaign targeting US citizens and other countries

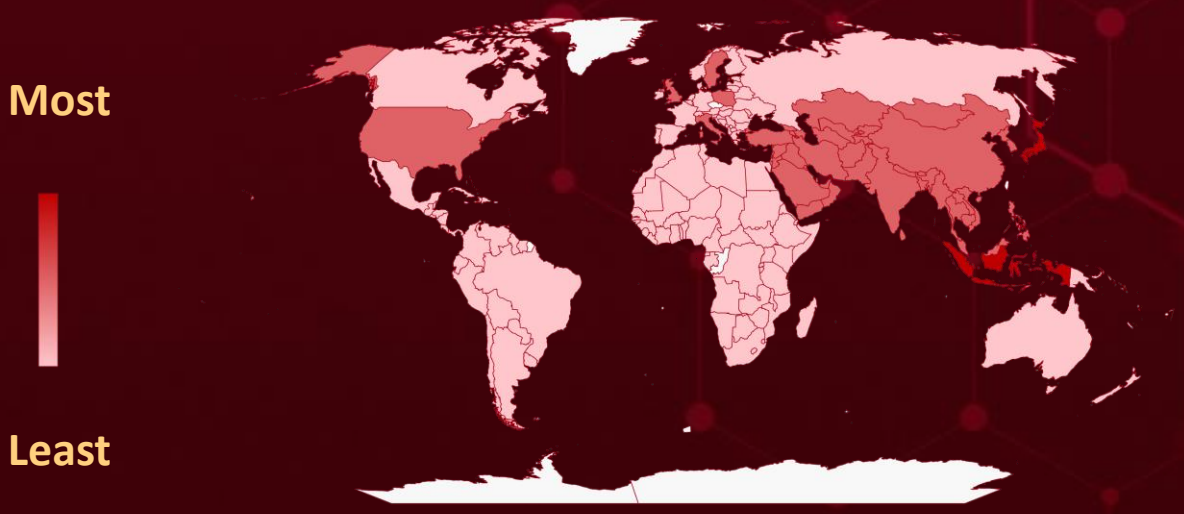
DuckTail

Malware targets digital marketers with malicious operations and is designed to steal saved session cookies from web browsers.

Threat Distribution



Targeted Countries



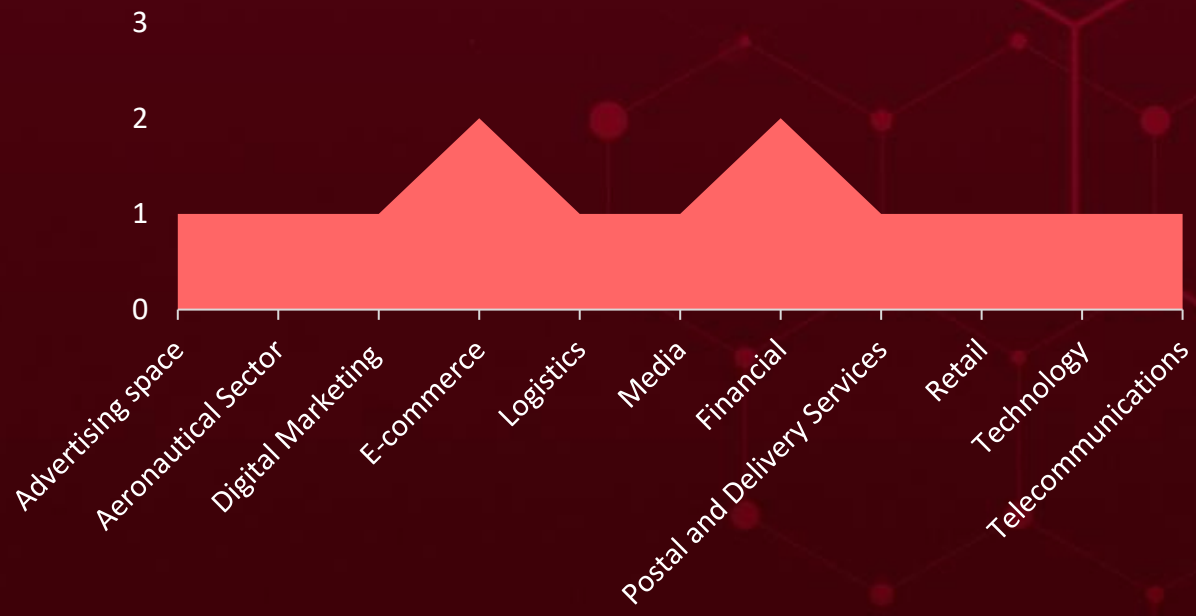
Countries
Indonesia
Japan
Pakistan
United States
Syria
Bahrain
Myanmar
Bangladesh
South Korea
Bhutan
Turkey
Brunei
Maldives
Cambodia
North Korea
China
Poland
Cyprus
State of Palestine
Georgia
Thailand
India

Countries
United Arab Emirates
Armenia
Malaysia
Iran
Mongolia
Iraq
Nepal
Israel
Oman
Italy
Philippines
Qatar
Azerbaijan
Saudi Arabia
Singapore
Jordan
Sri Lanka
Kazakhstan
Sweden
Kuwait
Tajikistan
Kyrgyzstan
Timor-Leste
Laos

Countries
Turkmenistan
Lebanon
United Kingdom
Vietnam
Uzbekistan
Afghanistan
Yemen
Dominican Republic
Sao Tome & Principe
Palau
Eritrea
St. Vincent & Grenadines
Estonia
Nicaragua
Eswatini
Colombia
Ethiopia
Slovenia
Fiji
Tanzania
Finland
El Salvador

Countries
France
North Macedonia
Gabon
Peru
Gambia
Saint Kitts & Nevis
Algeria
Seychelles
Germany
Costa Rica
Ghana
Cuba
Greece
Tonga
Grenada
DR Congo
Guatemala
Netherlands
Guinea
Nigeria
Guinea-Bissau
Central African Republic
Guyana
Burundi

Targeted Industries



TOP MITRE ATT&CK TTPS

T1203
Exploitation for Client Execution

T1110
Brute Force

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1574.002
DLL Side-Loading

T1005
Data from Local System

T1083
File and Directory Discovery

T1573
Encrypted Channel

T1053
Scheduled Task/Job

T1059.001
PowerShell

T1497
Virtualization/ Sandbox Evasion

T1140
Deobfuscate/ Decode Files or Information

T1588.005
Exploits

T1486
Data Encrypted for Impact

T1057
Process Discovery

T1566
Phishing

T1105
Ingress Tool Transfer

T1588
Obtain Capabilities

T1070.004
File Deletion

T1012
Query Registry

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
IDAT loader	The IDAT loader is a new, sophisticated malware loader that was first seen in July 2023. It is designed to deliver other malware, such as infostealers and RATs (Remote Access Trojans). The IDAT loader uses a variety of evasion techniques to avoid detection by security software, including process doppelgänging, DLL search order hijacking, and Heaven's Gate.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StealC	StealC is a new information stealer that is designed to steal sensitive information from compromised systems. It is a Windows-based malware that is uses a variety of evasion techniques to avoid detection by security software, such as code obfuscation, anti-debugging, and anti-virtualization.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	c1399000e984bfca6a9bff0f51ea5fc4342c5504080a41c68749034b87d6e6c3, 56b20f8eebb0f9ecdd8be61665112fd3ff75d97c037e45bbe1ce74b9d382882f, 521b495bda0f7be6271f3a21014ca95a59aa8e4ea630dc5b07cb352429c4d4e7, d2661804f3e73ebaf2bc7b9c0dc7ece259464b2e6f89d4212804602572b44fa2, e30d0c23bba711c7fa9e7e192cc6682cf86806d34cf4a24a1ba0985336e4ec23		

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
Lumma Stealer	Lumma Stealer is a malware that steals sensitive information from infected devices. It is distributed through a Malware-as-a-Service (MaaS) model on Russian-speaking forums. The malware is written in C language and is constantly being updated with new features.	Malware-as-a-Service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1deecd4e2aeae42cba		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Amadey Bot	Amadey Bot is a modular Trojan malware that steals sensitive information and can download other malware. It can be customized to perform a variety of tasks.	Phishing emails, exploit kits, and drive-by downloads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d		
URLs	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]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
SuperBear	SuperBear is a remote access trojan (RAT) that was first discovered in 2022. It is a sophisticated piece of malware that is designed to steal sensitive information from compromised systems. SuperBear is primarily targeted at journalists and other individuals who cover sensitive topics.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Steal and compromised systems	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FreeWorld	FreeWorld is a new ransomware that targets Microsoft SQL servers using brute-force attacks. It encrypts files with a .freeworldencryption extension and demands a ransom for decryption. It is a variant of the Mimic ransomware and uses Cobalt Strike to establish persistence on the compromised servers.	Brute Force	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Encrypt	MS SQL servers
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	75975B0C890F804DAB19F68D7072F8C04C5FE5162D2A4199448FC0E1AD03690B		

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
Chae$ 4	A new Chaes malware variant, "Chae$ 4," targeting logistics, finance, and prominent platforms has emerged with enhanced capabilities, including Python-based architecture and an expanded range of targeted services and data theft functions.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a, 628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57, 6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c		
Ipv4	18.228.15[.]16 18.229.122[.]137		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DreamBus	DreamBus is a modular Linux-based botnet that has been around since early 201912. The malware can spread internally by scanning private subnet ranges for vulnerable systems, using common and default passwords via brute force or application-specific exploits.	Exploiting vulnerabilities	CVE-2023-33246
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Compromise system	Apache RocketMQ
ASSOCIATED ACTOR			**PATCH LINK**
-			https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp
IOC TYPE	**VALUE**		
SHA256	e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d, 9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f, 371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c, 21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417, 0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f		

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
DuckTail	DuckTail malware is a .NET Core-based information stealer that targets Facebook users and business accounts. It can extract browser cookies and use social media sessions to obtain sensitive information and place fraudulent advertisements for financial gain. It has been active since 2018 and has evolved with new malicious capabilities to bypass Facebook's security measures.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	740fd780b2b45c08d1abb45cddc6d1017c9fcc6bcce54fd8415d87a80d328ff6, d93c40de3e43ec58b115e5590c98ef62de15df9b706ef6d4a06d022fa874bb48, aaf44bce6a5a2ab5b7f3f75f8238d6abe46f9fd2f2e2a2b2672ba6e52f4d5754, 4f43c031ff415fcb2f6865e98e91eaf611eb6a576acfe3250b57dc5e47a7d34f, f433fc47b9ccd66aa80196e04a4e4bf54fe3d1c689e4b5d5bcdf86017c3f8abe		

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
Agent Tesla	New variants of Agent Tesla that have been detected in recent phishing campaigns that target various sectors and regions4512. These variants use crafted Excel documents or malicious links to download the malware onto the victim's device12. They also use AutoIT scripts to obfuscate and execute the malware payload2.	Phishing emails	CVE-2017-11882 CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Compromise data	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

IOC TYPE	VALUE
SHA256	fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904c22638, 36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda7702820efcfc3a
SHA1	e2437078fe7f3abd635dacae65cf6ae2d10ef98e
MD5	c1ac31ebcbfb8dc95d4eea6d4c95a474

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-2023-28432		MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:minio:minio:*:*:*:*:*:*:*:*	-
MinIO Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1082: System Information Discovery	https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33246		Apache RocketMQ: 4.2.0 - 5.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	DreamBus
Apache RocketMQ Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882		Microsoft Office: 2007 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*	Agent Tella
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1495: Firmware Corruption	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0802		Microsoft Office: 2007 – 2016; Microsoft Word: 2007 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*	Agent Tella
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1495: Firmware Corruption	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966	✗	Multiple products of Zoho ManageEngine	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	-
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42475	✗	FortiOS: 6.2.0 - 7.2.2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	-
Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://fortiguard.com/psirt/FG-IR-22-398

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Smishing Triad</td><td>China</td><td rowspan="3">Financial Services, Retail, E-commerce, Postal and Delivery Services, Technology, Telecommunications</td><td rowspan="3">United States, United Kingdom, Poland, Sweden, Italy, Indonesia, Japan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and Financial fraud</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0005:Defense Evasion, TA0006:Credential Access, TA0042:Resource Development, TA0040:Impact, TA0043:Reconnaissance, TA0001:Initial Access, TA0002:Execution, T1588:Obtain Capabilities, T1589.001:Credentials , T1589:Gather Victim Identity Information , T1598:Phishing for Information , T1036:Masquerading, T1078:Valid Accounts, T1586:Compromise Accounts,</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actor **Smishing Triad** and **IDAT Loader, StealC , Lumma, Amadey, SuperBear RAT, FreeWorld Ransomware, Chae$ 4, DreamBus, DuckTail, Agent Tesla** malware.

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Smishing Triad** and **IDAT Loader, StealC , Lumma, Amadey, SuperBear RAT, FreeWorld Ransomware, Chae$ 4, DreamBus, DuckTail, Agent Tesla** in Breach and Attack Simulation(BAS).

Threat Advisories

New IDAT Loader Unleashes Infostealers in Fake Browser Update Campaign

MinIO Vulnerabilities Exposed as Hackers Breach Through Storage

Unveiling The SuperBear RAT campaigns Targeting the Journalists

FreeWorld Ransomware Targets MSSQL Servers Facing Siege

New Variant of Chaes Malware 'Chae$ 4' Targeting Financial and Logistics Sectors

DreamBus Botnet Exploiting A Critical Vulnerability in Apache RocketMQ

DuckTail Targets the Digital Marketers with Malicious Operations

Agent Tesla's New Variant Spreads Through Crafted Excel Files

Chinese 'Smishing Triad' Group Targeting US Citizens

Critical Remote Code Execution Vulnerabilities Discovered in ASUS Routers

Nation-State Actors Infiltrate U.S. by Exploiting Zoho and Fortinet Flaws

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LummaC Stealer	MD5	507bddfabd74a3d024b2ad5f67d666ea
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock
Amadey Bot	MD5	952d825a264745bb52b6977ba5983568
	SHA1	627a0a841c2fe194dd54f9ec6b0c1231d7da135f
	SHA256	d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c,

Attack Name	TYPE	VALUE
Amadey Bot	SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d
	URLS	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe
SuperBear RAT	SHA256	282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb
FreeWorld	SHA256	75975B0C890F804DAB19F68D7072F8C04C5FE5162D2A4199448FC0E1AD03690B
Chae$ 4	SHA256	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395dd cf7d134a, 628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac 372a57, 6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e 244898c
	Domains	4.q111[.]sbs, <day_domain>[.]mail89[.]us[.]to, <day_domain>[.]ns99[.]uk[.]ms
	IPv4	18.228.15[.]16, 18.229.122[.]137, 13.248.205[.]89, 13.248.185[.]41
	URLs	hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com, hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com
	WebSocket URLs	ws://54.233.147[.]24, ws://18.231.31[.]151, ws://18.229.170[.]213, ws://54.94.248.[]242, ws://18.231.70[.]213, ws://18.231.91[.]245, ws://18.230.36[.]203, ws://54.232.236[.]117

Attack Name	TYPE	VALUE
DreamBus Bot	SHA256	1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047, 1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d, 601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443, 153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2, e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d, 9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f, 371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c, 21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417, 0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f
DuckTail	Domains	marketingagency[.]social, a1outreach[.]software, mangogroup[.]sale, la-roche-posay[.]click, li-ning[.]agency, li-ning[.]news, hrm[.]social, hrms[.]social, mccann[.]fyi, avalonorganics[.]work, li-ningagency[.]news, li-ningjod[.]news, ogilvy[.]social, narscosmetics[.]social, yodo1game[.]software, louisvuitton-social[.]news, luoisviitton[.]news, eucerin[.]work, guessinc[.]work, samsungagency[.]link, brandresource[.]social, recruiterofbrand[.]social, brandrecruitment[.]social, hrmmarketing[.]link, marketingmanager[.]social, recruitmentagency[.]social, marketing-project[.]social, nike-agency[.]link,

Attack Name	TYPE	VALUE
DuckTail	Domains	recuiter[.]company, louisvuitton-agency[.]link, louisvuitton-agencyjod[.]live, mccann[.]expert, ogilvysocial[.]company, louisvuitton-hr[.]news, louisvuitton-jod[.]chat, hyundaimotorjob[.]social, hyundaimotor[.]social, hyundaimotorgroup[.]social, adplexity[.]site, adplexitydesk[.]tech, fbadsguide[.]tech, affiliateguide[.]tech, newguide[.]tech, businessmanagerads[.]tech, businessmanager-update[.]info, marketing-tool[.]info, connectads[.]agency, disruptiveadvertising[.]agency, impressionagency[.]co, themars[.]social, ommmarketing[.]agency, growmemarketing[.]agency, ommmarketing[.]digital, impressiondigitals[.]agency, impressiondigital[.]info, passions[.]agency, brandstyle[.]agency, brandstyle[.]digital
	SHA1	92a7ac122ab87ccfd19224b2be89fd7bbee6d0b1, C8d5b988464e7e49b932a01d3b75e192fc7a0026, 27ac50a5f2751429eed99fd4abff73c2129ba387, 2e1b5903131ad42591021919ac27beecd70c9253, Ce5f839cb8a3473330256ed72c144f689ad3c55d, B14deb48c60771fb05cddf6a16ea9fc4e56ac6be, 1b07ce1f47ba6b19087499fa4ba2e93beac227c4
	SHA256	740fd780b2b45c08d1abb45cddc6d1017c9fcc6bcce54fd8415d87a80d328ff6, d93c40de3e43ec58b115e5590c98ef62de15df9b706ef6d4a06d022fa874bb48, aaf44bce6a5a2ab5b7f3f75f8238d6abe46f9fd2f2e2a2b2672ba6e52f4d5754,

Attack Name	TYPE	VALUE
DuckTail	SHA256	4f43c031ff415fcb2f6865e98e91eaf611eb6a576acfe3250b57dc5e47a7d34f, f433fc47b9ccd66aa80196e04a4e4bf54fe3d1c689e4b5d5bcdf86017c3f8abe, a5026e7a88c3b833ee3678944d003fdfe51f86d44515c470dd2c8aa62e0fd0d2, 4759cb5a37f2c8661c3817206b4d34d65825d80526ce41461f6c11ea56289ff3, 4c546c259cbbf0daf1d0aa00d3385a1ea9e74b6fb2e3692ef44e1da27ba30abc, 71a89855974dcd69f3547632368f2ce8cfa490ee96b514d832f04cc22923f143, a6decb34e5688f543e541dbc79e6884ace29c93d7fc43716eb32204cb3c0003e, 59caef212349c6423e1fc581aaf76ab735269990bb7dc8e193e2877957c71e91, 1000d705806b940af52b54cba98261b64ed658a355e0922d64551c5acb7f1a40, 47f9122f0a25f4909795ede9bb4458495ae70fa2657745ec7c47ee172e040209, 52e295073d2114c0683d95c8d323bddc95baa5c68f8362ebcc81124a06e42672, 6e797da70db98e1f8fb5a7cf794b8a8e90549e8915f4d04f510690ae23aeb505, 25b427a06608ebfc48c778829427a732c17986c64345acf35e92d03ccb126b8f, d3633c2372b67db37b11de741bfa676a425322c5208b8396c62983aed88d2bcc, 600a498e55512723074b6f5a952ffd38b249c30117e9eaafcccda4fd1a0c1e75, e74f131d1e5ed725383ee5b89ec1216c642fbd77928dafd991b406a7f59251b6, 469bcbd18e2b5d4ca15f449d43c13656758503fcc4042a05721ef5f3c35345e2, dec248f011c1f945f590bb5aeefbbcb41bdaa6c665625a594f8b315f014ea4bb, e8d5af5ebff12d0cbb8b1cd70f149a8234b993facc32b3808fc7db94f2bf80a9, 7952eb4832bfe5155e2f37abb68d552ed8f2f426715f2bc65eae5a69f1f28d87, 7c6b1a349ad96d8368e1f9742992f764a7de32e9c07870937210a88a721c532, 7eb994eaa7be9dcfb37bdfd7c8bec1dc8b90e3ec4aa86de6e6125c97eeb64426, af75e8c1f3229868d41b141165714c56baf38f3f49c8c014c4fa18bc934720bf,

Attack Name	TYPE	VALUE
DuckTail	SHA256	6688e027e837f8e86dbbe40e2e663e72a1b7e977ae25d1157ecd8793d947f0c7, 7d15d3cdc41cc0c3452a538ed3bf8e0dbc9a0cbd4bbca453a293287e240dfff8, b83059cc733ad4af37a15a24222b09be3ee02af3964bc62ae5de6354cd85f65b, 61953e2d6e80fca18173bd3ce695274c5a25db449ac32addd8ee5b0ac29efa02, f17d2acb4c1bd0332b3c0cdba83001b82fd96d62d5bf829ae1e409902195b038, 1092ab1743ca59c29bee69d73918ee78e2195fafa232a16ba790429d39dc9083, 1e6ff886f386afbbcf8dc175bd1fbdfd8079448f1cb5a546352d7065c5fa5e7b, a81cbb9871f692350bf21d07b9acc233268df233b79c311a482d9783eb9bd539, d7f4372daf2729c956ce63e0ba2b7149f1bae03da7fbae486bbcfb0bda0f8d70, 3f9300d5d84482010bce08e9cc7b0a5b605086dc4143e8470e9e23ef14f0c27f, e2a343dfa801882625c264f944f89665319ea9b3a2793ec47a02bb4a126f5e15, 8cf5a4d0b6848604c338ad2d8bde8ceab2e86fff0d65e777bc574025f26bad73, 994039645f60d5fc9621cb10826b7583c83667827c195b3fa9d875a8ee50b170, c9c5409e6327f2f443dfa3cb6ffa527b291a34a572c14e93b65205fd305f4ff1, 83126452e240cdebbfaabeda58dcb4ea68f1e9836596e6032119592b4057ca4e, 7395aa619010fee65ef640f46023be5732188df36079e13f023aa2dc69602e21, a09f560a1ddbc7c60695d5651cff0ae0f0911399cb5146bb531caccb4d14089e, 34392151e58955b0bd7eb70a90499127ec5810a8488c2ae5bd4da1f9167a7762, 9d24436f652abe1df6319fbfa0a5468f1061e280d41fb00a60265d6c2aa7871d, 8c87c2d7f3932fa6661daf8fbf058ab4b721d0d6fe0849da30ae695b61d3ddc2, f47a002d93df2190e47e7026663bea34ea0299a4afe2810b8cb45b51bf330a8b, 6578a3dfaa2c59443b02581c0097e8c356babcb388c4ab48ef651c90c262e9e7, 4a56e4a753a5fa615aec4f80eb842ea2f089bd439e93ecf406f8433e97b659e8, a8196b3995bfbc62ec073dd35377a5412db30e9070ab72743694cceaddd2495c,

Attack Name	TYPE	VALUE
DuckTail	SHA256	958ff188086e33caf119347ef7d81a99716e83bc688ed1ada1ad25feab7088b9, 697307235b627a33f4308a14dda9c1f33e38c9efb572026320bca453f6301b0a, b0968ac6489e7f2122ef2deafbc5a5f5968451918a8023c7aa8ded7171264ba4, 625b5b3f5bc9e1fce5486812051b187975210a46bc2d9a712e9ef9ae5c68f09c, d6c18d9efcbb6ce7292c4d6bdba70a64acca10561b66fd88e9e47cb9c7b63392, 4089277eff9f088684f53697c2f5615dcf4c940c1693d9d8c85a7de47dce7161, ce1f6a00bf9f79ffe879c2e7ef40166ecacbe6a17a382544648f0f25c5c4177b, 2c9824d0faff9a0485c36546ac7884697d1773bd221c2586ae9ddb0e54208731, a99fa349faabd5773816c53a11b67a7be95f277b622ebe93c1ca3625500b8384, 1fcbf708854f7ebf93726d5dd08c08648e84aee0a33a618a29c7e50df09e12d5, cd8b9cc35064b76df01ba5ce7536fd8b60dc773e32889ceca95f586112b6f3c5, 044eba497f9259d18a3ea593de3fc39c6123805ce485cf4a193083f9e0b74bb7, e81db61004834afb0dbf47db128942e3353774764466fb9269e88a553e6dfc33, ee5dcf9b070e19b87842e5c9ce3548bb1507e41d7aad272ae697afcd9f3ab7c2, 7af6cbfd7d1e7fe2f8c8c0382ee43860ec2cbe25ca845588981263ff8144f236, a30548fa4058d1309d4d75dd2dc36a492c503168f4d1c2f6c52cce57069629cc, fc8c250c2346e5440e249942eb8fe7c8b9b7d8d013f275c5fae2ae142ac50171, 8db1a51d514811057d29ddda85858f52303999cebdeae25f88d05a39594afd3a, f7c015d65d4966936927ae5241ead77c9d167d749e97667a571d7439e652ffa3, a3c5cd4f1afbe10de154bf3f669479496ff2e93da660a849ff41c29d5f118a4a, 9ef977e0403f9dff5cebe3935402d7a776ca3c9a79618e4d6992d3754051f603, d6c7c6a9098769b015802a278eb81bc7b72b08c5e18534ac71f01394a95c1f28, 647793166e03397bb1c30f0935330bcabc9f2f0f4ba8d7a821fc145237d96b2f,

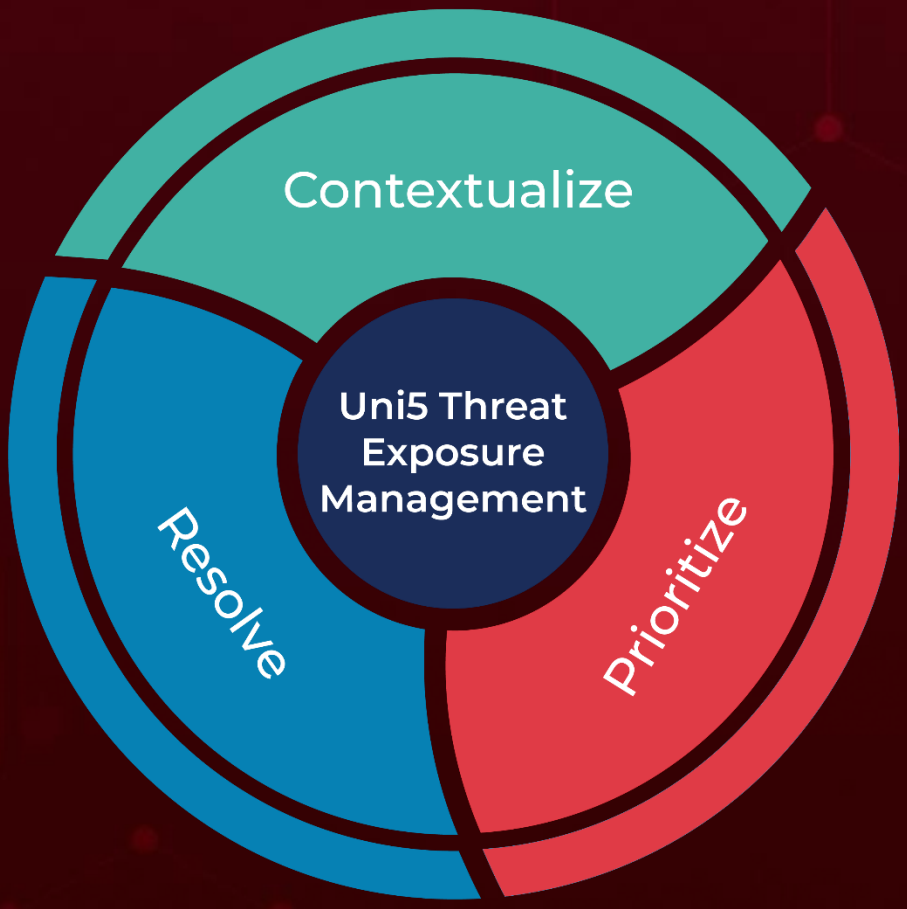
Attack Name	TYPE	VALUE
DuckTail	SHA256	300358895c7895c14949c80d7b4ef6fa50ec5027e65e4578d503c39f2bd6618e, e4bf8cfc1035f51020ff033b9366dd1fefef8ae5664e2fde6798831399c51d1d, c1e65ebb05c500b5ade389a2f880e9116b74b24782d9ea13955adab087194b43, 4874878056cebe9627bbf44a3bc977315d6e14492af855319103b99103241c5f, d26b0baa30cc13df88eca57ce22f651a744cf5683b8b62121b4292e1005527f7, d5939fc12c88264cb28ac867767e5492aa145f0499aeaaa83cdaca8b15da07ee, 507376fa684f17508a195426d933e0e2ef92028d5956ed66cba825b6ce61df8e, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df, a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, 51abe6d7196e93c4264ff508a11611b871bb1c9d96df2086efe84dd48af96cc2, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 07d5d4721c3ed9a860dc10d25f226dd81a83602023c63310f9634b8dd704e7f8, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c,

Attack Name	TYPE	VALUE
DuckTail	SHA256	161d081e9ba94ee1749c3192888702f6a25e8e2fb59b9d1f9d989ffc885566a6, 80160fd48ba4d174ccd1d2d8e72afc3674c1ce7c73ef18d3e372a6d68e6b3227, a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, 8731ec7667084e649622e9f553e291b889eb0709c669545bd19f3ec0c2878687, de0a568803eb5b3d51eac593d2c9174e6fdef9a9ee11f222e5822ae3f182b5b0, a979cf0a2a44f2c23e01eb72cb72cbfadbae40bea38a3d390977d79bad610bc8, 40da0bc61a4ccf170f43981a7d908b0c3b541b1652cbb959b1ea9a87dd5944a7, d76260578caf24dbb6dd2d10c60b066d7659f5c21da8c998f34ab0f675d626d2, 5d9b287df9b9b3f019e8d5834f117200f0651ecd0988338fb395ef1382fabc26, cd5c66a206e92be1e7eb77d5cb69c63fc2acc9ffbfcf7031713c9fddca11b3e7, f4e9feb547dcd6a233f71c7ad57a0759a584ae94a9e822a64831ed26cb32ecf4, 0241555cc3e21a658c78cbe93ab75eaa4f978a013df22852ada57652a3a57b6a, cc5483d21c84ac73c410194205b529d6190b322b8da49577ee36ae9d8878c0c3
Agent Telsa	MD5	c1ac31ebcbfb8dc95d4eea6d4c95a474
	SHA1	e2437078fe7f3abd635dacae65cf6ae2d10ef98e
	SHA256	fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904 c22638, 36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda770282 0efcfc3a
	URL	hxxp://23[.]95.128.195/3355/chromium[.]exe
	File Name	Order 45232429.xls, dasHost.exe

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

September 11, 2023 . 8:20 AM

More at www.hivepro.com