Date of Publication
September 4, 2023

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

28 AUGUST to 3 SEPTEMBER 2023

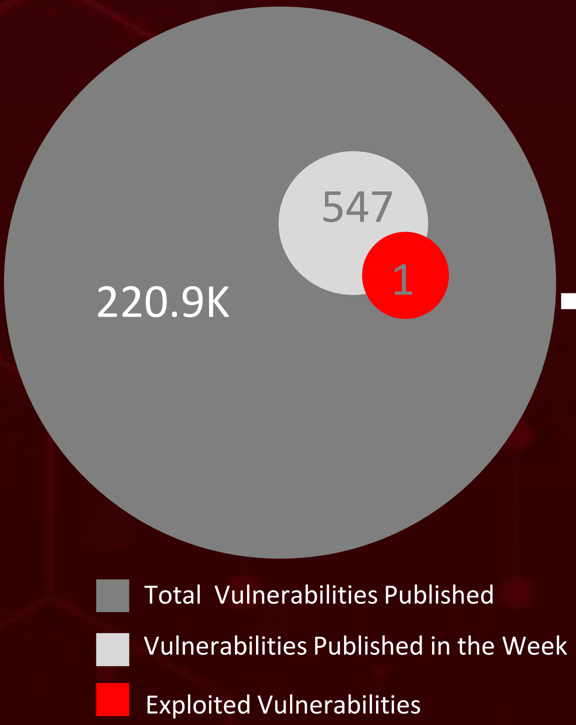
Table Of Contents

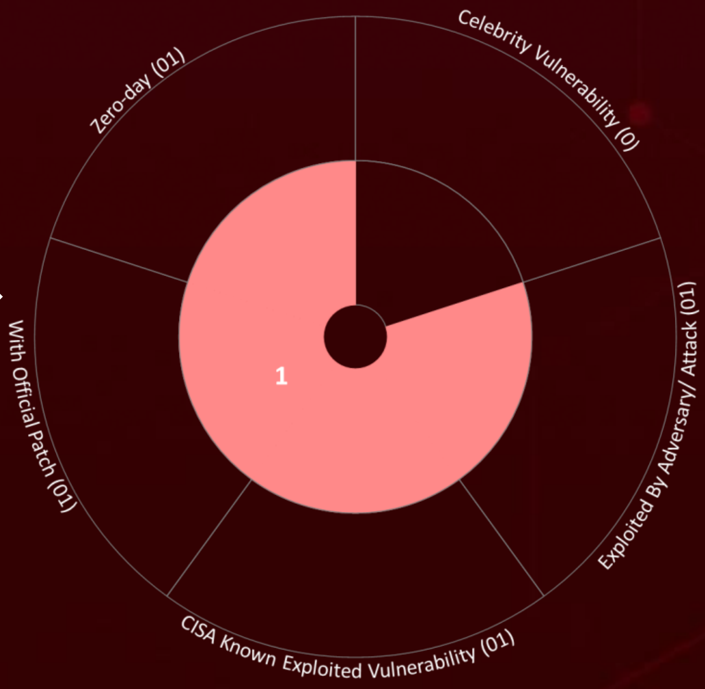
Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **six** attacks executed, **one** vulnerability, and **two** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForce Labs discovered that the **Barracuda zero-day** vulnerability was exploited by the **UNC4841** threat actor, playing a pivotal role in their extensive global espionage campaign. Additionally, identified **Trash Panda** a ransomware strain that specifically targets Windows platforms in the United States and the Czech Republic.

In the meantime, a Chinese nation-state activity group known as **Flax Typhoon** is engaging in espionage against organizations in Taiwan. These attacks are on the rise, posing a significant threat to users worldwide.





High Level Statistics

6

Attacks Executed

- Agniane Stealer
- Trash Panda Ransomware
- DEPTHCHARGE
- SKIPJACK
- FOXTROT
- FOXGLOVE

1

Vulnerabilities Exploited

- CVE-2023-2868

2

Adversaries in Action

- Flax Typhoon
- UNC4841

Insights

Crypto Heist Alert:
AgnianeStealer, the Silent Predator of Cryptocurrency Wallets

Trash Panda Ransomware:
Disseminating Ransom Notes with Political Messages While Targeting the United States and Czech Republic

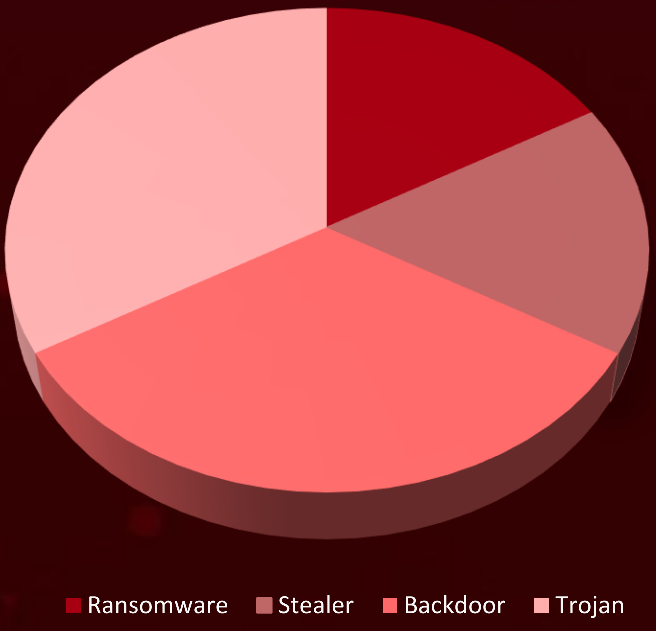
UNC4841's Tactical Arsenal
Deploys an array of Malware Mayhem to yield Persistence.

UNC4841: Spearheading Global Espionage with Barracuda ESG Exploits

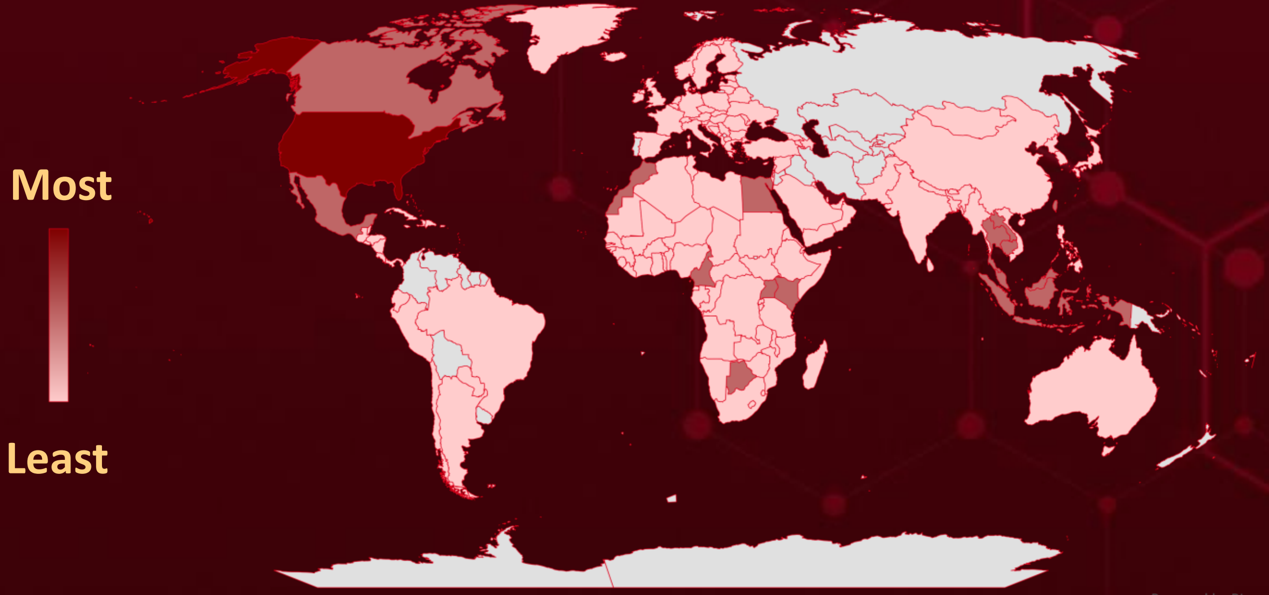
Global Cyber Hotspots: **United States**, **Thailand**, and **Mexico** Top the List of Targets Last Week

Flax Typhoon
A Stealthy Chinese Espionage Threat in Taiwan

Threat Distribution



Targeted Countries

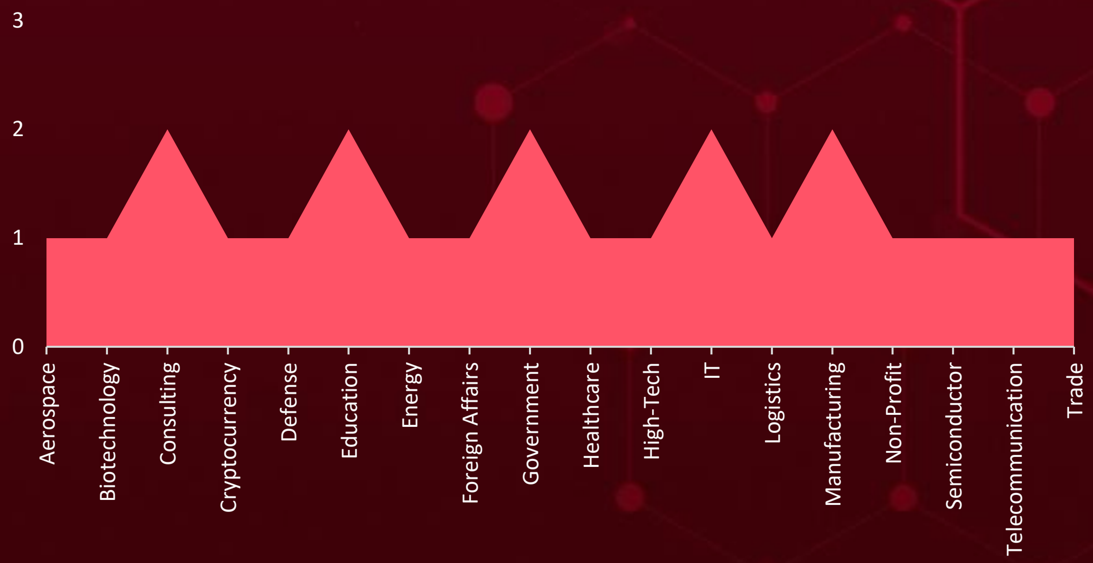


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

	Countries
■	United States
▨	Thailand
▨	Mexico
▨	Western Sahara
▨	Brunei
▨	Singapore
▨	Cambodia
▨	Kenya
▨	Cameroon
▨	Malaysia
▨	Canada
▨	Morocco
▨	East Timor
▨	Taiwan
▨	Egypt
▨	Botswana
▨	Uganda
▨	Indonesia
▨	Laos
□	Saint Vincent and the Grenadines
□	Montenegro
□	United Arab Emirates
□	Bermuda
□	Palestine
□	Bhutan
□	Spain
□	Bosnia and Herzegovina
□	Malta
□	Algeria
□	Nicaragua
□	Brazil
□	Republic of the Congo
□	British Virgin Islands
□	Bangladesh
□	Andorra
□	Belarus
□	Bulgaria
□	Malawi
□	Burkina Faso
□	Bahamas
□	Burundi
□	Myanmar
□	Angola
□	North Macedonia
□	Anguilla
□	Philippines
□	Antigua and Barbuda
□	Saint Kitts and Nevis
□	Cape Verde
□	Senegal
□	Caribbean Netherlands
□	Somalia
□	Cayman Islands
□	Switzerland
□	Central African Republic
□	Turkey
□	Chad
□	Vatican City
□	Chile
□	Maldives
□	China
□	Mauritania
□	Comoros
□	Monaco
□	Costa Rica
□	Bahrain
□	Croatia
□	Nepal
□	Cuba
□	Nigeria
□	Curaçao
□	Oman
□	Cyprus
□	Paraguay
□	Czech Republic
□	Puerto Rico
□	Czechia
□	Rwanda
□	Denmark
□	Saint Martin
□	Djibouti
□	São Tomé and Príncipe
□	Dominica
□	Seychelles
□	Dominican Republic
□	Slovakia
□	DR Congo
□	South Korea
□	Argentina
□	Sudan
□	Ecuador
□	Barbados
□	Armenia
□	Trinidad and Tobago
□	El Salvador
□	Belgium
□	Equatorial Guinea
□	Belize
□	Eritrea
□	Benin
□	Estonia
□	Azerbaijan
□	Eswatini
□	Mali
□	Ethiopia
□	Martinique
□	Finland

Targeted Industries



TOP MITRE ATT&CK TTPs

T1036 Masquerading

T1059 Command and Scripting Interpreter

T1105 Ingress Tool Transfer

T1543 Create or Modify System Process

T1003 OS Credential Dumping

T1071 Application Layer Protocol

T1082 System Information Discovery

T1005 Data from Local System

T1486 Data Encrypted for Impact

T1190 Exploit Public-Facing Application

T1036.005 Match Legitimate Name or Location

T1027.002 Software Packing

T1041 Exfiltration Over C2 Channel

T1027 Obfuscated Files or Information

T1047 Windows Management Instrumentation

T1212 Exploitation for Credential Access

T1055 Process Injection

T1505 Server Software Component

T1056 Input Capture

T1543.004 Launch Daemon

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agniane Stealer	The AgnianeStealer, coded in C#, operates as an information pilferer. It primarily focuses on extracting stored credentials from a wide array of sources, with a specific emphasis on targeting cryptocurrency extensions and wallets.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Credential theft	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

IOC TYPE	VALUE
Host Name	Central-cee-doja[.]ru
MD5	522101881b87ccda4d78fac30e951d19, 0d20e90382f881116201ac7c9298aab6, a1b5e20b58d23b26f640f252ece0891b, 5c0f65523f7ecb773c599b59d5cc3578, a2b20120a92c3de445b0b384a494ed39, d811a57bc0e8b86b449277f9ffb50cc9, b62ef0920a545f547d6cd3cd2abd60d2

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Trash Panda Ransomware	Trash Panda is a ransomware that encrypts files on Windows machines, replaces the desktop wallpaper, and drops a ransom note with political messages. It adds a '.monochrome' extension to the encrypted files and demands payment for decryption.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db
SHA1	d5d37ae269008e9bfddc171c3b05bd3d43a5cd4d
MD5	a0fea954561663f60059420e6c78fa5c

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
DEPTHCHARGE (aka SUBMARINE)	UNC4841 employed the backdoor DEPTHCHARGE to sustain persistence. DEPTHCHARGE passively listens for encrypted com mands, which it decrypts with OpenSSL and perfor ms before delivering the results back to the comm and and control (C2) serv er disguised as SMTP co mmands.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and Espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINKS**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

IOC TYPE	VALUE
MD5	c5c93ba36e079892c1123fe9dffd660f, dde2d3347b76070fff14f6c0412f95ba, 03e07c538a5e0e7906af803a83c97a1e, 0dd78b785e7657999d05d52a64b4c4cf

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SKIPJACK	SKIPJACK is a backdoor trojan that was used by the Chinese nexus threat group UNC4841. It is a modular malware that can be customized to perform a variety of tasks. It's delivered via phishing emails or exploit kits. Once it is installed on a system, it can be used to steal sensitive information.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and Espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINKS**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

IOC TYPE	VALUE
MD5	d81263e6872cc805e6cf4ca05d86df4e, ad1dc51a66201689d442499f70b78dea, 3273a29d15334efddd8276af53c317fb, 446f3d71591afa37bbd604e2e400ae8b, 87847445f9524671022d70f2a812728f, 9aa90d767ba0a3f057653aadcb75e579

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
FOXTROT	FOXTROT is a malware family that has been used by the Chinese-nexus threat group UNC4841. It is a C++ implant that is launched using a C-based program dubbed FOXGLOVE. Communicating via TCP, it comes with features to capture keystrokes, run shell commands, transfer files, and set up a reverse shell.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft and Espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINKS**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

IOC TYPE	VALUE
MD5	a28de396aa91b7faca35e861b634c502

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FOXGLOVE	FOXGLOVE is a malware family that has been used by the Chinese-nexus threat group UNC4841. It is a modular malware that can be customized to perform a variety of tasks.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft and Espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINKS**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

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-2023-2868	✗	Barracuda Networks Email Security Gateway (ESG): 5.1.3 -9.2	UNC4841
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:barracuda:email_security_gateway_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:barracuda:email_security_gateway:-:*:*:*:*:*:*:*	DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE
Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20 CWE-77	T1059: Command and Scripting Interpreter	https://status.barracuda.com/incidents/34kx82j5n4q9

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Flax Typhoon	China	Government agencies, Education, Critical Manufacturing, and Information Technology Organizations	Taiwan, Southeast Asia, North America and Africa
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1190: Exploit Public-Facing Application; T1505.003: Web Shell; T1505: Server Software Component; T1059: Command and Scripting Interpreter; T1546: Event Triggered Execution; T1546.008: Accessibility Features;T1105: Ingress Tool Transfer ; T1543: Create or Modify System Process; T1543.003: Windows Service; T1003.001: LSASS Memory; T1550: Use Alternate Authentication Material; T1003: OS Credential Dumping; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1003.002: Security Account Manager; T1572: Protocol Tunneling; T1550.002: Pass the Hash			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UNC4841	China	Government, High-Tech, IT, Healthcare, Biotechnology, Telecommunication, Defense, Aerospace, Education, Consulting and Professional Services, Trade, Semiconductor, Energy, Non-Profit, Logistics, Manufacturing, Foreign Affairs	Parts of Europe, Asia, South Africa, Australia, and the USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-2868	DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE	Barracuda Networks Email Security Gateway (ESG) Appliance
TTPs			
T1543: Create or Modify System Process; T1543.004: Launch Daemon; T1574: Hijack Execution Flow; T1068: Exploitation for Privilege Escalation; T1055: Process Injection; T1211: Exploitation for Defense Evasion; T1059: Command and Scripting Interpreter; T1212: Exploitation for Credential Access; T1056: Input Capture; T1056.001: Keylogging; T1560 Archive Collected Data T1005 Data from Local System l; T1132: Data Encoding; T1105: Ingress Tool Transfer; T1588.006: Vulnerabilities;			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actors **Flax Typhoon, UNC4841,** and malware **Agniane Stealer, Trash Panda Ransomware, Depthcharge, Skipjack, Foxtrot, Foxglove**.

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 **one exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Flax Typhoon, UNC4841** and malware **Agniane Stealer, Trash Panda Ransomware, Depthcharge, Skipjack, Foxtrot, Foxglove** in Breach and Attack Simulation(BAS).

Threat Advisories

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)

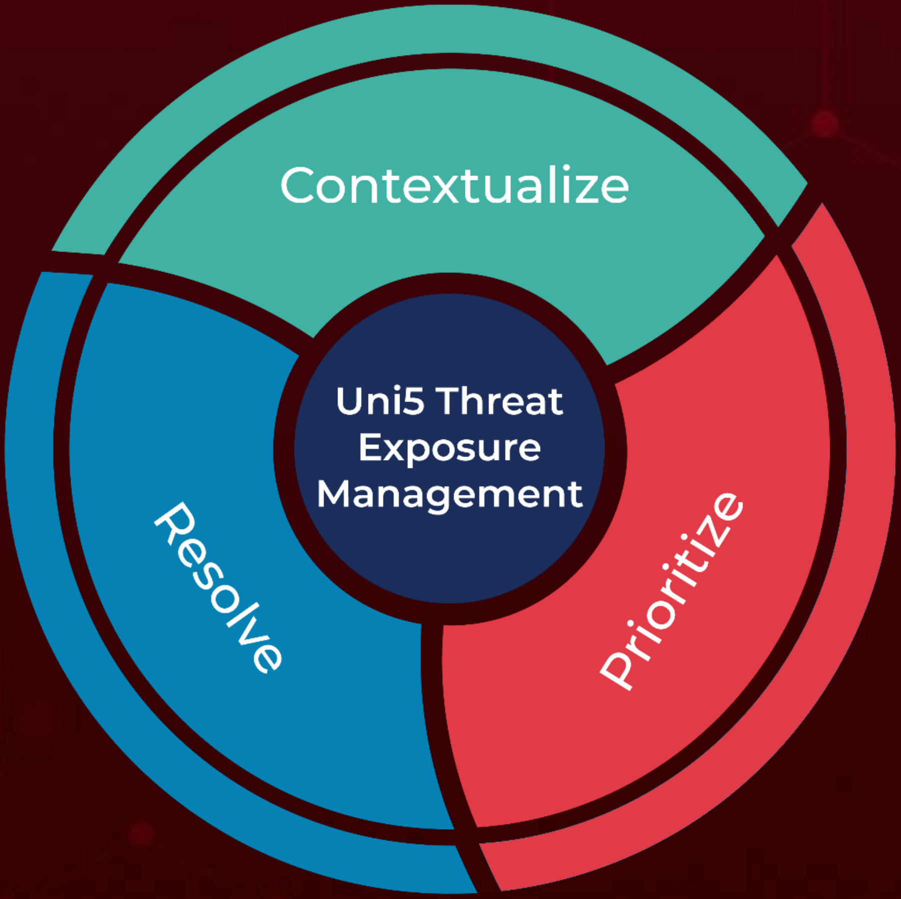
Attack Name	TYPE	VALUE
Agniane Stealer	Host Name	Central-cee-doja[.]ru
	MD5	522101881b87ccda4d78fac30e951d19, 0d20e90382f881116201ac7c9298aab6, a1b5e20b58d23b26f640f252ece0891b, 5c0f65523f7ecb773c599b59d5cc3578, a2b20120a92c3de445b0b384a494ed39, d811a57bc0e8b86b449277f9ffb50cc9, b62ef0920a545f547d6cd3cd2abd60d2
	SHA256	b5f11e9a19a7972bb65d5c46664a7f7594a946b3bdd9760697fd39f6d607b557, 560017cc0ca317e8c6437ed46a417e782f02a860f917d6fa682bca26158d1cf0, 24bd790bc9427021121ec0e318db93369c2d893e40309f7083f178d3a5819161
	SHA1	f82093aa3c483dca6ace0f5c8dec104800b8d494, cdab34eea2dfd5e96412e34c0b3eb090a9661377, 3830039ada6bb8d3050dc7748d77bcb7b0cc003f
Trash Panda Ransomware	SHA256	ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db
	SHA1	d5d37ae269008e9bfddc171c3b05bd3d43a5cd4d
	MD5	a0fea954561663f60059420e6c78fa5c
DEPTHCHARGE	MD5	c5c93ba36e079892c1123fe9dffd660f, dde2d3347b76070fff14f6c0412f95ba, 03e07c538a5e0e7906af803a83c97a1e,

Attack Name	TYPE	VALUE
DEPTHCHARGE	MD5	0dd78b785e7657999d05d52a64b4c4cf, 35a432e40da597c7ab63ff16b09d19d8, 806250c466824a027e3e85461dc672db, 830fca78440780aef448c862eee2a8ac, b354111afc9c6c26c1475e761d347144, b745626b36b841ed03eddfb08e6bb061, b860198feca7398bc79a8ec69afc65ed, c2e577c71d591999ad5c581e49343093, e68cd991777118d76e7bce163d8a2bc1, ed648c366b6e564fc636c072bbcac907, ff005f1ff98ec1cd678785baa0386bd1
SKIPJACK	MD5	d81263e6872cc805e6cf4ca05d86df4e, ad1dc51a66201689d442499f70b78dea, 3273a29d15334efddd8276af53c317fb, 446f3d71591afa37bbd604e2e400ae8b, 87847445f9524671022d70f2a812728f, 9aa90d767ba0a3f057653aadcb75e579, e4e86c273a2b67a605f5d4686783e0cc, ec0d46b2aa7adfdff10a671a77aeb2ae
FOXTROT	MD5	a28de396aa91b7faca35e861b634c502

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 4, 2023 • 10:00 PM

More at www.hivepro.com