

Date of Publication
May 27, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

20 to 26 MAY 2024

Table Of Contents

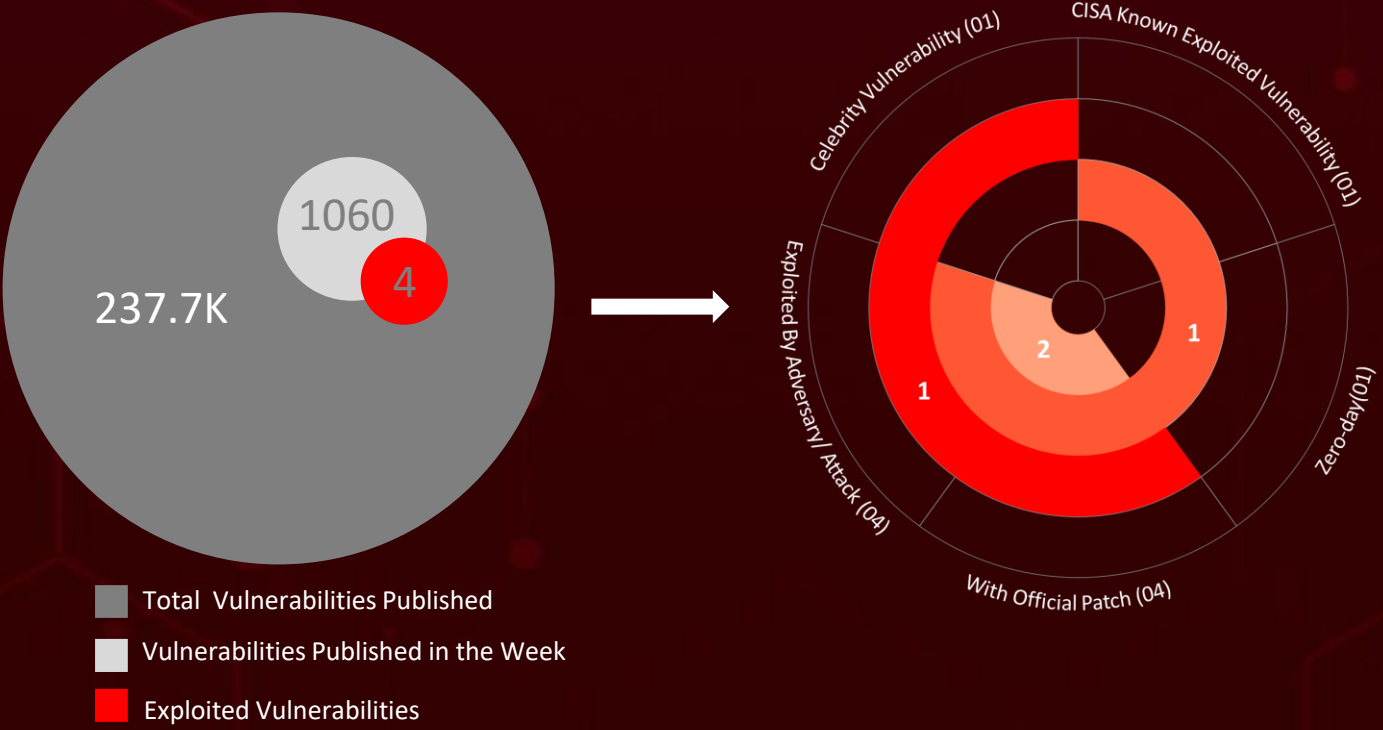
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	29

Summary

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

Furthermore, HiveForce Labs discovered that the '**REF4578**' campaign uses the GhostEngine payload to exploit driver vulnerabilities, disable security products, and install an XMRig miner. GhostEngine ensures the miner's persistence and undetected operation by leveraging elevated privileges and disabling antivirus and endpoint protection tools.

The China-linked threat actor **Sharp Dragon**, previously known as Sharp Panda has expanded its cyber espionage campaign to target governmental organizations in Africa and the Caribbean. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

12

Attacks
Executed

4

Vulnerabilities
Exploited

3

Adversaries in
Action

- [Metamorfo](#)
 - [Grandoreiro](#)
 - [Dora RAT](#)
 - [Nestdoor](#)
 - [D3F@ck](#)
 - [GhostEngine](#)
 - [XMRig](#)
 - [Acrid](#)
 - [ScarletStealer](#)
 - [Sys01](#)
 - [5.t Downloader](#)
 - [Tiny backdoor](#)
- [CVE-2024-4323](#)
 - [CVE-2024-27130](#)
 - [CVE-2024-4985](#)
 - [CVE-2023-0669](#)
- [Andariel](#)
 - [Sharp Dragon](#)
 - [Turla](#)



Insights

Metamorfo

an advanced banking trojan primarily targeting users in North and South America

Linguistic Lumberjack

CVE-2024-4323 as known as Linguistic Lumberjack is a critical memory corruption vulnerability found in Fluent Bit versions 2.0.7 through 3.0.3

D3FCK Loader

is a new malware loader that leverages Google Ads and EV certificates to bypass security measures

Grandoreiro

banking Trojan, initially targeting Latin America, has evolved to attack financial institutions globally, now targeting over 1500 banks in 60 countries

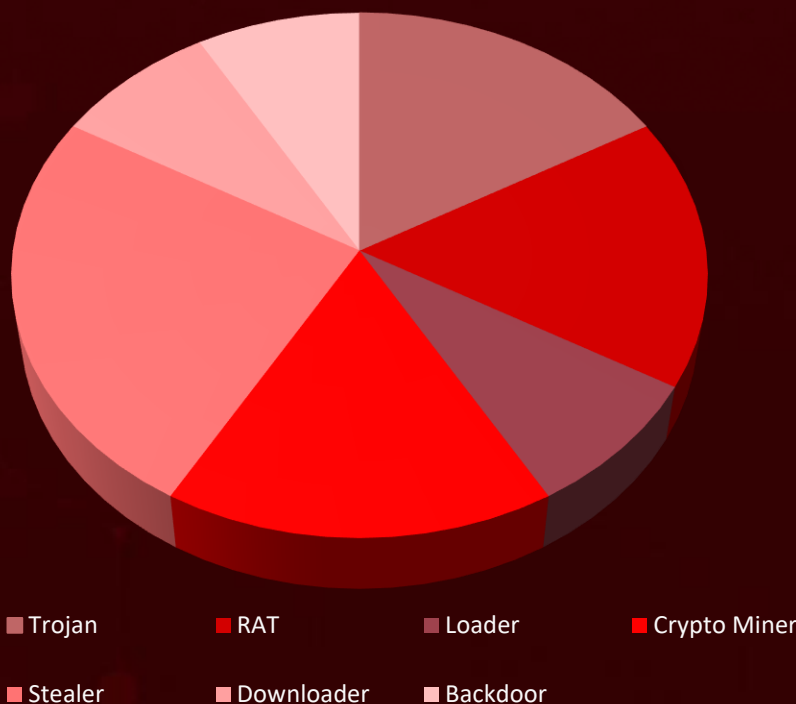
Andariel APT group

attacked South Korean manufacturing, construction, and educational companies using the Dora RAT and proxy tools to infiltrate systems, extract data, and control compromised machines

CLOUD#REVERSER

is a campaign using Google Drive and Dropbox for malicious operations by threat actors

Threat Distribution

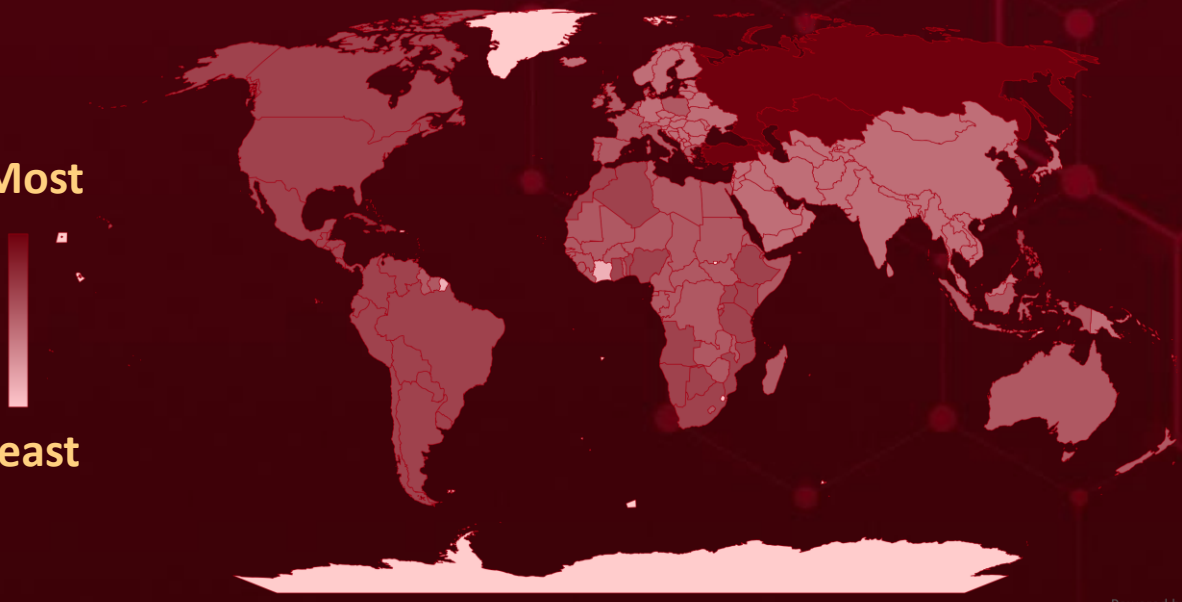




Targeted Countries

Most

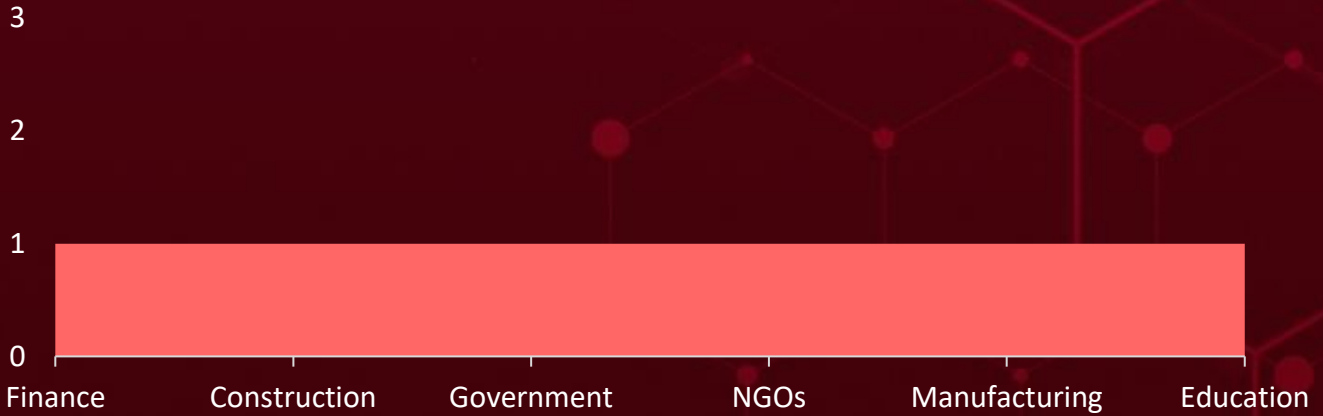
Least



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Countries	Countries	Countries	Countries
Cyprus	South Africa	Honduras	Guyana
Russia	Panama	Chile	Mali
Kazakhstan	Mozambique	Uruguay	Sierra Leone
Armenia	Djibouti	Costa Rica	Mauritania
Turkey	Algeria	Canada	South Sudan
Azerbaijan	Bolivia	Tanzania	Mauritius
Georgia	Uganda	Argentina	Switzerland
Bahamas	Botswana	Angola	Equatorial Guinea
Saint Vincent and the Grenadines	Nicaragua	Kenya	Tunisia
Saint Kitts and Nevis	Ecuador	Benin	Eritrea
Barbados	Peru	Mexico	Belgium
Grenada	El Salvador	Venezuela	Cameroon
Cuba	Colombia	Senegal	Rwanda
Jamaica	Ethiopia	Italy	France
Antigua and Barbuda	Belize	Sudan	Guinea-Bissau
Saint Lucia	United States	Comoros	Netherlands
Dominica	Morocco	Guinea	São Tomé and Príncipe
Trinidad and Tobago	Ghana	Lesotho	New Zealand
Dominican Republic	Namibia	Central African Republic	Seychelles
Haiti	Brazil	Liberia	Gabon
	Nigeria	Togo	Somalia
	Guatemala	Madagascar	Niger
	Paraguay	Denmark	South Korea
	Burundi	Malawi	Gambia
	Philippines		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566

Phishing

T1190

Exploit Public-Facing Application

T1057

Process Discovery

T1027

Obfuscated Files or Information

T1059

Command and Scripting Interpreter

T1055

Process Injection

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1068

Exploitation for Privilege Escalation

T1059.001

PowerShell

T1140

Deobfuscate/Decode Files or Information

T1010

Application Window Discovery

T1588.005

Exploits

T1056

Input Capture

T1547

Boot or Logon Autostart Execution

T1041

Exfiltration Over C2 Channel

T1204.002

Malicious File

T1204

User Execution

T1082

System Information Discovery

T1562.001

Disable or Modify Tools

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Metamorfo</u>	Metamorfo, also referred to as Mekotio or Casbaneiro, is an advanced banking Trojan disseminated through malspam campaigns, primarily targeting users in North and South America. Active since 2018, this malware is designed to pilfer financial information and banking credentials.	Malspam campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Data theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	71908b731b9bd2c6e5430f35eea2ded9041c272d61dd676a4456201e31e07444, 8c27321c5bc40131cf7873a52907433ae736e8e2801ec8aad350c17852b55af, c3d85c05121900c93f667ff65073ef331d37e65eea9bd4c60252dba9764056a3, 690ada1acafbfbffbb68f52e981ef1d98cbb781627dfa7b3d5653aba2feaf5d79		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Grandoreiro</u>	The Grandoreiro banking Trojan, initially targeting Latin America, has evolved to attack financial institutions globally, now targeting over 1500 banks in 60 countries. The latest variant can harvest email addresses from infected Outlook clients to send further phishing emails.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Data theft and Manipulate transactions	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5feb69dfd81e85f581, afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40, f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb, 10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1, 55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965		

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
<u>Dora RAT</u>	The attackers introduced a new malware, Dora RAT, developed in the Go language. Dora RAT is relatively simple, supporting reverse shell and file download/upload functions. It exists in two variants: one as a standalone executable and another injected into the explorer.exe process.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			-
ASSOCIATED ACTOR			PATCH LINK
Andariel group			-
IOC TYPE	VALUE		
MD5	4bc571925a80d4ae4aab1e8900bf753c, 951e9fcd048b919516693b25c13a9ef2, fee610058c417b6c4b3054935b7e2730, afc5a07d6e438880cea63920277ed270, d92a317ef4d60dc491082a2fe6eb7a70,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nestdoor</u>	Nestdoor is a RAT malware that has been active since at least May 2022. It enables attackers to control infected systems by receiving commands remotely. The Andariel group has been consistently linked to attack cases involving this malware.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			-
ASSOCIATED ACTOR			PATCH LINK
Andariel group			-
IOC TYPE	VALUE		
MD5	7416ea48102e2715c87edd49ddbd1526, a2aefb7ab6c644aa8eeb482e27b2dbc4, e7fd7f48fbf5635a04e302af50dfb651, 33b2b5b7c830c34c688cf6ced287e5be		

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
D3F@ck	D3F@ck Loader is a new malware loader that leverages Google Ads and EV certificates to bypass security measures. It can download other malware, including Raccoon Stealer and Danabot. It impersonates legitimate applications to trick users into downloading it.	Google ads	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			Windows
ASSOCIATED ACTOR			PATCH LINK
-		Malware Deployment and System Compromise	-
IOC TYPE	VALUE		
MD5	44b14057ff868e25ad444fac098d89f0, 87cb408a03daa827f9cc10698ba69a90, 56f2d534631400ef294d321f8dbdfea, 5cf2e80ac2a7f7fa24f74966d3ec904f, 815b3c88950fd572bb4bfef96d2ca23d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GhostEngine	GhostEngine is a sophisticated malware that disables security measures and uses advanced techniques to install and maintain a persistent crypto-miner on infected systems. It employs methods like leveraging vulnerable drivers and PowerShell scripts to deploy the XMRig Monero miner.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Crypto Miner			-
ASSOCIATED ACTOR			PATCH LINK
-		Cryptomining	-
IOC TYPE	VALUE		
SHA256	2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59ecbd25753, 6f3e913c93887a58e64da5070d96dc34d3265f456034446be89167584a0b347e, 7c242a08ee2dfd5da8a4c6bc86231985e2c26c7b9931ad0b3ea4723e49ceb1c1, cc4384510576131c126db3caca027c5d159d032d33ef90ef30db0daa2a0c4104		

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
XMRig	<p>XMRig is an open-source cryptocurrency mining software commonly used to mine Monero (XMR). While it can be used legitimately, it is often exploited by cybercriminals in malware campaigns to secretly mine cryptocurrency on infected systems, draining system resources and reducing performance</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Crypto Miner			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	<p>23924cb27039491348cfa9a78c65ab3f6af5d0fa1efe61c90b6d7541c6de896fc184a73f45c5b340409258c3a9c38e459a6aef8307f710f0eb967a7ff547858be875c8c9ee9962f28684d9090a96e6a0112cd4d875c802686de158ee64f0925f1afdadf62ec8d374f9c601bf77660f1816998e773c040631c0bbcd28e479b1aafe854f6d0ab457d19c354d227ace5edcd43c13194a058671403d42556b103eb3</p>		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Acrid	<p>Acrid malware is a type of information stealer that spreads primarily through malicious email attachments and websites, targeting login credentials, cookies, and other sensitive data from browsers. Acrid is written in C++ for the 32-bit system.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	<p>abceb35cf20f22fd8a6569a876e702cb, 2b71c81c48625099b18922ff7bebbf51, b9b83de1998ebadc101ed90a6c312da8</p>		

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
ScarletStealer	ScarletStealer is a sophisticated information-stealing malware that often disguises itself as legitimate software to trick users. It targets a wide range of data, including cryptocurrency wallets, gaming accounts, and social media credentials.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Data theft	-
IOC TYPE	VALUE		
MD5	1d3c3869d682fbd0ae3151b419984771, c0cf3d6d40a3038966f2a4f5bfe2b7a7, f8b2b941cffb9709ce8f422f193696a0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sys01	SYS01, also known as "Album Stealer" or "S1deload Stealer," is a relatively unknown malware active since at least 2022. It has evolved from a C# stealer to a PHP-based variant, with recent versions combining both C# and PHP payloads.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Data theft	-
IOC TYPE	VALUE		
MD5	6e2b16cc41de627eb7ddcd468a037761, 21df3a69540c6618cfbdaf84fc71031c, 23ae473bc44fa49b1b221150e0166199		




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
<u>5.t Downloader</u>	The 5.t downloader is a malicious program specialized in downloading and installing additional malware on infected systems. It spreads via phishing emails, malicious websites, or bundled software, establishing connections to remote servers to fetch and deploy harmful payloads, facilitating multi-stage cyberattacks.	-	CVE-2023-0669
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader			
ASSOCIATED ACTOR		Downloads other malware	PATCH LINK
Sharp Dragon			
IOC TYPE	VALUE		
SHA256	21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6, 7575ebdd90aa0ab66c4eeaec628c475e406ac9bcc54de5e01a3d372a050aec7, b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab339214f4e57, 42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc, 941e52ce5ce89b7307bdf1b88657dfd76892b475971b86683cfc6fbca23e209,		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Tiny backdoor</u>	A sophisticated campaign by the Turla APT group, is employing a Tiny backdoor. It uses malicious .LNK files disguised as legitimate documents to target individuals and leverages MSBuild to evade detection.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Data theft	PATCH LINK
Turla			
IOC TYPE	VALUE		
SHA256	b4db8e598741193ea9e04c2111d0c15ba79b2fa098efc3680a63ef457e60dbd9, 6829ab9c4c8a9a0212740f46bf93b1cbe5d4256fb4ff66d65a3a6eb6c55758a1, 8c97df4ca1a5995e22c2c4887bea2945269d6f5f158def98d5ebdd5311bb20c4, 76629afb86bd9024c3ea6759e0041d1f8182d206cf3bd1b4, c2618fb013135485f9f9aa27983df3371dfdcb7beecde86d02cee0c258d5ed7f, cac4d4364d20fa343bf681f6544b31995a57d8f69ee606c4675db60be5ae8775		




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-2024-4323		Fluent Bit versions 2.0.7 thru 3.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fluent_bit:fluent_bit:*:*:*:*:*	-
Linguistic Lumberjack (Fluent Bit Memory Corruption Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1190 : Exploit Public-Facing Application, T1082 : System Information Discovery	https://github.com/fluent-bit/releases/tag/v3.0.4

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27130		QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qnap:qts:*:*:*:*:* cpe:2.3:a:qnap:quts_hero:*:*:*:*:*	-
QNAP QTS/QuTS hero Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1068 : Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://www.qnap.com/en-in/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4985</u>		All versions of GitHub Enterprise Server prior to 3.13.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
GitHub Enterprise Server Authentication Bypass Vulnerability		cpe:2.3:a:github:enterprise_server:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-303	T1190 : Exploit Public-Facing Application, T1556 : Modify Authentication Process	https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.4 ; https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.10 ; https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.12 ; https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.15

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-0669</u>		Fortra GoAnywhere MFT version prior to 7.1.2	Sharp Dragon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortra:goanywhere _managed_file_transfer:*:*: *:*:*:*:*	5.t Downloader
Fortra GoAnywhere MFT Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059 : Command and Scripting Interpreter, T1203 : Exploitation for Client Execution	https://my.goanywhere.com/webclient/Login.xhtml


Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)</u></p>	North Korea	Government Agencies, Military Organizations, Financial Services	South Korea
	MOTIVE Espionage, Monetary Gains		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Dora RAT, Nestdoor	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1113: Screen Capture; T1056.001: Keylogging; T1584: Compromise Infrastructure; T1584.004: Server; T1566: Phishing; T1204: User Execution; T1055: Process Injection; T1027: Obfuscated Files or Information; T1049: System Network Connections: Discovery; T1082: System Information Discovery; T1057: Process Discovery; T1560: Archive Collected Data; T1005: Data from Local System; T1056: Input Capture; T1115: Clipboard Data; T1657: Financial Theft; T1053.005: Scheduled Task; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Sharp Dragon</u>	China	Government	Africa and the Caribbean
	MOTIVE Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	CVE-2023-0669	5.t Downloader	Fortra GoAnywhere MFT

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0043: Reconnaissance, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1036: Masquerading, T1012: Query Registry, T1018: Remote System Discovery, T1057: Process Discovery, T1082: System Information Discovery, T1083: File and Directory Discovery, T1001: Data Obfuscation, T1071: Application Layer Protocol, T1095: Non-Application Layer Protocol, T1105: Ingress Tool Transfer, T1573: Encrypted Channel, T1053: Scheduled Task/Job, T1588.001: Malware, T1588.002: Tool, T1588.006: Vulnerabilities, T1566: Phishing, T1203: Exploitation for Client Execution, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File:

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa)</u></p>	Russia	NGOs	Philippines
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	TARGETED CVEs		
-	Tiny backdoor	Windows	

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0005: Defense Evasion; TA0011: Command and Control; T1036: Masquerading, T1573: Encrypted Channel, T1053: Scheduled Task/Job, T1566: Phishing, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File, T1059.001: PowerShell, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1127: Trusted Developer Utilities Proxy Execution, T1127.001: MSBuild, T1071: Application Layer Protocol, T1041: Exfiltration Over C2 Channel, T1027: Obfuscated Files or Information

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **Andariel, Sharp Dragon, Turla** and malware **Metamorfo, Grandoreiro, Dora RAT, Nestdoor, D3F@ck, GhostEngine, XMRig, Acrid, ScarletStealer, Sys01, 5.t Downloader, Tiny backdoor**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **four exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Andariel, Sharp Dragon, Turla** and malware **Metamorfo, Grandoreiro, Nestdoor, D3F@ck, GhostEngine, Acrid, ScarletStealer** in Breach and Attack Simulation(BAS).

Threat Advisories

[Metamorfo Banking Trojan Targets the Americas](#)

[Grandoreiro Trojan: An Evolving Threat to Global Banking](#)

[Critical 'Linguistic Lumberjack' Flaw in Fluent Bit Hits Major Cloud Providers](#)

[Breaking Down Andariel APT's Strike on South Korean Entities](#)

[QNAP Flaws Enable Remote Code Execution Under Certain Conditions](#)

[CLOUD#REVERSER: From Cloud Storage to Command and Control](#)

[D3F@ck Loader: New Malware Exploits Google Ads and EV Certificates](#)

[Patch Now: Critical Auth Bypass Flaw in GitHub Enterprise Server Fixed](#)

[REF4578 Campaign Unleashes the Highly Modular GhostEngine Malware](#)

[Stealing the Spotlight a Comprehensive Look at Stealers](#)

[Sharp Dragon's Foray into African and Caribbean Governance Networks](#)

[Turla's Tiny Backdoor Exploits MSBuild to Evade Detection](#)

[GitLab Flaw Allows Account Takeover via XSS Attacks](#)

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
<u>Metamorf</u> <u>o</u>	SHA256	71908b731b9bd2c6e5430f35eea2ded9041c272d61dd676a4456201e31e07444, 8c27321c5bc40131cf7873a52907433ae736e8e2801ec8aad350c17852b55af, c3d85c05121900c93f667ff65073ef331d37e65eea9bd4c60252dba9764056a3, 690ada1acafbfbfb68f52e981ef1d98cbb781627dfa7b3d5653aba2feaf5d79
	SHA1	45f8c91f0299012a8dcb40d9a2fb5ce7962b887a, a9e9df6762418bbbed030e825099282da59278db0, 2bd4acea5c3bf107cc6615af65d1617c847814cc, 4b5b7cf403ac7d6e3dd787104e3e6bd088743815
<u>Grandorei</u> <u>ro</u>	SHA256	97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5febf69dfd81e85f58, afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40, f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb, 10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1, 55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965, bfcd71a4095c2e81e2681aaf0239436368bc2ebddae7fdc8bb486ffc1040602c, 3f920619470488b8c1fda4bb82803f72205b18b1ea31402b461a0b8fe737d6bd, 84572c0de71bce332eb9fa03fd342433263ad0c4f95dd3acd86d1207fa7d23f0,

Attack Name	TYPE	VALUE
Grandoreiro	SHA256	29f19d9cd8fe38081a2fde66fb2e1eff33c4d4b5714ef5cada5cc76ec09bf2fa, 2ab8c3a1a7fe14a49084fbf42bbdd04d6379e6ae2c74d801616e2b9cf8c8519c, 70f22917ec1fa3a764e21f16d68af80b697fb9d0eb4f9cd6537393b622906908, fb3d843d35c66f76b1b1b88260ad20096e118ef44fd94137dbe394f53c1b8a46, 6772d2425b5a169aca824de3ff2aac400fa64c3edd93faaab17d9c721d996c1
	URLs	hxxps[:]//onwfacttasunslahf[.]norwayeast[.]cloudapp[.]azure[.]com?_task=mail&_action=get&_mbox=INBOX&_uid=19101&_token=rbrJMXNUOQvrlaWOOxGAyj7vcufaFN3r&_part=1.2.3&_embed=1&_mimeclass=image, hxxps[:]//pjohconstruccionescpaz[.]com?docs/xml/WCA161006TN9/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp.azure[.]com/?PDF-XML-71348793, hxxps[:]//officebusinessaccount[.]eastus[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//hilcfacdigitaelpichipt[.]norwayeast[.]cloudapp.azure[.]com/?docs/pdf/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//pjohconstruccionescpaz[.]com/?8205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796
	Emails	gruposat[.]gob[.]mx, root[[@]]zpmbox[.]crazydocuments[.]com, marcasat[.]gob[.]mx , assistance[.]gov[.]za , ^root[.]yhspld{2}[.]rufnag[.]com\$
	Domains	Rufnag[.]com, pjohconstruccionescpaz[.]com
	IPv4	18[.]231[.]181[.]227, 18[.]231[.]158[.]159, 15[.]229[.]211[.]175, 15[.]228[.]245[.]103

Attack Name	TYPE	VALUE
<u>Dora RAT</u>	MD5	4bc571925a80d4ae4aab1e8900bf753c, 951e9fcd048b919516693b25c13a9ef2, fee610058c417b6c4b3054935b7e2730, afc5a07d6e438880cea63920277ed270, d92a317ef4d60dc491082a2fe6eb7a70, 5df3c3e1f423f1cce5bf75f067d1d05c, 094f9a757c6dbd6030bc6dae3f8feab3
	Domain	kmobile[.]bestunif[.]com
	IPv4:PORT	206[.]72[.]205[.]117[:]:443
<u>Nestdoor</u>	MD5	7416ea48102e2715c87edd49ddbd1526, a2aefb7ab6c644aa8eeb482e27b2dbc4, e7fd7f48fbf5635a04e302af50dfb651, 33b2b5b7c830c34c688cf6ced287e5be
	IPv4:PORT	45[.]58[.]159[.]237[:]:443, 4[.]246[.]149[.]227[:]:1443, 209[.]127[.]19[.]223[:]:443
<u>GhostEngine</u>	SHA256	2fe78941d74d35f721556697491a438bf3573094d7ac091b42e4f59e cbd25753, 6f3e913c93887a58e64da5070d96dc34d3265f456034446be8916758 4a0b347e, 7c242a08ee2dfd5da8a4c6bc86231985e2c26c7b9931ad0b3ea4723e 49ceb1c1, cc4384510576131c126db3caca027c5d159d032d33ef90ef30db0daa 2a0c4104
<u>XMRig</u>	SHA256	23924cb27039491348cfa9a78c65ab3f6af5d0fa1efe61c90b6d7541c6 de896f, c184a73f45c5b340409258c3a9c38e459a6aef8307f710f0eb967a7ff5 47858b, e875c8c9ee9962f28684d9090a96e6a0112cd4d875c802686de158ee 64f0925f, 1afdadf62ec8d374f9c601bf77660f1816998e773c040631c0bbcd28e 479b1aa, fe854f6d0ab457d19c354d227ace5edcd43c13194a058671403d4255 6b103eb3, 1d9876889cfdd7a19e0e847f87f069fd9152cb55d63ad2b1a4ee8e7ab d373e59, 265945c6b195c7d80665414a6f8789ddcd087c8804847b67662a780c 7bcdd748, 0c0fe53264eb7d9c50651ceaf3cafda42d765c13e6b2b7d845ad5e1f3 01c6d1f,

Attack Name	TYPE	VALUE
<u>XMRig</u>	SHA256	<p>2f135bcc75cf029452fd95e7f14a56ac0745c08f1a47d1218443a4e85a9b7, df99a6272dd4098f15e779047507f4bf95ba8350d8911382fab6fca66dc0a58a, 37aca4a08a53e90247b03a0da697b0cb47e566bf64ef58698f09f6509c09111f, 2d6fac4d3df78fed33d0e0e63dc49bc28657d92dc03379b79aafbc3bda791503, d0271cf08762e9abf52a8d7c1601686bdcd93b0ee32efb12987268049813a7ec, 9dad543968781b6c0af82369e57acf1f52938d77a6bb0fe5d0e8563588f43a95, c6207f7a4f92ad987e43dd3a65a0b50e1778ec8dccb63313d1a6df7d223ddf33, f829a7b5ab31ac6a37035b282e83d55da7d313c70d1ec11f8b6999d78294695e, 08f3805606e1d457ed9e80b975bee0320651e3d5626e9e7cb896fd45e8fd0f7b, cdeebebb4af40a2cea1aaf41db75f51d5bb511c328e8726256cb4fe7bacab2c8, 674f21780c32078f45bc05baeb308e16e841c4262d5aab352f3596669736b13b, 42fbdcb34832ff79d85b0c7c0cc7779fa3705dd28ba2119ef8e7e7a411afe467, 5f56885a9ac4593449b028b38341b16aabec3adb10702c0f498bc0feb9a2ecbe, 92da2571e11a7109bfbcb842dc2859df90feb518302e82d5ddebcd0192fc5b63, fde1de57feca954ba860096e3d209b247d7e498c4210eef1bf1f57f6658e361e, a37dfed9e6f606b7bac6f7aff22b4624e4f670c00a8abc2b229dca8477271bcc, b92736e9915aa13e805583eb82ef68d3de6c2869dd82fe774d013c92365f65ba, 38d6aab4e818507641c0eb76d6448299099823ae7d13bc2bb3be088ae3e24573, 8a73d77a47d29d0e94b3a0de81d626d625b36397ab308f2af2860feb9e9e465bf, 3b16767f4702e0eedb9461f53bb7794cc188627484efe72f80c4db492e0217d0, d44227d8241bd1ad48cc76771969f96152728d25916dc07b8b15290b9ba767a9, 29d73b2aed43aba1cf0b90278b0cf4d402c3e5e22b0ade679df88bd9e0142ba4, 5d7fc3917f5c5c77543305a2a5185e11755aadac4464937fea223c6e6520a5f3,</p>

Attack Name	TYPE	VALUE
<u>XMRig</u>	SHA256	<p>87903c2711c047be5ef295419311bc2a4712e0ab10cd4afe2ee01af6145995d0, e0dc29cd9f9fb36a67782abf6231073d54365fa1a4ddade12cf47984a6113b45, cd493e0109f708ba1ccd380f1efaeb6e7533baedf041ed055c621405cdf907b8, 209e301207a4695fa9d1642dd949f270298a82446e027ab8dd78a0d4e1ab2c35, 0d61b6eed0b001f11ed885a2223b39fdc461c2fe0f3338b81c22e11a4f1e9e52, b84cef08f737a9ad878e3ed98e4f3b61cc2e7440e7e0fc325a994e99f8c0cd2e, f241db8dea553a2add84eb7f7818a01bffcd5764e498953cd5a06e54ec8f5599, 8acc667814a5415b89bfaa445609dd68657359f78e6fe50013b436ff5506019e, e0ac7a9fa5503c78d75afbae370f4931aff9d7a18ff80c9c14060cd47045dcb5, be7ae8b05042920a137d990556062ad14b13607a222b8998f93d44dbd48bfda3, d68a529120da32c9e66410a0420f65b98752372bd321c7ff6f58ee3e0cf7af34, 065f21780636063a7b405e6d163b4db90960b84f99df884fbb1c616402ef0ff4, f7257f0645fb84a67c5a5b2dd12104cec156916f64aa7dadb1e354063f9a47a8, 507c455463c8222b988a2d988e742835e42ccc1ec45c3118039441c7e7242d95, 7ff80e19b49a455bd9facded8d476e79379514d78e6ada6087ae33a73cdfbc0c, 65321478bb2725e8c6285bf2b8aaa798034953a8b76f9cdf61a664066cee8444,</p>
<u>Acrid</u>	MD5	<p>abceb35cf20f22fd8a6569a876e702cb, 2b71c81c48625099b18922ff7bebbf51, b9b83de1998ebadc101ed90a6c312da8</p>
<u>ScarletStealer</u>	MD5	<p>1d3c3869d682fbd0ae3151b419984771, c0cf3d6d40a3038966f2a4f5bfe2b7a7, f8b2b941cffb9709ce8f422f193696a0</p>

Attack Name	TYPE	VALUE
<u>Sys01</u>	MD5	6e2b16cc41de627eb7ddcd468a037761, 21df3a69540c6618cfbdaf84fc71031c, 23ae473bc44fa49b1b221150e0166199
<u>5.t Downloader</u>	SHA256	21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df3 94cd7e6, 7575ebdd90aa0ab66c4eeaecd628c475e406ac9bcc54de5e01a3d372 a050aec7, b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab33 9214f4e57, 42095521622c055db8d79441317952c0899c34d7b776f6f45855581f b86522dc, 941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbc a23e209, e848355359de1e59901aa387f2d208889c368663438909fd3bb0a975 66de2b2d, cc805511e106a9b5302a4db4bfbb98609aca3dcbd2f709aee8ae316f4 79dfd49, ea72011929dece4684a2dcb5b76f34cef437dbe50306f19c531d632bf 26e7f32, 7b21b95c4256308e8089bff38d5d20845f2dc28fa9e536de979ceab9b 7962afa, e6faf05234ceaaba3bdcca60285a7ba83eea229a0ca241e94fb314a73 ad98d87, 20a4256443957fbae69c7c666ae025522533b849e01680287177110 603a83a41, 1c2a10f282f1a24d88c74d8d324fb59b172cee4ee2e3e3996d9a62ba 979812a6
<u>Tiny backdoor</u>	SHA256	b4db8e598741193ea9e04c2111d0c15ba79b2fa098efc3680a63ef45 7e60dbd9, 6829ab9c4c8a9a0212740f46bf93b1cbe5d4256fb4ff66d65a3a6eb6c 55758a1, 8c97df4ca1a5995e22c2c4887bea2945269d6f5f158def98d5ebdd531 1bb20c4, 76629afb86bd9024c3ea6759eeea197ba6c8c780e0041d1f8182d206 cf3bd1b4, c2618fb013135485f9f9aa27983df3371dfdcb7beecde86d02cee0c25 8d5ed7f, cac4d4364d20fa343bf681f6544b31995a57d8f69ee606c4675db60be 5ae8775

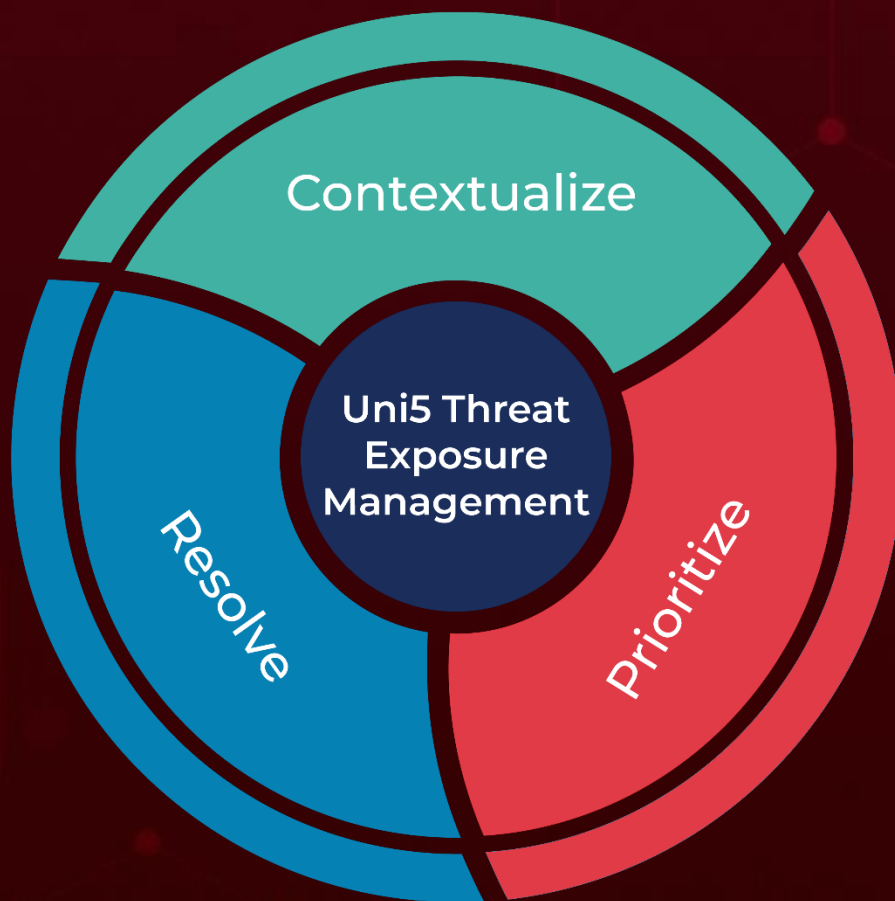
Attack Name	TYPE	VALUE
<u>D3F@ck</u>	MD5	44b14057ff868e25ad444fac098d89f0, 87cb408a03daa827f9cc10698ba69a90, 56f2d534631400ef294d321f8dbdfea, 5cf2e80ac2a7f7fa24f74966d3ec904f, 815b3c88950fd572bb4bfef96d2ca23d, be9989c6c218b0e99671a5bde240341e
	IPv4	194[.]147[.]35[.]251, 116[.]202[.]188[.]155, 195[.]20[.]16[.]155

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

May 27, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com