Date of Publication
January 08, 2024

Hive Pro®

HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

01 to 07 JANUARY 2024

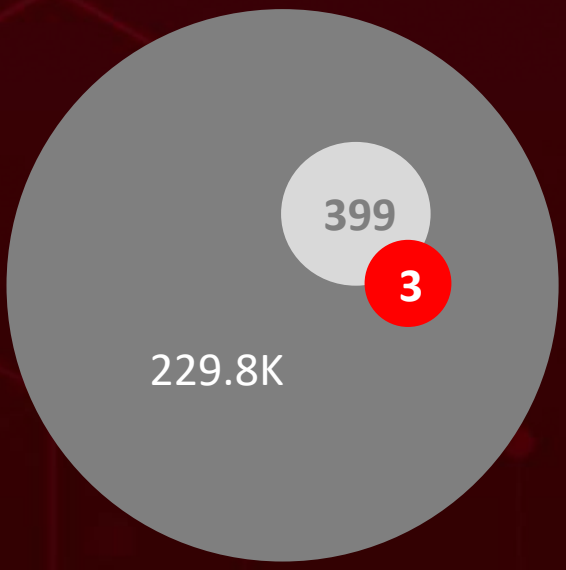
Table Of Contents

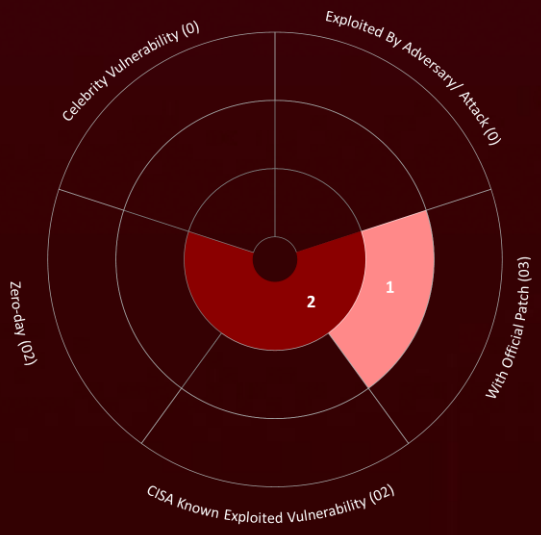
Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **twelve** executed attacks, **two** instances of adversary activity, and **three** exploited vulnerability, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered **APT28**, targeting Ukraine and Poland to deploy previously undocumented malware, OCEANMAP, MASEPIE, and STEELHOOK, to gather sensitive information.

Meanwhile, a high severity zero-day vulnerability (**CVE-2023-39336**), in Ivanti Endpoint Manager that posed a risk of pre-authenticated sql injection and possibly Remote Code Injection in case of core server. These observed attacks have been on the rise, posing a significant threat worldwide.





Total Vulnerabilities Published

Vulnerabilities Published in the Week

Exploited Vulnerabilities

High Level Statistics

12
Attacks Executed

3
Vulnerabilities Exploited

2
Adversaries in Action

- InfectedSlurs
- JenX Mirai
- OCEANMAP
- MASEPIE
- STEELHOOK
- Nim Backdoor
- Lumma
- Rhadamanthys
- Risepro
- Meduza
- Stealc Stealer
- Remcos RAT

- CVE-2023-49897
- CVE-2023-47565
- CVE-2023-39336

- APT28
- UAC-0050

Insights

CVE-2023-39336 a critical flaw in Ivanti Endpoint posed a significant risk, potentially allowing unauthenticated attackers to take control of devices

InfectedSlurs conducting a sophisticated campaign by exploiting two zero-day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices

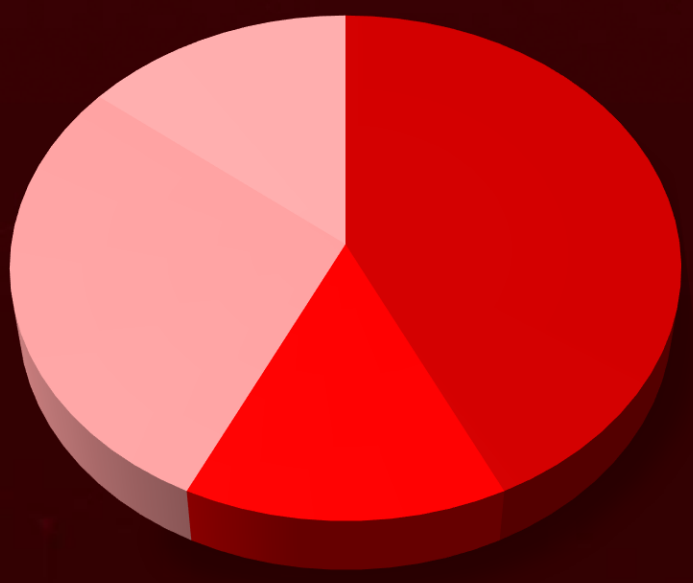
UAC-0050 targeting Ukraine, employing innovative strategies to spread Remcos RAT

APT28 identified targeting Ukrainian government entities and Polish organizations, with a goal to deploy previously undocumented malware, to gather sensitive information

Nim Backdoor Masquerades as Nepal Government Security, to trick victims into downloading and executing a backdoor program

Malicious JavaScript Used by threat actors to steal sensitive information

Threat Distribution



Targeted Countries

Countries
Ukraine
Nepal
Poland
Oman
Liechtenstein
State of Palestine
Angola
Mongolia
Antigua and Barbuda
Mexico
Argentina
Tuvalu
Armenia
Malta
Australia
Netherlands
Austria
Poland
Azerbaijan
Singapore
Bahamas
Thailand
Bahrain

Countries
Vanuatu
Bangladesh
Malawi
Italy
Mexico
Belarus
Myanmar
Belgium
Nigeria
India
Mexico
Russia
Algeria
Bhutan
Japan
Bolivia
South Sudan
Bosnia and Herzegovina
Switzerland
Botswana
Trinidad and Tobago
Brazil

Countries
Algeria
United Kingdom
Brunei
Zambia
Bulgaria
Luxembourg
Germany
Maldives
Burundi
Mauritania
Cabo Verde
Moldova
Cambodia
Morocco
United Arab Emirates
Nauru
Canada
South Africa
Central African Republic
North Macedonia
South Korea
Turkey
Chile
Peru

Countries
China
Qatar
Colombia
Saint Kitts & Nevis
Comoros
Sao Tome & Principe
Congo
Seychelles
Costa Rica
Andorra
Côte d'Ivoire
Sri Lanka
Croatia
United States
France
Tajikistan
Cyprus
Iran
Czech Republic (Czechia)
Turkey
Denmark
Albania
Djibouti

Targeted Industries

TOP MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1566
Phishing

T1588.006
Vulnerabilities

T1555
Credentials from Password Stores

T1659
Content Injection

T1036
Masquerading

T1588
Obtain Capabilities

T1203
Exploitation for Client Execution

T1204
User Execution

T1543
Create or Modify System Process

T1583
Acquire Infrastructure

T1059.007
JavaScript

T1105
Ingress Tool Transfer

T1537
Transfer Data to Cloud Account

T1140
Deobfuscate/Decode Files or Information

T1547.001
Registry Run Keys / Startup Folder

T1185
Browser Session Hijacking

T1567
Exfiltration Over Web Service

T1189
Drive-by Compromise

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
InfectedSlurs	InfectedSlurs is a new Mirai- based malware botnet, and is actively conducting a sophisticated campaign by exploiting two zero day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, facilitate the creation of a distributed denial-of-service (DDoS) botnet.	Exploiting vulnerabilities	CVE-2023-49897 CVE-2023-47565
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Launch DDoS attacks And Data Theft	QNAP VioStor NVR, FXC AE1021, AE1021PE
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.fxc.jp/form/certify/ , https://www.qnap.com/en/download

IOC TYPE	VALUE
SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JenX Mirai	The JenX Mirai variant, like many Mirai variants, prints a unique hard-coded string to the console when compromising a machine.	Exploiting vulnerabilities	CVE-2023-49897 CVE-2023-47565
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Launch DDoS attacks And Data Theft	QNAP VioStor NVR, FXC AE1021, AE1021PE
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.fxc.jp/form/certify/ , https://www.qnap.com/en/download

IOC TYPE	VALUE
SHA256	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1

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
OCEANMAP	OCEANMAP is a malicious program developed using the C# programming language. The main functionality consists in executing commands using cmd.exe. The IMAP protocol is used as a control channel.	distribution of e-mails	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		patching the backdoor executable and restarting the process	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-
IOC TYPE	**VALUE**		
SHA256	fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23, 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MASEPIE	MASEPIE is a malicious program developed using the Python programming language. The main functionality consists in uploading/unloading files and executing commands. The TCP protocol is used as a control channel. Data is encrypted using the AES-128-CBC algorithm	distribution of e-mails	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Upload or unload files, execute commands	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-
IOC TYPE	**VALUE**		
MD5	47f4b4d8f95a7e842691120c66309d5b		
SHA256	18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6		

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
STEELHOOK	STEELHOOK is a PowerShell script that provides the theft of Internet browser data ("Login Data", "Local State") and the DPAPI master key by sending them to the management server using an HTTP POST request in base64-encoded form.	distribution of e-mails	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Steal data	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
APT28			-

IOC TYPE	VALUE
SHA256	6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
MD5	5f126b2279648d849e622e4be910b96c

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nim Backdoor	Nim Backdoor is written in Nim programming language . A backdoor is a hidden way to access a system or application that is not intended for public use.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Spying on victims	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
MD5	e2a3edc708016316477228de885f0c39, 777fcc34fef4a16b2276e420c5fb3a73, EF834A7C726294CE8B0416826E659BAA, 32C5141B0704609B9404EFF6C18B47BF

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 Infostealer	Lumma is an information stealer, developed using the C programming language. It is offered for sale as a malware-as-a-service, with several plans available. It usually targets cryptocurrency wallets, login credentials, and other sensitive information on a compromised system.	Exploiting Google OAuth endpoint	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys	Rhadamanthys is a C++ information stealer that first emerged in August 2022, targeting email, FTP, and online banking service account credentials.	Exploiting Google OAuth endpoint	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2		

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
Risepro	RisePro is a stealer that is spread through downloaders like win.privateloader. Once executed on a system, the malware can steal credit card information, passwords, and personal data.	Exploiting Google OAuth endpoint	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	e8b221cba5c3598522f1ebd2b5e52b2f45699a1965b5dd677a9b9d074677873e, 356019c5f0ab89bcaff1639b2b2a427d7777fcfa13c09f889ef5ea8eb1c031c7, 5aa9cbeb84e41ab814e989920c76278d94827fb490f05d7421082570d1a1a3bb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Meduza	The Meduza Stealer malware has a singular objective: comprehensive data theft. It pilfers users' browsing activities, extracting a wide array of browser-related data.	Exploiting Google OAuth endpoint	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	eba71e82cb96780b4711bf898067ba81, 5c1e871a99108b68c90f6adbac5b190f, 3894a29e43d8847778f0fbb81bb479b9, 73070434952f46d1f37f9ab4bb99754f, eb52c4a4bef2367e721bbe13e89aacf5		

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
Stealc	Stealc is an information stealer sold as a Malware-as-a-Service since January 9, 2023. It is a non-resident stealer with flexible data collection settings and its development is relied on other prominent stealers. Stealc is written in C and uses WinAPI functions. It mainly targets date from web browsers, extensions and Desktop application of cryptocurrency wallets.	Exploiting Google OAuth endpoint	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	e6e1106fec7137b46da15bdd0853b1b9a6104bce649a24145793e4d451261c6b, d63a83fb534fd92df1de5373ce6fa7febf6ca715c7528a2a806de49da2889078		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes but has been used in numerous hacking campaigns. Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		remote surveillance and control	-
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0050			-
IOC TYPE	**VALUE**		
MD5	56154fedaa70a3e58b7262b7c344d30a, 9b777d69b018701ec5ad19ae3f06553f, 74865c6c290488bd5552aa905c02666c, 7c05cfed156f152139a6b1f0d48b5cc1, 7c05cfed156f152139a6b1f0d48b5cc1		

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-2023-49897	✗	FXC AE1021 & AE1021PE version 2.0.9 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fxc:ae1021_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:fxc:ae1021:-:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
FXC OS command injection vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://www.fxc.jp/form/certify/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47565	✗	QVR Firmware 4.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:qnap:qvr_firmware:*:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
QNAP VioStor OS command injection vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://www.qnap.com/en/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-39336	✕	Ivanti Endpoint Manager: Before 2022 SU5	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:ivanti_endpoint_manager:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager SQL injection Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter T1055: Process Injection	https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Energy, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	OCEANMAP, MASEPIE, and STEELHOOK	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1095: Non-Application Layer Protocol; T1567: Exfiltration Over Web Service; T1021: Remote Services; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1003: OS Credential Dumping; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.003: Mail Protocols; T1132: Data Encoding; T1132.001: Standard Encoding; T1572: Protocol Tunneling;

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UAC-0050	-	Government	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Remcos RAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1007: System Service Discovery; T1059.001: PowerShell; T1547: Boot or Logon Autostart Execution; T1216: System Script Proxy Execution; T1027: Obfuscated Files or Information; T1555: Credentials from Password Stores; T1547.001: Registry Run Keys / Startup Folder; T1041: Exfiltration Over C2 Channel; T1204: User Execution;

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerability** and block the indicators related to the threat actor **APT28, UAC-0050** and malware **InfectedSlurs, JenX Mirai, OCEANMAP, MASEPIE, STEELHOOK, Nim Backdoor, Remcos RAT.**

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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT28, UAC-0050** and malware **InfectedSlurs, JenX Mirai, OCEANMAP, MASEPIE, STEELHOOK, Nim Backdoor, Remcos RAT** 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 have been branded with catchy names and logos due to their profound and multifaceted impact.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
InfectedSlurs	SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380, f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1, a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26, cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87, 8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6, 35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a, 7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2, 29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff, cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9, a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1

Attack Name	TYPE	VALUE
JenX Mirai	SHA256	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1
OCEANMAP	MD5	6fdd416a768d04a1af1f28ecaa29191b, 5db75e816b4cef5cc457f0c9e3fc4100
	SHA256	fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23, 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04
	IP	74[.]124.219.71
	Domains	jrb@bahouholdings[.]com, qasim.m@facadesolutionsuae[.]com, webmail.facadesolutionsuae[.]com
MASEPIE	MD5	47f4b4d8f95a7e842691120c66309d5b
	SHA256	18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
STEELHOOK	SHA256	6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
	MD5	5f126b2279648d849e622e4be910b96c
Nim Backdoor	MD5	e2a3edc708016316477228de885f0c39, 777fcc34fef4a16b2276e420c5fb3a73, EF834A7C726294CE8B0416826E659BAA, 32C5141B0704609B9404EFF6C18B47BF
	SHA1	3aa803baf5027c57ec65eb9b47daad595ba80bac, 5D2E2336BB8F268606C9C8961BED03270150CF65, 4CAE7160386782C02A3B68E7A9BA78CC5FFB0236, 0599969CA8B35BB258797AEE45FBD9013E57C133
	Hostname	mail[.]mofa[.]govnp[.]org, nitc[.]govnp[.]org, mx1[.]nepal[.]govnp[.]org, dns[.]govnp[.]org
	SHA256	b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e, 696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83, 88FA16EC5420883A9C9E4F952634494D95F06F426E0A600A8114F69A6127347F, 1246356D78D47CE73E22CC253C47F739C4F766FF1E7B473D5E658BA1F0FDD662

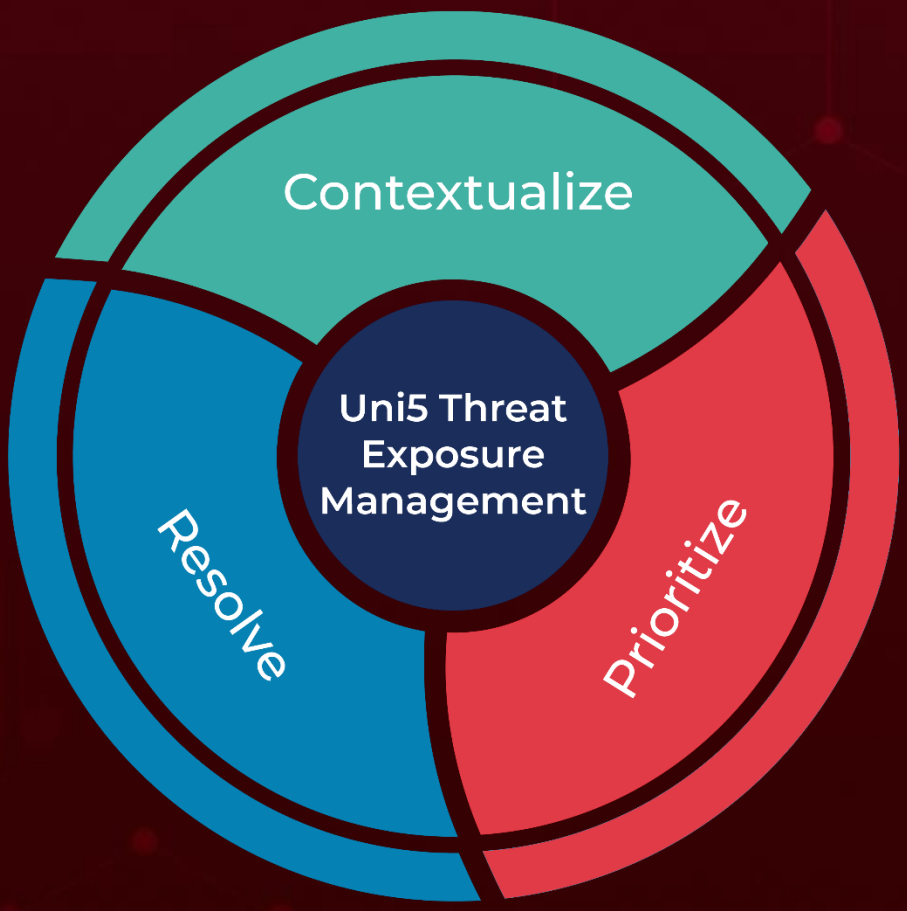
Attack Name	TYPE	VALUE
Lumma	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd
Rhadamanthys	SHA256	bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

Attack Name	TYPE	VALUE
Risepro	SHA256	e8b221cba5c3598522f1ebd2b5e52b2f45699a1965b5dd677a9b9d074677873e, 356019c5f0ab89bcaff1639b2b2a427d7777fcfa13c09f889ef5ea8eb1c031c7, 5aa9cbeb84e41ab814e989920c76278d94827fb490f05d7421082570d1a1a3bb
Meduza	MD5	eba71e82cb96780b4711bf898067ba81, 5c1e871a99108b68c90f6adbac5b190f, 3894a29e43d8847778f0fbb81bb479b9, 73070434952f46d1f37f9ab4bb99754f, eb52c4a4bef2367e721bbe13e89aacf5, adc35bb330618a365685b5864e403007, 02fa600eb8a92d7ce676f87269365ca0, 021b649ce9d11e2ca9c67761953b1408, c1824076854acac6858177062c1f5493, 80136b6c96f8b23f8e938e38e01c58e6, c712a1b8a70fb7d0c7a714e12eff0e38
Stealc	SHA256	e6e1106fec7137b46da15bdd0853b1b9a6104bce649a24145793e4d451261c6b, d63a83fb534fd92df1de5373ce6fa7febf6ca715c7528a2a806de49da2889078
Remcos	MD5	56154fedaa70a3e58b7262b7c344d30a, 9b777d69b018701ec5ad19ae3f06553f, 74865c6c290488bd5552aa905c02666c, 7c05cfed156f152139a6b1f0d48b5cc1, 7c05cfed156f152139a6b1f0d48b5cc1, 0b2d0eb5af93a3355244e1319e3de9da, 7f87d36c989a11edf0de9af392891d89, f5ee6aa31c950dfe55972e50e02201d3, 5c734bb1e41fab9c7b2dabd06e27bc7b, 1c3e1e0319dc6aa24166d5e2aaaec675, 818beece85ecd90d413782dd51d939b1, 8158b43f745e0e7a519458b0150e1b61, f71ef85824f906856cb3d2205058bdd2, 8bebea01d914a3c3a2d876417f7d1d54, b1f8484ee01a7730938210ea6e851888

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

January 08, 2023 . 5:30 AM

More at www.hivepro.com