

Date of Publication
August 26, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

19 to 25 AUGUST 2024

Table Of Contents

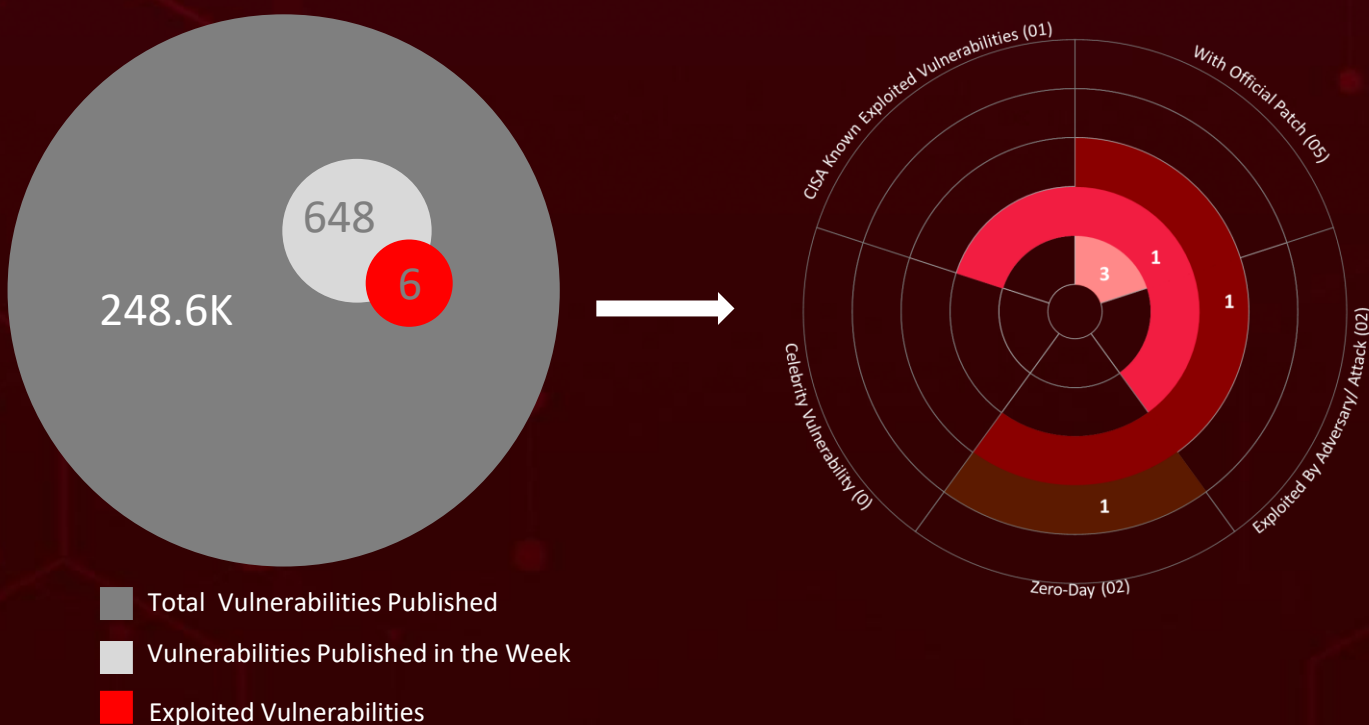
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	22

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **six** attacks were executed, **six** vulnerabilities were uncovered, and **one** active adversary was identified, underscoring the persistent danger of cyberattacks.

HiveForce Labs has also identified a state-sponsored North Korean cyber threat actor known as **UAT-5394**, which may be a separate group or a sub-division of the well-known Kimsuky APT group. This group is actively developing and using a new variant of the XenorAT malware, dubbed **MoonPeak**.

Additionally, a zero-day vulnerability in Chrome's V8 JavaScript engine, identified as **CVE-2024-7971**, has been discovered. This flaw can lead to remote code execution through type confusion and is currently being actively exploited. In a recent cyberattack targeting a university in Taiwan, the **Msupedge Backdoor** was deployed. This advanced malware is known for using DNS traffic to communicate with its command-and-control (C&C) server. The attack likely exploited a critical PHP vulnerability, enabling remote code execution. These escalating threats pose a significant and immediate risk to users globally.



High Level Statistics

6

Attacks
Executed

6

Vulnerabilities
Exploited

1

Adversaries in
Action

- [BANSHEE Stealer](#)
- [Mad Liberator Ransomware](#)
- [UULoader](#)
- [Gh0st RAT](#)
- [Msupedge Backdoor](#)
- [MoonPeak](#)

- [CVE-2024-5932](#)
- [CVE-2024-4577](#)
- [CVE-2024-28000](#)
- [CVE-2024-7971](#)
- [CVE-2024-28987](#)
- [CVE-2024-41992](#)

- [UAT-5394](#)



Insights

UAT-5394

North Korean cyber threat actor, deploying new XenorAT malware variant, known as MoonPeak

CVE-2024-5932

a critical vulnerability in the GiveWP plugin for WordPress, exposes 100,000+ sites to RCE & file deletion

CVE-2024-

28000 flaw in the LiteSpeed Cache WordPress plugin, affects over 5 million+ websites

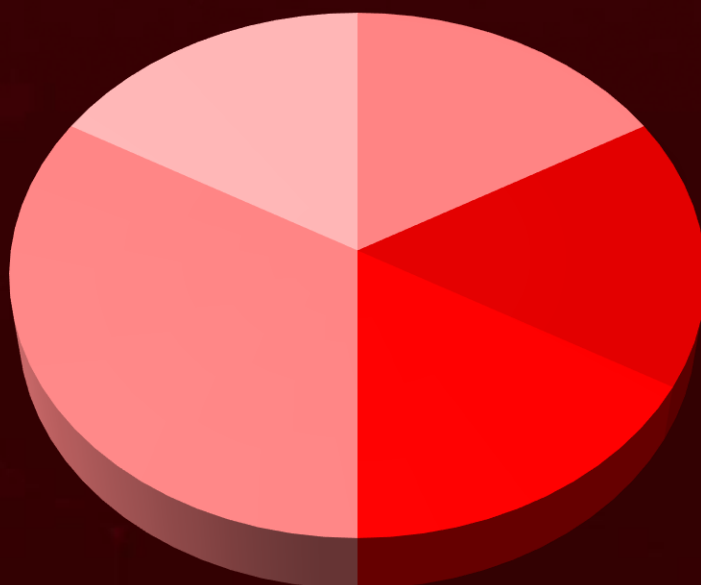
Msupedge is a novel backdoor which utilizes DNS tunneling to maintain covert communication with its C&C server, making it difficult to detect and block

BANSHEE Stealer a new macOS malware targets crucial system information, browser data, and cryptocurrency wallets

CVE-2024-7971

Zero-day vulnerability in Chrome's V8 JavaScript engine, leading to RCE

Threat Distribution



■ Stealer ■ Ransomware ■ Loader ■ RAT ■ Backdoor

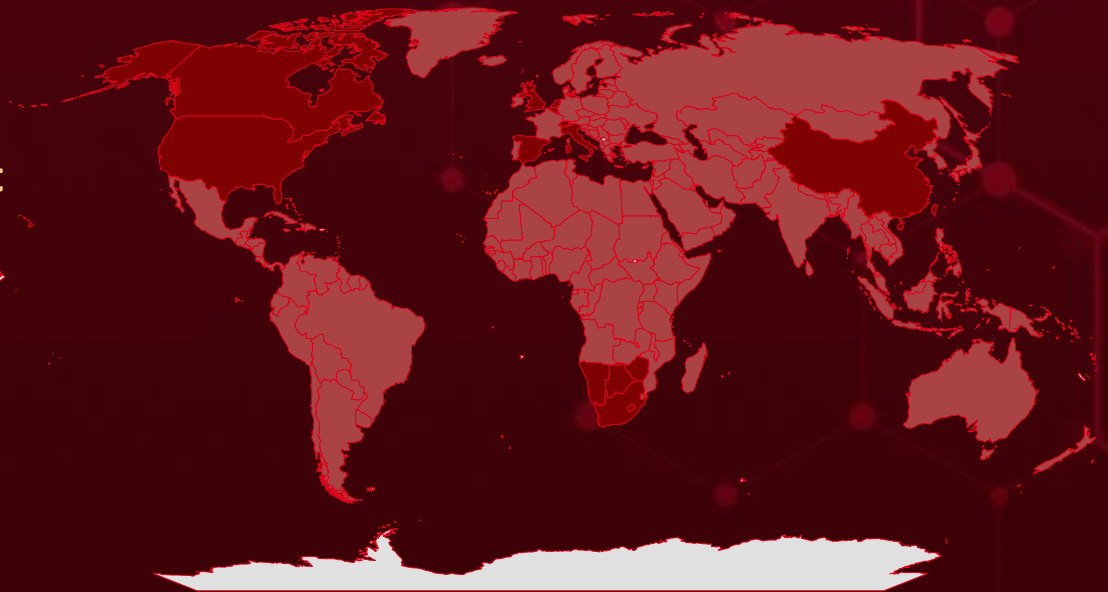


Targeted Countries

Most



Least



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

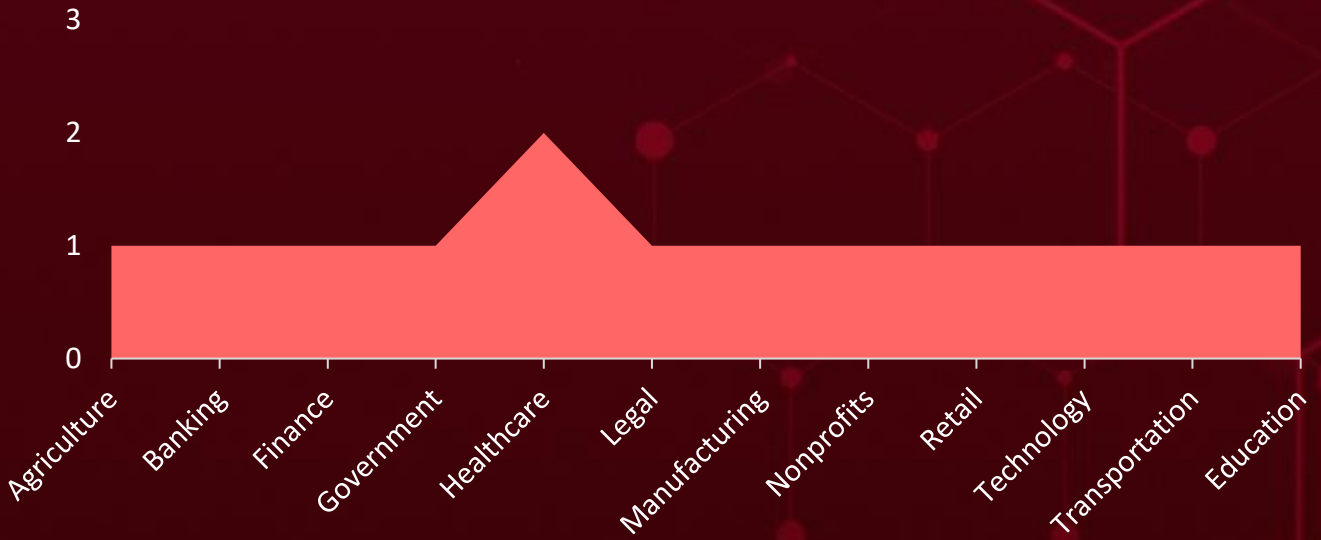
Countries
Namibia
Switzerland
South Africa
Belgium
United States
Botswana
Netherlands
Canada
Spain
China
United Kingdom
Italy
Zimbabwe
Lesotho
Portugal
Marshall Islands
Syria
Belarus
New Zealand
Albania
Singapore
Belize

Countries
Bangladesh
Benin
Montenegro
Bhutan
Pakistan
Bolivia
Samoa
Bosnia and Herzegovina
Azerbaijan
Algeria
Tunisia
Brazil
Malaysia
Brunei
Micronesia
Bulgaria
Armenia
Burkina Faso
North Korea
Burundi
Paraguay
Cabo Verde
Russia

Countries
Cambodia
Senegal
Cameroon
Somalia
Andorra
Sudan
Central African Republic
Timor-Leste
Chad
Uganda
Chile
Venezuela
Angola
Mali
Colombia
Mauritius
Comoros
Monaco
Congo
Mozambique
Costa Rica
Nepal

Countries
Qatar
Hungary
Romania
Iceland
Rwanda
India
Saint Lucia
Indonesia
San Marino
Iran
Saudi Arabia
Iraq
Serbia
Ireland
Sierra Leone
Israel
Slovakia
Antigua and Barbuda
Solomon Islands
Jamaica
Austria
Japan

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1082

System Information Discovery

T1203

Exploitation for Client Execution

T1588.005

Exploits

T1046

Network Service Discovery

T1068

Exploitation for Privilege Escalation

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1204

User Execution

T1036

Masquerading

T1005

Data from Local System

T1543

Create or Modify System Process

T1027

Obfuscated Files or Information

T1033

System Owner/User Discovery

T1083

File and Directory Discovery

T1592

Gather Victim Host Information

T1105

Ingress Tool Transfer

T1574

Hijack Execution Flow

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BANSHEE Stealer</u>	<p>BANSHEE Stealer, a macOS-based malware. Priced at \$3,000 per month, its cost is significantly higher compared to many Windows-based stealers.</p> <p>BANSHEE Stealer is designed to target a wide array of browsers, cryptocurrency wallets, and around 100 different browser extensions. This stealer can collect extensive which can lead to significant data breaches and financial losses for affected users. One of the unique technical aspects of BANSHEE Stealer is its use of AppleScripts to perform malicious actions.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			macOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	11aa6eeca2547fcf807129787bec0d576de1a29b56945c5a8fb16ed8bf68f782		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mad Liberator Ransomware</u>	<p>Mad Liberator is a ransomware group targeting AnyDesk users by displaying a fraudulent Microsoft Windows update screen to divert attention while it extracts data. Notably, Mad Liberator does not employ data encryption during the post-exfiltration process.</p>	Fake Microsoft Windows update screen	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	f4b9207ab2ea98774819892f11b412cb63f4e7fb4008ca9f9a59abc2440056fe		

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>UULoader</u>	UULoader is a new malware strain that primarily serves as a delivery mechanism for various malicious payloads, including RATs like Gh0stRat and hacking tools such as Mimikatz. One of the distinguishing features of UULoader is its primary method of evading static detection by security software: file header stripping.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			
ASSOCIATED ACTOR		Deploys another malware	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	5c698ede5260b1eb170c375015273324b86bae82722d85d2f013b22ae52d0c, 240999322f426e0e3d4921e691e10afe20f0b7383038f57f39840c14a5cdf92c, E8d2a953c4423dc1836165d3cb734418f5276aa5ed46297d03bf01dbc78c8e70		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Gh0st RAT</u>	Gh0stRat is a well-known RAT used by multiple threat actors and is often associated with cyber espionage and data exfiltration activities. This RAT provides attackers with extensive capabilities to control and monitor infected systems, making it a powerful tool for malicious activities.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		System Compromise	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	311198eeb76c5cb081151452a73159c194300121515e3fd875429152ae7761aa, 0dbd951b6a7b43300cf161aa7df612560c38a92743c47b71b034aec4f54c51c7		

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>Msupedge Backdoor</u>	<p>Msupedge is a backdoor malware that exists in the form of a dynamic link library (DLL). This backdoor is strategically installed in specific file paths on the victim's system, allowing it to persist and evade detection. Msupedge's use of DNS tunneling for C&C communication and its deployment as a DLL make it a stealthy and resilient threat.</p>	Exploiting Vulnerabilities	CVE-2024-4577
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		System Compromise	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	e08dc1c3987d17451a3e86c04ed322a9424582e2f2cb6352c892b7e0645eda43, f5937d38353ed431dc8a5eb32c119ab575114a10c24567f0c864cb2ef47f9f36		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>MoonPeak</u>	<p>A new remote access trojan (RAT) family, named MoonPeak, has emerged as a variant of the well-known XenoRAT. MoonPeak has been actively developed by a state-sponsored group of threat actors linked to North Korea. This malware variant retains much of the functionality of its predecessor, XenoRAT, which has been widely used in various cyber attacks for its capabilities in keylogging, command execution, and file manipulation.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Data Exfiltration	PATCH LINK
UAT-5394			
IOC TYPE	VALUE		
SHA256	0b8897103135d92b89a83093f00d1da845a1eae63da7b57f638bab48a779808e, 2b35ef3080dcc13e2d907f681443f3c3eda832ae66b0458ca5c97050f849306		




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
<u>CVE-2024-5932</u>		WordPress GiveWP plugin versions prior to 3.14.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:givewp_plugin:givewp_plugin:*.~*.~*.~*.~*.~*	-
WordPress GiveWP Plugin Remote Code Execution Vulnerability			
	CWE ID		
	CWE-502	T1059: Command and Scripting Interpreter T1485: Data Destruction	https://wordpress.org/plugins/give/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4577</u>		PHP version: 5 -8.3.7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*.~*.~*.~*.~*.~*	Msupedge Backdoor
PHP-CGI Argument Injection Vulnerability			
	CWE ID		
	CWE-78	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://www.php.net/downloads


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-28000</u>		WordPress LiteSpeed Cache Versions from 1.9 through 6.3.0.1.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:litespeed:cache_plugin:*.:*:*:*:*:*	-
WordPress LiteSpeed Cache Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-266	T1068: Exploitation for Privilege Escalation T1136: Create Account	https://wordpress.org/plugins/litespeed-cache/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-7971</u>		Google Chrome V8 prior to 128.0.6613.84	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*.:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1189: Drive-by Compromise T1204: User execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28987		WHD 12.8.3 HF1 and all previous versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:solarwinds:web_help_desk:12.8.3_hotfix_1:*:*:*:*:*:*	-
SolarWinds Web Help Desk Hardcoded Credential Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1190: Exploit Public-Facing Application T0891: Hardcoded Credentials	https://support.solarwinds.com/SuccessCenter/s/article/SolarWinds-Web-Help-Desk-12-8-3-Hotfix-2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41992		Arcadyan FMIMG51AX000J DUT-Wi-FiTestSuite-9.0.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:o:arcadyan:fmimg5ax000j_firmware:*:*:*:*:*:*	-
Arcadyan Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter T1203: Exploitation for Client Execution	-

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>UAT-5394</u>	North Korea	All	Worldwide
	MOTIVE Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	MoonPeak	-
	TTPs		
TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1082: System Information Discovery; T1071: Application Layer Protocol; T1008: Fallback Channels; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1046: Network Service Discovery; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1574: Hijack Execution Flow; T1010: Application Window Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery			

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 **UAT-5394** and malware **BANSHEE Stealer, Mad Liberator Ransomware, UUloader, Gh0st RAT, Msupedge Backdoor, MoonPeak**.

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 **UAT-5394** and malware **BANSHEE Stealer, UUloader, Msupedge Backdoor, MoonPeak, Gh0st RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[New Banshee Stealer Threatens macOS Systems, Stealing Sensitive Data](#)

[Mad Liberator Uses AnyDesk to Pull Off Data Heists](#)

[UULoader Malware Emerges: Targeting Users with Advanced Evasion Tactics](#)

[Leaked Environment Variables Fuel Cloud Data Extortion](#)

[Critical WordPress GiveWP Flaw Exposes 100,000+ Sites to RCE & File Deletion](#)

[Msupedge Backdoor Haunts Taiwan Institution](#)

[LiteSpeed Cache Plugin Vulnerability Affects Over 5 Million Websites](#)

[CVE-2024-7971: Google Chrome's Zero-Day Flaw Exploited in the Wild](#)

[SolarWinds WHD Flaw Lets Attackers Infiltrate Systems with Hardcoded Credentials](#)

[CVE-2024-41992: Unpatched Zero-Day RCE Flaw Found in Arcadyan Routers](#)

[North Korean Hackers Roll Out Their New MoonPeak RAT](#)

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>BANSHEE Stealer</u>	SHA256	11aa6eeca2547fcf807129787bec0d576de1a29b56945c5a8fb16ed8bf68f782
	IPv4	45[.]142[.]122[.]92
<u>Mad Liberator Ransomware</u>	SHA256	f4b9207ab2ea98774819892f11b412cb63f4e7fb4008ca9f9a59abc2440056fe
	File Name	readme.txt, restore_files.txt
	TOR Address	k67ivvik3dikqi4gy4ua7xa6idijl4si7k5ad5lotbaeirfcsx4sgbid[.]onion
	Email	mad[.]liberator[@]onionmail[.]org
<u>UULoader</u>	SHA256	5c698edeba5260b1eb170c375015273324b86bae82722d85d2f013b22ae52d0c, 240999322f426e0e3d4921e691e10afe20f0b7383038f57f39840c14a5cdf92c, e8d2a953c4423dc1836165d3cb734418f5276aa5ed46297d03bf01dbc78c8e70, 4b25b4306cf8da05456484178e8e935d9f9a66f2e385b080e36cd652ab6880bc, bb64e8f94742afec20156e75915070f6c23ca13021a80c4637f92c2760009d72, 4dfa9e07224c1d7ef6a6ffae2027b1df2f08c4ed2910d872ca248785bb35dad8, dc8925a926456878860c37ed01a996de4f858f33ac18cfcf9b29a997d7e38e5c, cd09451ba2d5ff87387087f75ad2fd4943c2c83b9ff6f87a2b8910e39bc3459b,

Attack Name	TYPE	VALUE
<u>UULoader</u>	SHA256	<p>0df0ff0ce0162b4498ad6a25b6e536cffb119316262cf89e4ccf77535ebc13a5, 7846c4aa9d6bc5a1d12fd1b885c28809203c5df4920df31220b7140ea206b7be, c675f276611ef53f8b74b8eb7b33590de19b07fc4b3b6d846ebca6f63a056ff7, c729bd033e705a2fddd3591c1e52a48932aeef628f6f63f460e56bfff9c3ab, 092ca5a50a0bf1d8f7b4e38fd80474f31f1d4eb8036ac13e101421b5df1687db, 0821a3f021856adf31bb07531030e922cbd33483402547daf3d1b98d5c4c1a57, ca543ff1fe2963a8daf5042b29c86e3d4abc0eb1365feb3ca53d006abc48f0cc, 598042a211e7c25ce34390851d344f084d3c625c478945c3bf4501ed65a18097, 81c25e14af8c4ca37b6fb7ed0d8122a6a5d3054943af89e839bffff907fe128f, d5a429457405c018e2536e3750044d93bf547f4dfa397a6d9b7dc9a691cfcddd, 45e1ad56a97a92633f41d873fd8cb6b6da8e0e8e4ef094ba433d1c90ea195874, 48df25302ef5df40e692acac546ed3713e28a0c02f563b98e65cbb28d9f1b675, b172b565dc16b29af83689cf6a26f62372e33f2640109a4ddb15d89f6bfff3e6d, 79aaa25a384729b3a6f04091459e09f9c5935cba7d27182ff6794337413886b8, 359fab75c195ebec1fea4237aa011092f4080d82236652f2be1252275ed7b4f, 267abb405b8010dda2546d0ac1e59d2e83a23754fc8af68a866335dd76422781, 4a4efcf4c80c5ec4f6479549097e04c272d640664b4f8d0768f159f9f295f24a, 69605f9958127a28e8448077ff9610c2da584a7528485c14046e6f4e13fe0f90, 165a1ef58ee6f29291685d98863f82d1875d78b16d0a1207b34a7719b2b4d43a, 63c07d1feb2402e92d57b637497372e8e8e2ef88419f482465c549dd0b90fe13, 5b5e8f9d1e317fd0963be2b5b46ca7a4710c5fec145a5a8bcb7eec1ff519a842, 591a2fb480864f0c793d055dee3d948e3cb150fc56df0644bb424bf912557440,</p>

Attack Name	TYPE	VALUE
<u>UUloader</u>	SHA256	b3e0aaf9a5c37408fca964220c9d294e4842a2901feaa373f056c191b8c6896d, e5459a53509b40edc3c6019cf0f7b0d05e14cd1a0641824e1cfecfe952a33f64, 972f9dc83a69fa5297e4d0e05113b6fab86bcefb0b3af913f7349bfe0e79fc87, eabd8606040bda54ad02062091e9af1840f557c61cb736f1c2f3d68a678f2798, fd0c66d3899702138f893f919f21b6d155a53a93a2181eaf4b602030c7adf5c7, 63b065324ea96ec5785c4d18c78ccc2e7d071a8e2f92a06835e2366567bbf31d, 3761a7ac0427692e4194d0a988b0d7985d7a909de69c3fc0ce028eb76a1297f9, f144be0bd8d377de067e4cdf5256a33f8ba03c8f0b15afb2593fa258b71a4005, ea193e1c13a142ed7d9f499a814d9480441f18c75e0617de8fdcc8443f7d1eae, b562b190f6c3174943993f0da38133d4b4b20f80ac8d11f0757d45e1ad462154, 5d3c87c115092f7c3da9a9144c1b594b0229830b258cbc27fe20841f38b78ca9, 962d1fd45f1e164ec54c2f62eb71acacbd70c425bae8dfce0e8d5612baedef75, 742e6e4db5056b45254125f809ec158fdb5303c6c378fc1a23c599965a4aaa67, eaff614d9223fe13ebe45c04eacf31acf970e0aedbe1811bab32e55718395625, 596ffd75ab3512cba1e7328d902460b55401c094ddb67fe9f98263c06d10b517, 796466e5146bb76e9e81ca32014842b355d7df96d6c6bab0dcf02e6a8f9be11e
<u>Gh0st RAT</u>	SHA256	311198eeb76c5cb081151452a73159c194300121515e3fd875429152ae7761aa, 0dbd951b6a7b43300cf161aa7df612560c38a92743c47b71b034aec4f54c51c7, 30af33cc275298269f2f8bb65529f0861090d49984d2200fa21812bdd558174a, f07465ea271cedaffa98eb8fe5160e9f50c71b326826cf32c6ce618955bc18bb, acb615b72532d8020f1fa9afa65c44bd67caa1ec83f39f4b029287e70c344d0b, 122f13cfff3a8747c05829fa21c72dbda254412d88e43625906915f1b9ef4cb,

Attack Name	TYPE	VALUE
<u>Gh0st RAT</u>	SHA256	0f72e9eb5201b984d8926887694111ed09f28c87261df7aab663f5dc493e215f, d3e842a19d952d896bf00b7c9ae1cbdd9ca4813940f709f77abf3e45f6695951, 81cb227b1d2a8bddeaab023fb7093940c8b8bd8907f625d52ce0dc2ab95ba5eb, 6098e5ccff15e8e03affd9ebb17d9731f87748bddda3ba4e411d3775e5ae45ed, f6e15f90b07e9d9bf2abb87722bf26616dd0df4ce68367591b61ef18ae5fb55a, 50af61f3f54cf5820debfe709a7a464bdf604bbe02dd420b07e02903a2f5ce6b, f31a39cbedd024d5b24f3cb622b9d66039771c5cf90e261197d10d05e113b79a, 660d751e714e0113ed7aa8a65adc005fc6d525355bc7025cef51fcf2ad229190, 6da0526678cf24ec66d855156fb2e7d3002997449196769f67119e6335fc83db, 4027995b0a77793ccb5b415d66ba3b6ea1dfdbdc70249ab2f7f66a35f97a80d3, 64aa5070c73e39d9368213964d16226c5f5167bb1e5deee1feddab1d725b7e44, f8bd914389a739b00043dba62b8976f31907fe05f243106c8009aeea6c8fd31a, 3e5f69ea887923030a3e789c33920a63a7727a2adb154b3497f76cfc4112ad5, bcb9d9086fcf884565fde0d8b7f9ca3f945eb9b69f9b75660220ba798ca4eff5, 4b9af32cc911b66a2e31664bdc71566c67b04b10d1042d900d84e061d3b1a151, 6b8dbe3bb2ca13ab48641f4b9bb1aaa4970680e8bc5e8a70bf0af0f67422c3c1, bdf3720e09043bd3749e1195af8790037944e969e90ed0c15246f4cef68c3f09, ff5cef611bd3fc92d5e0979eac5b228ca6339dfa105a1f8e38a572a392e5ef31, 873df098203c98f2364321fa1295a8cb3542af83727b9dc335829f5ba0dc1c97, 252283a77c47a726452e660a27e434048a2020b8b7ff473164546d2f0d42d6db, 0e3285bd2185663e1edbe7f203f325254d0f759c1a413fa363aa53500d097804
<u>Msupedge Backdoor</u>	SHA256	e08dc1c3987d17451a3e86c04ed322a9424582e2f2cb6352c892b7e0645eda43, f5937d38353ed431dc8a5eb32c119ab575114a10c24567f0c864cb2ef47f9f36

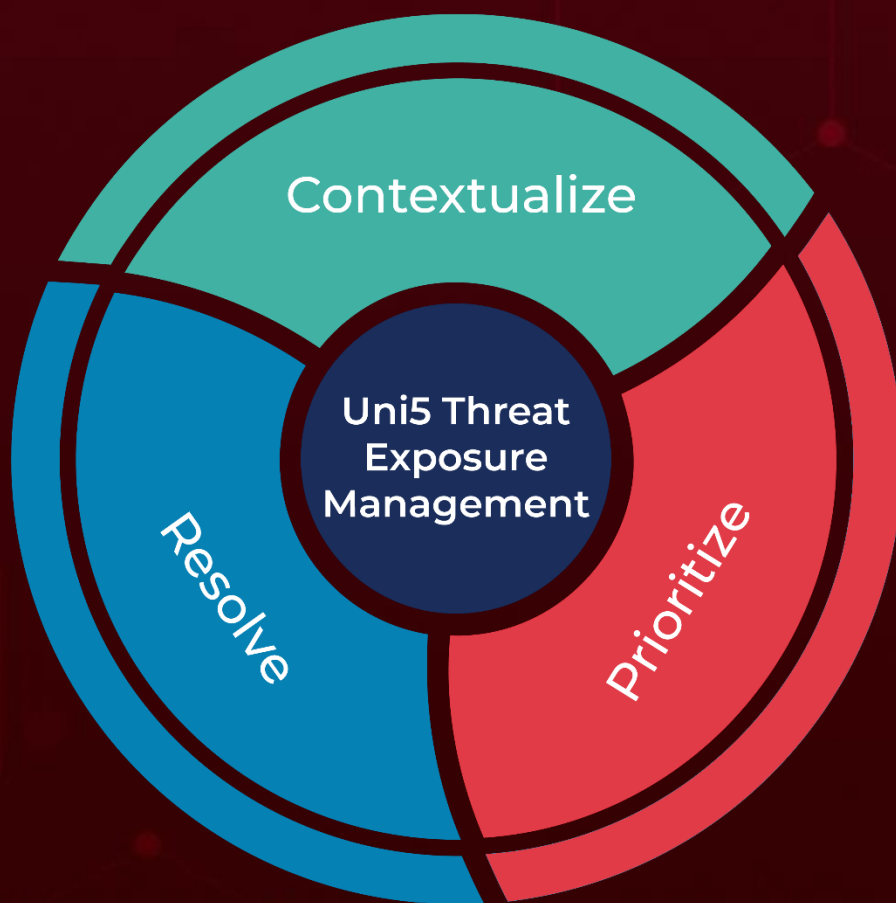
Attack Name	TYPE	VALUE
<u>MoonPeak</u>	SHA256	0b8897103135d92b89a83093f00d1da845a1eae63da7b57f638bab48a779808e, 2b35ef3080dcc13e2d907f681443f3c3eda832ae66b0458ca5c97050f849306, 4108c5096a62c0a6664eed781c39bb042eb0adf166fcc5d64d7c89139d525d4f, 44e492d5b9c48c1df7ef5e0fe9a732f271234219d8377cf909a431a386759555, 4599a9421e83fb0e2c005e5d9ac171305192beabe965f3385accaf2647be3e8e, 58fdc1b6ce4744d6331f8e2efc4652d754e803cae4cc16101fc78438184995e6, 97ba8d30cf8393c39f61f7e63266914ecafd07bd49911370afb866399446f37d, a80a35649f638049244a06dd4fb6eca4de0757ef566bfbe1affe1c8bfd96b04, b8233fe9e903ca08b9b1836fe6197e7d3e98e36b13815d8662de09832367a98a, f4aa4c6942a87087530494cba770a1dcbcb263514d874f12ba93a64b1edb2ae21c, facf3b40a2b99cc15eee7b7aee3b36a57f0951cda45931fcde311c0cc21cdc71, 0ed643a30a82daacecfec946031143b962f693104bcb7087ec6bda09ade0f3cb, 41d4f7734fbf14ebcdf63f51093718fd5a22ec38a297c0dc3d7704a3fb48b3f9, 6a3839788c0dafa591718a3fb6316d12ccd8e82dbcb41ce40e66b743f2dd344d, 148c69a7a1e06dc06e52db5c3f5895de6adc3d79498bc3ccc2cbd8fdf28b2070, 1ad43ddfce147c1ec71b37011d522c11999a974811fead11fee6761ceb920b10, 458641936e2b41c425161a9b892d2aa08d1de2bc0db446f214b5f87a6a506432, 8a4fbcdec5c08e6324e3142f8b8c41da5b8e714b9398c425c47189f17a51d07b, 293b1a7e923be0f554ec44c87c0981c9b5cf0f20c3ad89d767f366afb0c1f24a

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the 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

August 26, 2024 • 6:45 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com