

Date of Publication
June 12, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

05 to 11 JUNE 2023

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>	12
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	25

Summary

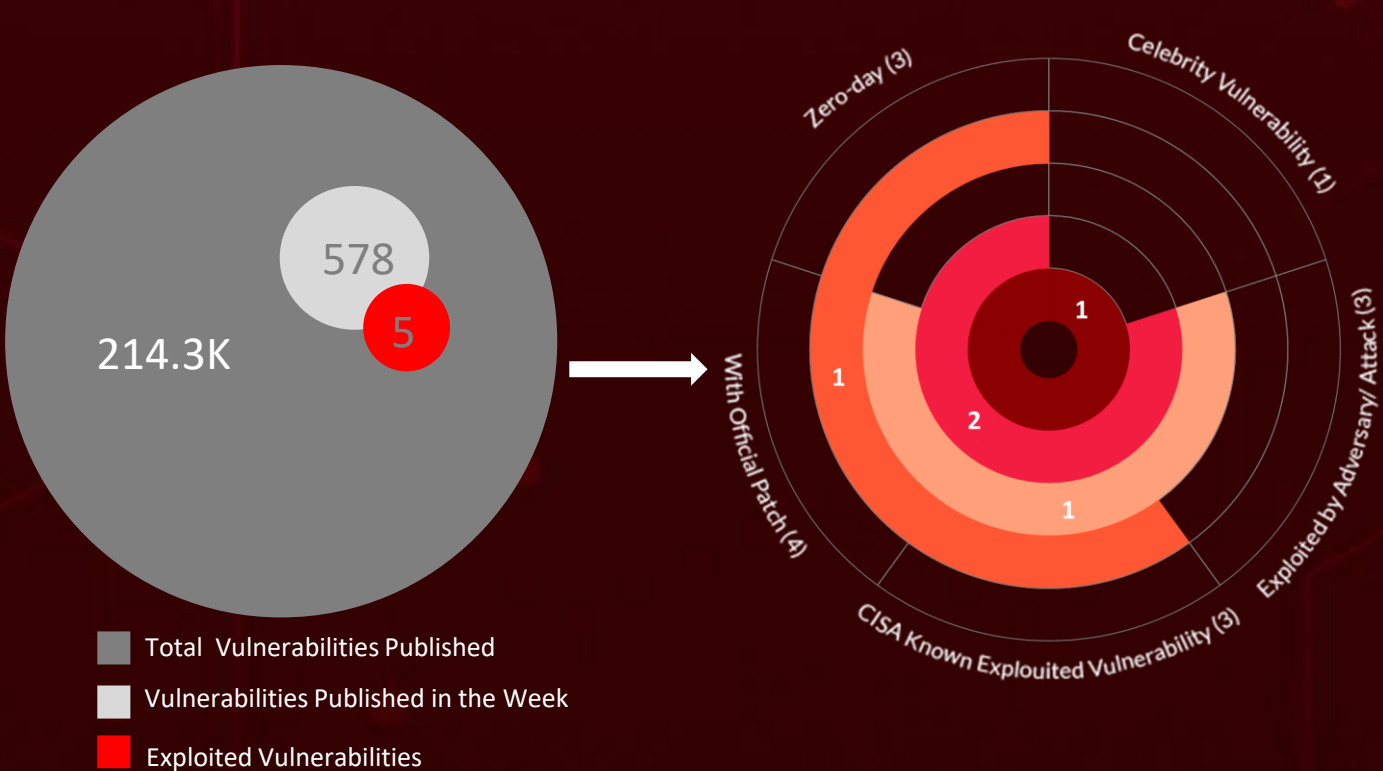
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **seven** attacks executed, taking advantage of **five** different vulnerabilities in various systems, and involving **two** different adversaries highlights the ever-present danger of cyber attacks.

Interestingly, all five vulnerabilities are part of the known exploited vulnerability catalog by CISA, out of which four are zero-day

Moreover, HiveForce Labs also found that **Asylum Ambuscade** threat group was exploiting a one-year-old Follina vulnerability ([CVE-2022-30190](#)).

Furthermore, a new malware software called **MediaArena** Browser Hijacker has been identified, which is being distributed through **malvertising** campaigns.

In addition to these threats, there is also a **zero-day** vulnerability ([CVE-2023-34362](#)) associated with Lace Tempest, TA505, and Clop ransomware that enables unauthorized access to the **MOVEit** Transfer database. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

7

Attacks
Executed

5

Vulnerabilities
Exploited

2

Adversaries in
Action

- Clop Ransomware
- MediaArena
- Satacom (aka LegionLoader)
- NODEBOT
- AHKBOT
- SunSeed
- Stealth Soldier
- CVE-2023-34362
- CVE-2021-40539
- CVE-2021-27860
- CVE-2022-30190
- CVE-2023-3079
- Volt Typhoon
- Asylum
- Ambuscade



Insights

Stealth

Soldier Targeting Government and Foreign Affairs in Libya

Volt Typhoon APT

Targeting critical infrastructure organizations in the United States as well as the U.S. island territory of Guam

One 0-day

Found in Google Chromium V8 Engine

VMware

Addressed three critical vulnerabilities in VMware Aria Operations Networks

Satacom Malware

Targeting cryptocurrency websites performing web injections

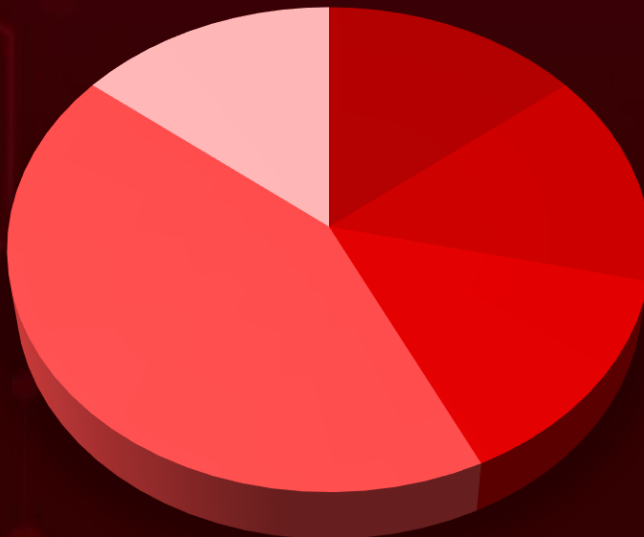
AHKBOT

Sophisticated and stealthy Trojan malware associated with Asylum Ambuscade group

MediaArena

A new Browser Hijacker software distributed through malvertising campaigns

Threat Distribution



■ Ransomware ■ Backdoor ■ Browser hijacker ■ Loader ■ Trojan



Targeted Countries

Most



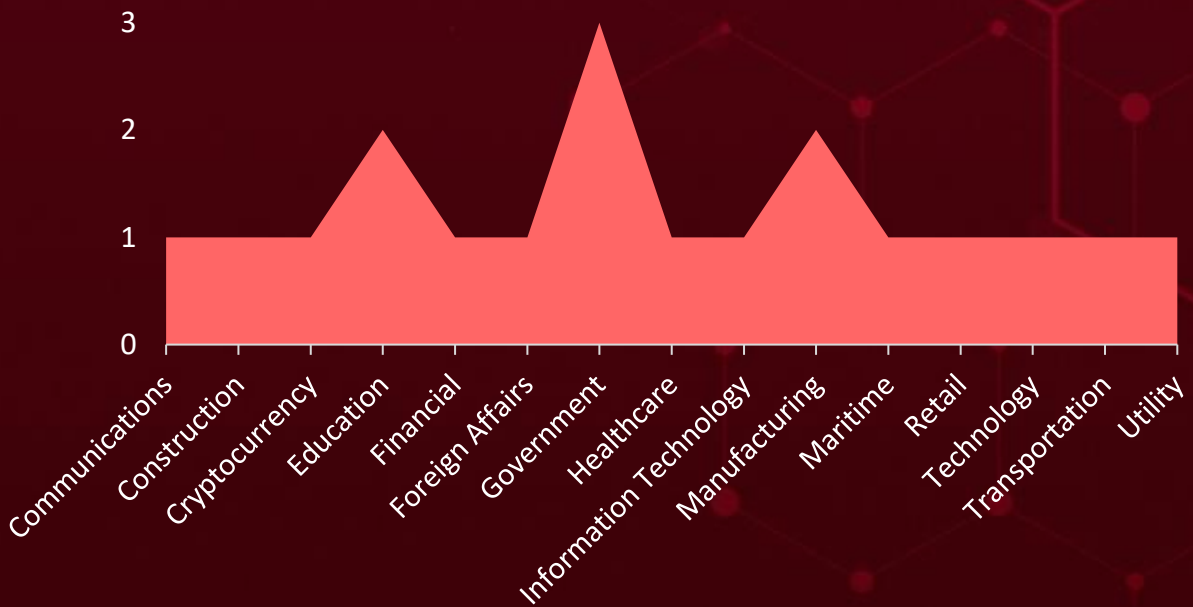
Least



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

Countries	Countries	Countries	Countries	Countries
Algeria	Bolivia	Marshall Islands	Sri Lanka	Australia
Egypt	Saudi Arabia	Colombia	Ecuador	Germany
Turkey	Bosnia and Herzegovina	Micronesia	Suriname	Myanmar
Mexico	State of Palestine	Comoros	Andorra	Ghana
Vietnam	Botswana	Montenegro	Tajikistan	Nauru
Morocco	Tuvalu	Congo	El Salvador	Greece
Brazil	Albania	Namibia	Togo	Netherlands
Sudan	Mali	Costa Rica	Equatorial Guinea	Grenada
Tunisia	Brunei	New Zealand	Bahamas	Nicaragua
India	Monaco	Côte d'Ivoire	Eritrea	Guatemala
United States	Bulgaria	North Korea	Ukraine	Nigeria
Indonesia	Nepal	Croatia	Estonia	Guinea
Mauritania	Burkina Faso	Pakistan	Uruguay	North Macedonia
Libya	Norway	Cuba	Eswatini	Guinea-Bissau
Romania	Burundi	Paraguay	Bangladesh	Oman
Mauritius	Philippines	Cyprus	Ethiopia	Guyana
Thailand	Cabo Verde	Portugal	Barbados	Palau
Belarus	Saint Lucia	Czech Republic (Czechia)	Fiji	Haiti
Niger	Cambodia	Rwanda	Malta	Papua New Guinea
Belgium	Sierra Leone	Denmark	Finland	Holy See
Solomon Islands	Cameroon	San Marino	Argentina	Peru
Belize	South Sudan	Djibouti	France	Honduras
Vanuatu	Canada	Serbia	Armenia	Poland
Benin	Switzerland	Dominica	Gabon	Hungary
Mozambique	Central African Republic	Slovakia	Moldova	Qatar
Bhutan	Trinidad and Tobago	Dominican Republic	Gambia	Iceland
Panama	Chad	South Africa	Mongolia	Russia
Zambia	United Kingdom	DR Congo	Georgia	Angola
China		Sri Lanka	Australia	Saint Kitts & Nevis

Targeted Industries



TOP MITRE ATT&CK TTPS

T1588

Obtain Capabilities

T1190

Exploit Public-Facing Application

T1059

Command and Scripting Interpreter

T1068

Exploitation for Privilege Escalation

T1021

Remote Services

T1027

Obfuscated Files or Information

T1566

Phishing

T1056

Input Capture

T1041

Exfiltration Over C2 Channel

T1569

System Services

T1036

Masquerading

T1055

Process Injection

T1078

Valid Accounts

T1057

Process Discovery

T1071

Application Layer Protocol

T1564

Hide Artifacts

T1518

Software Discovery

T1095

Non-Application Layer Protocol

T1505

Server Software Component

T1083

File and Directory Discovery

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clop	<p>Clop ransomware recently has been associated with a zero-day vulnerability in the MOVEit Transfer software, allowing unauthorized access to its database. This combination poses an increased threat to organizations, leading to potential data breaches and financial losses.</p>	Phishing emails	CVE-2023-34362
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Progress MOVEit Transfer
ASSOCIATED ACTOR			PATCH LINK
TA505			https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
IOC TYPE	VALUE		
Email Address	unlock@rsv-box[.]com unlock@rsv-box[.]com		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MediaArena	<p>MediaArena is a deceptive software that hijacks browsers, redirects searches, and collects user data for malicious activities, emphasizing the importance of removal and caution.</p>	Malvertising campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Browser hijacker			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6 cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630 e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260 6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e		

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>NODEBOT</u>	NODEBOT is a Node.js-based variant of AHKBOT, enabling functions like screenshot capture, password theft, and downloading of malicious plugins.	Spear-phishing emails	CVE-2022-30190	
TYPE		IMPACT	AFFECTED PRODUCTS	
Loader				Microsoft Windows
ASSOCIATED ACTOR				PATCH LINK
Asylum Ambuscade		Data Theft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	
IOC TYPE	VALUE			
SHA1	C98061592DE61E34DA280AB179465580947890DE			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>AHKBOT</u>	AHKBOT is a malware tool and it is capable of capturing screenshots, stealing passwords, and fetching additional plugins to carry out various malicious activities on compromised systems.	Spear-phishing emails	CVE-2022-30190	
TYPE		IMPACT	AFFECTED PRODUCTS	
Banking Trojan				Microsoft Windows
ASSOCIATED ACTOR				PATCH LINK
Asylum Ambuscade		Data Theft	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190	
IOC TYPE	VALUE			
SHA1	AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B64F5AC9F0C6C12F2A48A1CB941847B0662734FBF557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF85B82805C6204F34DB0858E2F04DA9F620A02775492061DE582E71B2A5DA046536D4150F6F497F1			

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>SunSeed</u>	SunSeed malware is a dangerous threat delivered via malicious email attachments, enabling attackers to download and execute additional payloads, posing a significant risk to compromised systems and data.	Spear-phishing emails	CVE-2022-30190
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			
ASSOCIATED ACTOR			
Asylum Ambuscade		System compromise, data loss, and unauthorized access	Microsoft Windows
		PATCH LINK	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	VALUE		
IPV4	146[.]70[.]79[.]119		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Stealth Soldier</u>	Stealth Soldier is a Custom backdoor used in targeted espionage attacks in Libya, enabling surveillance with file exfiltration, screen recording, keystroke logging, and browser data theft.	Unkown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR			
-		Data theft	PATCH LINK
IOC TYPE	VALUE		
SHA256	2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9cb9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110ed57fc4e8c14da6404bdc4e0e6ac79104386ffbd469351c2a720a53a52a677db e7794fac887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f		




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>Satacom (aka LegionLoader)</u>	Satacom is a notorious malware that uses DNS queries to retrieve encoded URLs, delivering additional malware through malicious ads and links on third-party websites.	Malicious ads or links	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data theft, system instability, unauthorized access, and financial loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
Domain	dns-beast[.]com		
MD5	0ac34b67e634e49b0f75cf2be388f244 1aa7ad7efb1b48a28c6ccf7b496c9cfd 199017082159b23decdf63b22e07a7a1 a7f17ed79777f28bf9c9cebaa01c8d70		




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-2023-34362</u>		MOVEit Transfer 2023.0.0(15.0),MOVEit Transfer 2022.1.x(14.1),MOVEit Transfer 2022.0.x(14.0),MOVEit Transfer 2021.1.x(13.1),MOVEit Transfer 2021.0.x(13.0),MOVEit Transfer 2020.1.x(12.1),MOVEit Transfer 2020.0.x(12.0) or older,MOVEit Cloud	Lace Tempest (aka FIN11, DEV-0950), TA505 (Graceful Spider, Gold Evergreen, Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo, Spandex)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*	Clop Ransomware
Progress MOVEit Transfer SQL Injection Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID	T1190: Exploit Public-Facing Application	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
	CWE-89		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-40539</u>		Zoho ManageEngine	Volt Typhoon (aka BRONZE SILHOUETTE)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adservice_plus:4.5:4510.*:*:*:*:*	-
Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1203: Exploitation for Client Execution	https://www.manageengine.com/products/self-service-password/advisory/CVE-2021-40539.html


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-27860</u>		FatPipe WARP, IPVPN, and MPVPN software	Volt Typhoon (aka BRONZE SILHOUETTE)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:fatpipeinc:ipvpn_firmware:5.2.0:r34:*:*:*:*:*	-
FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1203: Exploitation for Client Execution	https://www.fatpipeinc.com/support/cve-list.php

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3079		Google Chrome: 100.0.4896.60 - 114.0.5735.91	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:google:google_chrome:-:*:*:*:*:*	-
Google Chrome Type Confusion Vulnerability			
	CWE ID	T1190: Exploit Public-Facing Application	https://www.google.com/intl/en/chrome/?standalone=1
	CWE-843		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	Follina	Microsoft Windows	Asylum Ambuscade
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*	NODEBOT, AHKBOT, SunSeed
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
	CWE-78		

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Volt Typhoon (aka BRONZE SILHOUETTE)</u>	China	Communications, Manufacturing, Utility, Transportation, Construction, Maritime, Government, Information Technology, and Education	United States and the U.S. island territory of Guam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2021-40539 CVE-2021-27860	-	Zoho ManageEngine, FatPipe WARP, IPVPN, and MPVPN software
TTPs			
T1003:OS CredentialDumping; T1003.001:LSASS Memory; T1003.003:NTDS; T1016:System Network Configuration Discovery; T1033:System Owner/User Discovery; T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1059.001:PowerShell; T1059.003:Windows Command Shell; T1069:Permission Groups Discovery; T1069.001:Local Groups; T1069.002:Domain Groups; T1070: Indicator Removal; T1070.001:Clear Windows Event Logs; T1082:System Information Discovery; T1090:Proxy; T1090.002:External Proxy; T1110:Brute Force; T1110.003:Password Spraying; T1190:Exploit Public-Facing Application; T1505:Server Software Component; T1505.003:Web Shell; T1555:Credentials from Password Stores			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p>Asylum Ambuscade</p>	Unknown	Government entities, Financial, Cryptocurrency, Small and Medium Businesses including healthcare, manufacturing, technology, retail, and education	North America, Europe, Asia, Africa, and South America
	MOTIVE		
	Financial crime and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
CVE-2022-30190	NODEBOT, AHKBOT, SunSeed	Microsoft Windows	
TTPs			
<p>T1583.003:Acquire Infrastructure: Virtual Private Server; T1587.001:Develop Capabilities: Malware; T1189:Drive-by Compromise; T1566.001:Phishing: Spearphishing Attachment; T1059.005:Command and Scripting Interpreter: Visual Basic; T1059.006:Command and Scripting Interpreter: Python; T1059.007:Command and Scripting Interpreter: JavaScript; T1059:Command and Scripting Interpreter; T1204.002:User Execution: Malicious File; T1547.001:Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1027.010:Obfuscated Files or Information: Command Obfuscation; T1555.003:Credentials from Password Stores: Credentials from Web Browsers; T1087.002:Account Discovery: Domain Account; T1010:Application Window Discovery; T1482:Domain Trust Discovery; T1057:Process Discovery; T1518.001:Software Discovery: Security Software Discovery; T1082:System Information Discovery; T1016:System Network Configuration Discovery; T1056.001:Input Capture: Keylogging; T1115:Clipboard Data; T1113:Screen Capture; T1071.001:Application Layer Protocol: Web Protocols; T1041:Exfiltration Over C2 Channel</p>			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **Volt Typhoon**, **Asylum Ambuscade** and malware **MediaArena**, **Satacom**, **NODEBOT**, **AHKBOT**, **SunSeed**, and **Stealth Soldier**

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 **five exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Volt Typhoon**, **Asylum Ambuscade** and malware **MediaArena**, **Satacom**, **NODEBOT**, **AHKBOT**, **SunSeed**, and **Stealth Soldier** in Breach and Attack Simulation(BAS).

Threat Advisories

[The Exploitation of Critical Zero-Day Vulnerability Found in MOVEit Transfer](#)

[Volt Typhoon Chinese Espionage Group Targets U.S. Government](#)

[MediaArena: A Deceptive Browser Hijacker Exploiting User Data and Security Threats](#)

[Google Addresses High-Stakes Chrome Zero-Day Vulnerability](#)

[Critical Vulnerabilities in VMware Aria Operations Addressed and Secured](#)

[Satacom Malware Campaign Unleashed Crypto-stealing Extension](#)

[Asylum Ambuscade Unmasking the Hybrid Threat Group in Cybersecurity](#)

[Stealth Soldier Strikes North Africa with Espionage 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 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
<u>MediaArena</u>	SHA1	33c02d70abb2f1f12a79cfd780d875a94e7fe877 4041a7410598c46d7657ceb94b0af4ebbc7a9c0a
	SHA256	5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe61908 2abcc6794aebc e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45 a0bd28fbc2cae6 cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803 d68f08e337630 e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c 40a1ce9b6a260 6d37baeb841bcf6c4935a54f29df049d405df48345014cc1285 2b814d279d86e
	Hostname	Goto[.]searchpoweronline[.]com
<u>Satacom</u>	MD5	0ac34b67e634e49b0f75cf2be388f244 1aa7ad7efb1b48a28c6ccf7b496c9cfd 199017082159b23decdf63b22e07a7a1 a7f17ed79777f28bf9c9cebaa01c8d70
	Domains	dns-beast[.]com don-dns[.]com die-dns[.]com hit-mee[.]com noname-domain[.]com don-die[.]com old-big[.]com tchk-1[.]com you-rabbit[.]com web-lox[.]com

Attack Name	TYPE	VALUE
<u>Satacom</u>	Domains	ht-specialize[.]xyz ht-input[.]cfd ht-queen[.]cfd ht-dilemma[.]xyz ht-input[.]cfd io-strength[.]cfd fbs-university[.]xyz io-previous[.]xyz io-band[.]cfd io-strength[.]cfd io-band[.]cfd can-nothing[.]cfd scope-chat[.]xyz stroke-chat[.]click icl-surprise[.]xyz new-high[.]click shrimp-clock[.]click oo-knowledge[.]xyz oo-station[.]xyz oo-blue[.]click oo-strategy[.]xyz oo-clearly[.]click economy-h[.]xyz medical-h[.]click hospital-h[.]xyz church-h[.]click close-h[.]xyz thousand-h[.]click risk-h[.]xyz current-h[.]click fire-h[.]xyz future-h[.]click moment-are[.]xyz himself-are[.]click air-are[.]xyz teacher-are[.]click force-are[.]xyz enough-are[.]xyz education-are[.]click across-are[.]xyz although-are[.]click punishment-chat[.]click rjyy-easily[.]xyz guy-seventh[.]cfd back-may[.]com post-make[.]com

Attack Name	TYPE	VALUE
<u>Satacom</u>	Domains	filesend[.]live soft-kind[.]com ee-softs[.]com big-loads[.]com el-softs[.]com
<u>NODEBOT</u>	SHA1	C98061592DE61E34DA280AB179465580947890DE
<u>Sunseed</u>	IPV4	146[.]70[.]79[.]119
<u>AHKBOT</u>	SHA1	57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B 64F5AC9F0C6C12F2A48A1CB941847B0662734FBF 557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF F85B82805C6204F34DB0858E2F04DA9F620A0277 5492061DE582E71B2A5DA046536D4150F6F497F1 C554100C15ED3617EBFAAB00C983CED5FEC5DB11 AD8143DE4FC609608D8925478FD8EA3CD9A37C5D F2948C27F044FC6FB4849332657801F78C0F7D5E 7AA23E871E796F89C465537E6ECE962412CDA636 384961E19624437EB4EB22B1BF45953D7147FB8F 7FDB9A73B3F13DBD94D392132D896A5328DACA59 3E38D54CC55A48A3377A7E6A0800B09F2E281978 7F8742778FC848A6FBCFFEC9011B477402544171 29604997030752919EA42B6D6CEE8D3AE28F527E 7A78AF75841C2A8D8A5929C214F08EB92739E9CB 441369397D0F8DB755282739A05CB4CF52113C40 117ECFA95BE19D5CF135A27AED786C98EC8CE50B D24A9C8A57C08D668F7D4A5B96FB7B5BA89D74C3 95EDC096000C5B8DA7C8F93867F736928EA32575 62FA77DAEF21772D599F2DC17DBBA0906B51F2D9 A9E3ACFE029E3A80372C0BB6B7C500531D09EDBE EE1CFEDD75CBA9028904C759740725E855AA46B5
	IPV4	5.39.222[.]150 5.44.42[.]27 5.230.68[.]137 5.230.71[.]166 5.230.72[.]38 5.230.72[.]148 5.230.73[.]57 5.230.73[.]63 5.230.73[.]241 5.230.73[.]247 5.230.73[.]248 5.230.73[.]250 5.252.118[.]132 5.252.118[.]204 5.255.88[.]222

Attack Name	TYPE	VALUE
AHKBOT	IPV4	23.106.123[.]119
		31.192.105[.]28
		45.76.211[.]131
		45.77.185[.]151
		45.132.1[.]238
		45.147.229[.]20
		46.17.98[.]190
		46.151.24[.]197
		46.151.24[.]226
		46.151.25[.]15
		46.151.25[.]49
		46.151.28[.]18
		51.83.182[.]153
		51.83.189[.]185
		62.84.99[.]195
		62.204.41[.]171
		77.83.197[.]138
		79.137.196[.]121
		79.137.197[.]187
		80.66.88[.]155
		84.32.188[.]29
		84.32.188[.]96
		85.192.49[.]106
		85.192.63[.]13
		85.192.63[.]126
		85.239.60[.]40
		88.210.10[.]62
		89.41.182[.]94
		89.107.10[.]7
		89.208.105[.]255
		91.245.253[.]112
		94.103.83[.]46
		94.140.114[.]133
		94.140.114[.]230
		94.140.115[.]44
		94.232.41[.]96
		94.232.41[.]108
		94.232.43[.]214
		98.142.251[.]26
		98.142.251[.]226
		104.234.118[.]163
104.248.149[.]122		
109.107.173[.]72		
116.203.252[.]67		
128.199.82[.]141		

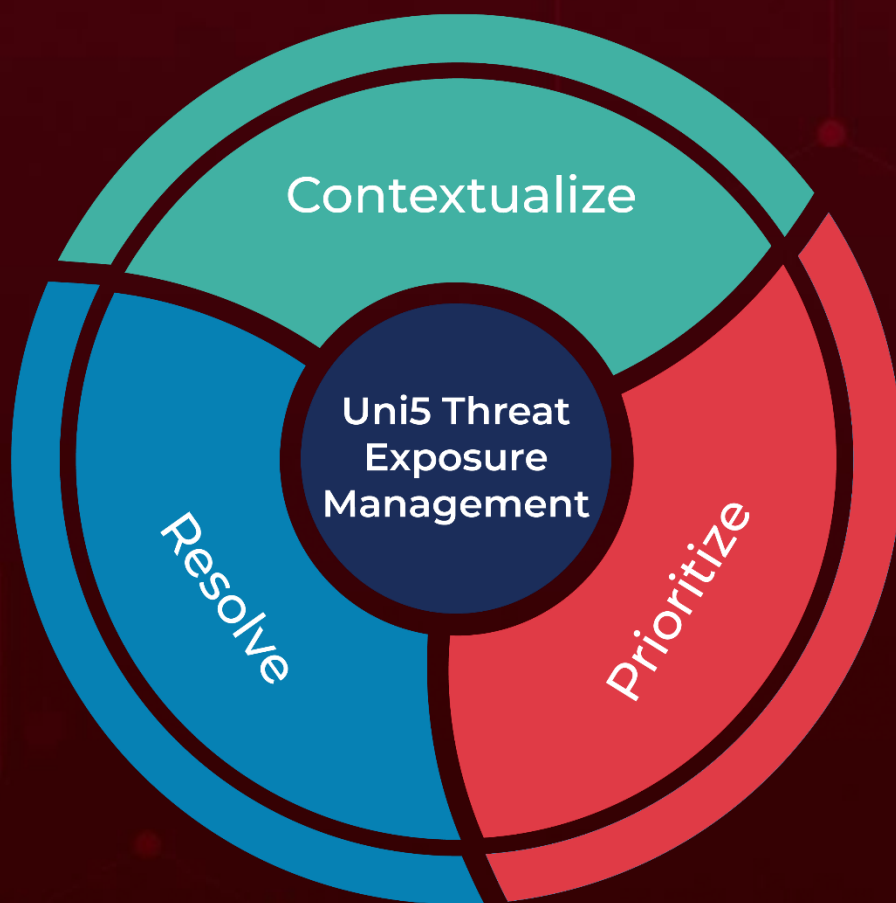
Attack Name	TYPE	VALUE
<u>AHKBOT</u>	IPV4	139.162.116[.]148 141.105.64[.]121 146.0.77[.]15 146.70.79[.]117 157.254.194[.]225 157.254.194[.]238 172.64.80[.]1 172.86.75[.]49 172.104.94[.]104 172.105.235[.]94 172.105.253[.]139 176.124.214[.]229 176.124.217[.]20 185.70.184[.]44 185.82.126[.]133 185.123.53[.]49 185.150.117[.]122 185.163.45[.]221 193.109.69[.]52 193.142.59[.]152 193.142.59[.]169 194.180.174[.]51 195.2.81[.]70 195.133.196[.]230 212.113.106[.]27 212.113.116[.]147 212.118.43[.]231 213.109.192[.]230
<u>Stealth Soldier</u>	IPV4	185.125.230[.]216 185.125.230[.]116 94.156.33[.]228 94.156.33[.]229 185.125.230[.]224 185.125.230[.]220
	Domains	filestoragehub[.]live customjvupdate[.]live filecloud[.]store webmailogemail[.]com loglivemail[.]com 2096[.]website

Attack Name	TYPE	VALUE
<u>Stealth Soldier</u>	SHA256	2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48 112862ceb3efb 05db5e180281338a95e43a211f9791bd53235fca1d07c00eda 0be7fdc3f6a9bc b9e9b93e99d1a8fe172d70419181a74376af8188dcb0324903 7d4daea27f110e d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a72 0a53a52a677db e7794fac887a20e08ed9855ac963573549809d373dfe4a287d 1dae03bffc59f 8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42 be6e9af24946 df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b 0b43c4c65ff0b4 e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0 fb574416354f a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5 236b0c31f08974 c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903 267d422878dbc6 cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43 a3370e24b8c90a d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c 5a0038d2ce19885 b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9 219ba75bfd5723 7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71 ea6d5682c92bd

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

June 12, 2023 • 7:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com