

Date of Publication
August 12, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

05 to 11 AUGUST 2024

Table Of Contents

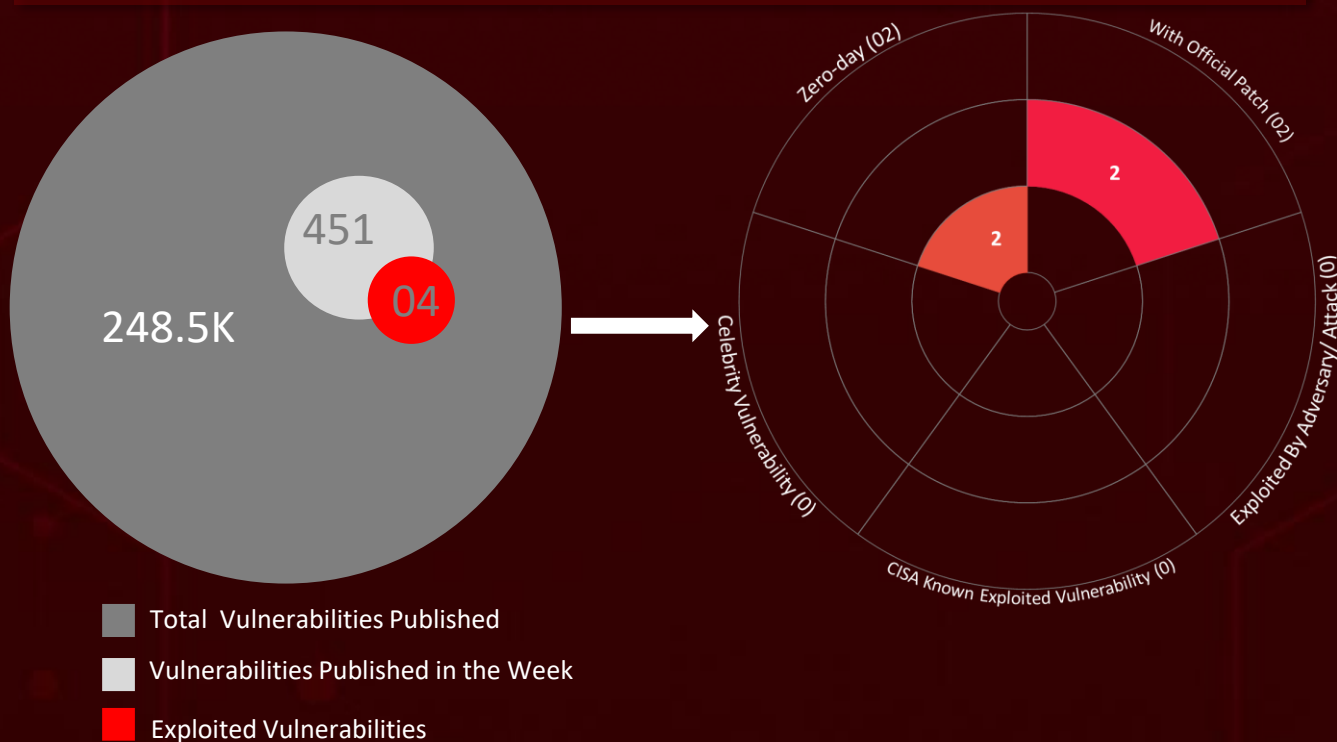
<u>Summary</u>	03
<u>High Level Statistics</u>	05
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	17
<u>Adversaries in Action</u>	19
<u>Recommendations</u>	23
<u>Threat Advisories</u>	24
<u>Appendix</u>	25
<u>What Next?</u>	30

Summary

HiveForce Labs has recently made significant progress in uncovering cybersecurity threats. Over the past week alone, the lab detected **eighteen** executed attacks, reported **four** exploited vulnerabilities, and identified **four** active adversaries. These findings underscore the persistent and escalating danger of cyber intrusions.

Furthermore, **Hunters International**, a Ransomware-as-a-Service (RaaS) operation suspected of being a rebranding of Hive ransomware, emerged in October 2023 and has claimed responsibility for 134 attacks in early 2024. A pre-authentication remote code execution vulnerability, **CVE-2024-38856**, has also been uncovered in Apache OFBiz, posing a severe risk to organizations utilizing this open-source enterprise resource planning (ERP) system.

Moreover, several critical security flaws in Progress Software's WhatsUp Gold, particularly **CVE-2024-4885**, are being actively exploited. The **Bloody Wolf** threat group has been targeting organizations in Kazakhstan since late 2023 using STRRAT malware. The "**0.0.0.0 Day**" vulnerability is another critical security flaw affecting major web browsers like Chromium, Firefox, and Safari, allowing malicious websites to exploit localhost APIs through the 0.0.0.0 IP address. Two new **zero-day** vulnerabilities in Windows, **CVE-2024-38202 and CVE-2024-21302**, allow attackers to revert systems to outdated, unpatched versions, making them vulnerable to previous exploits. These growing threats present an immediate and significant danger to users worldwide.



High Level Statistics

18

Attacks
Executed

4

Vulnerabilities
Exploited

4

Adversaries in
Action

- [HeadLace](#)
 - [BITSLOTH](#)
 - [SharpRhino](#)
 - [Hunters International](#)
 - [STRRAT](#)
 - [AsyncRAT](#)
 - [GuLoader](#)
 - [PureLogs](#)
 - [Remcos RAT](#)
 - [VenomRAT](#)
 - [Xworm](#)
 - [MACMA](#)
 - [POCOSTICK](#)
 - [Cmoon](#)
 - [GoGra](#)
 - [Grager](#)
 - [MoonTag](#)
 - [Onedrivetools](#)
- [CVE-2024-38856](#)
 - [CVE-2024-4885](#)
 - [CVE-2024-38202](#)
 - [CVE-2024-21302](#)
- [APT28](#)
 - [Bloody Wolf](#)
 - [Moonstone](#)
 - [Sleet](#)
 - [StormBamboo](#)



Insights

CVE-2024-38856: The RCE Threat Lurking in Apache OFBiz

Rebirth of Hive: Hunters International Claims Responsibility for 134 Attacks in 2024

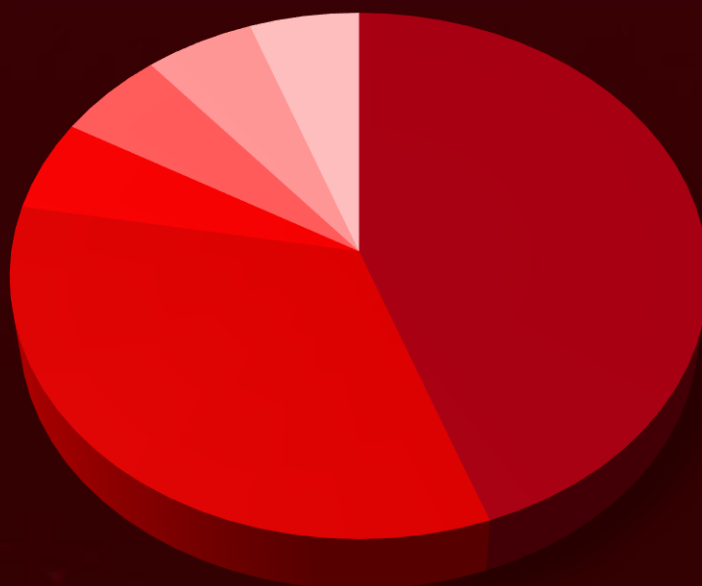
0.0.0.0 Day Vulnerability: The Silent Browser Threat Since 2006

Exploits in the Wild: WhatsUp Gold's CVE-2024-4885 Threatens Network Security

Windows Under Attack: Zero-Day Vulnerabilities Downgrade Security Patches

APT28's Deceptive Drive: Fake Car Ads Deliver HeadLace Malware

Threat Distribution



■ Backdoor ■ RAT ■ Ransomware ■ Downloader ■ Information Stealer ■ Worm

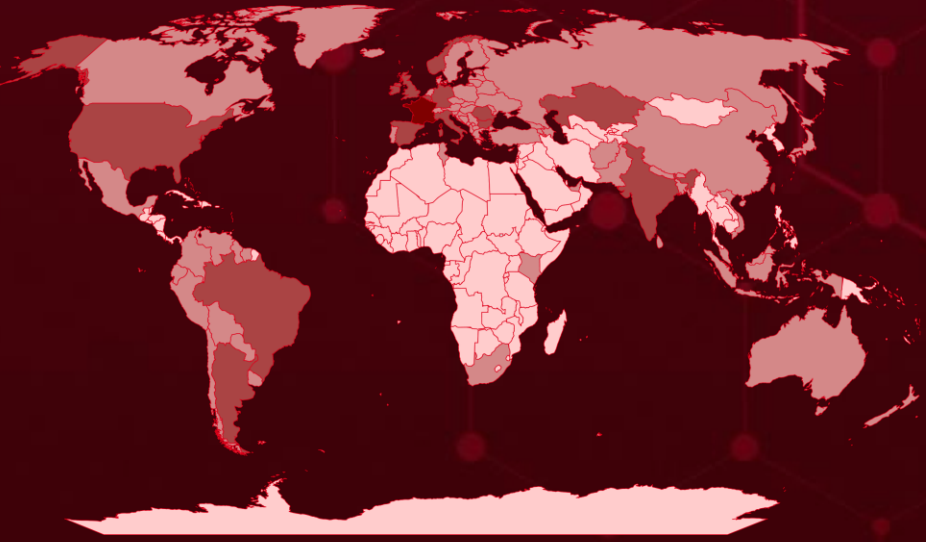


Targeted Countries

Most



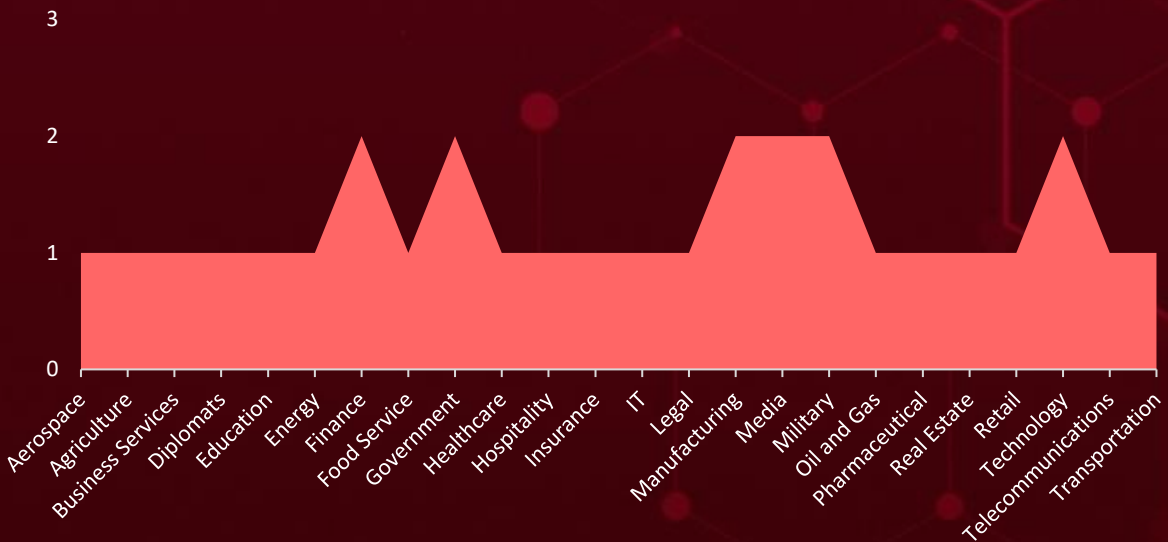
Least



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

Countries	Countries	Countries	Countries
France	Colombia	Greece	Switzerland
Ireland	Akrotiri and Dhekelia	Mexico	Kenya
Argentina	Croatia	Greenland	Transnistria
Kazakhstan	Tunisia	Monaco	Kosovo
Belgium	Cyprus	Guernsey	Turkey
United Kingdom	Malaysia	Nepal	Abkhazia
Brazil	Czech Republic	Guyana	United Arab Emirates
United States	Moldova	New Zealand	Liechtenstein
Bulgaria	Denmark	Hong Kong	Bosnia and Herzegovina
Norway	Netherlands	Northern Cyprus	Lithuania
Romania	Ecuador	Hungary	Vatican City
Spain	Bangladesh	Pakistan	Japan
Taiwan	Estonia	Iceland	Vietnam
Germany	Poland	Peru	Jersey
India	Falkland Islands	Armenia	Latvia
Italy	San Marino	Portugal	French Guiana
Slovakia	Faroe Islands	Indonesia	Western Sahara
Montenegro	South Africa	Russia	Guinea-Bissau
Bolivia	Finland	Australia	Sint Maarten
Åland	Suriname	Serbia	Haiti
Paraguay	Andorra	Isle of Man	Puerto Rico
Albania	Bhutan	Slovenia	Honduras
Sweden	Georgia	Austria	South Korea
Canada	Ukraine	South Ossetia	Burkina Faso
Malta	Afghanistan	Uruguay	Togo
Chile	Luxembourg	Sri Lanka	Burundi
North Macedonia	Gibraltar	Venezuela	British Virgin Islands
China	Maldives	Svalbard	
Belarus		Azerbaijan	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1588

Obtain Capabilities

T1071

Application Layer Protocol

T1608

Stage Capabilities

T1566

Phishing

T1573

Encrypted Channel

T1068

Exploitation for Privilege Escalation

T1588.006

Vulnerabilities

T1070

Indicator Removal

T1070.004

File Deletion

T1189

Drive-by Compromise

T1574.002

DLL Side-Loading

T1543

Create or Modify System Process

T1059.007

JavaScript

T1071.001

Web Protocols

T1190

Exploit Public-Facing Application

T1082

System Information Discovery

T1059.003

Windows Command Shell

T1083

File and Directory Discovery

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HeadLace	A new campaign uses a car-for-sale phishing lure to deliver a modular Windows backdoor called HeadLace. HeadLace is modular malware that operates in stages.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure	PATCH LINK
APT28			
IOC TYPE	VALUE		
SHA256	6b96b991e33240e5c2091d092079a440fa1bef9b5aecbf3039bf7c47223bdf96		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BITSLOTH	BITSLOTH is a newly discovered, highly advanced Windows backdoor malware. Leveraging the Background Intelligent Transfer Service (BITS) for its command-and-control (C2) mechanism, BITSLOTH highlights the technical prowess of its likely Chinese developers.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	4a4356faad620bf12ff53bcfac62e12eb67783bd22e66bf00a19a4c404bf45df, dfb76bcf5a3e29225559ebbd8e8bdd24f69262492eca2f99f7a9525628006d88, 4fb6dd11e723209d12b2d503a9fcf94d8fed6084aceca390ac0b7e7da1874f50, 0944b17a4330e1c97600f62717d6bae7e4a4260604043f2390a14c8d76ef1507		

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>SharpRhino</u>	SharpRhino, a new C# remote access trojan distributed via typosquatting domains. SharpRhino enables Hunters International RaaS to achieve initial infection, escalate privileges on compromised systems, execute specific PowerShell commands, and ultimately deploy the ransomware payload.	Dropped via typosquatting domains	-
		IMPACT	AFFECTED PRODUCTS
TYPE	International RaaS to achieve initial infection, escalate privileges on compromised systems, execute specific PowerShell commands, and ultimately deploy the ransomware payload.	Information Theft, Compromise Infrastructure	-
RAT			PATCH LINK
ASSOCIATED ACTOR	-		-
-			
IOC TYPE	VALUE		
SHA256	223aa5d93a00b41bf92935b00cb94bb2970c681fc44c9c75f245a236d617d9bb, 09b5e780227caa97a042be17450ead0242fd7f58f513158e26678c811d67e264		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Hunters International</u>	Hunters International, a Ransomware-as-a-Service (RaaS) operation suspected to be a rebrand of Hive ransomware, surfaced in October 2023. Before encrypting files, Hunters International exfiltrates data from victim organizations.	Dropped by another malware	-
		IMPACT	AFFECTED PRODUCTS
TYPE	Before encrypting files, Hunters International exfiltrates data from victim organizations.	Information Theft, Financial Loss	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR	-		-
-			
IOC TYPE	VALUE		
SHA256	c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e, c83e982448ed1a0a52efa8c87db40f499b052e0495730d3324540bee10ffdb9a		

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>STRRAT (aka Strigoi Master)</u>	STRRAT also a Java-built RAT,, available for purchase on underground forums for 80\$, exfiltrates sensitive data and allows remote control of compromised systems. The use of legitimate web services like Pastebin helps the attackers evade detection.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Information Theft, Compromise Infrastructure, Remote Control	-
ASSOCIATED ACTOR			PATCH LINK
Bloody Wolf			-
IOC TYPE		VALUE	
SHA256	e35370cb7c8691b5fdd9f57f3f462807b40b067e305ce30eabc16e0642eca06b, 00172976ee3057dd6555734af28759add7daea55047eb6f627e5491701c3ec83		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AsyncRAT</u>	AsyncRAT is a malware known malicious activities since 2019. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system.	Phishing Emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Information Theft, Espionage	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE		VALUE	
Domain	dcxwq1[.]duckdns[.]org, todfg[.]duckdns[.]org		
MD5	c9562d033d5e13674af5b5fdc3e5801c, e618be3fea2925a6637d8fcf05ff5c8a		

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>GuLoader</u>	<p>GuLoader malware operates covertly, delivering malicious payloads to your device. First identified in late 2019, this sophisticated downloader employs various techniques to avoid detection.</p>	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	7faedb38872ca436e3fd84faaf822ccfee2ce5ffae16b4d7ce5d2552cf61d6, 00efaea983bd75aa20453d6a0807f5f41d8b117ec6fa7e28d8ca58dbd54a441c, 50a240dd81f289babfee552b103ca3a5cb94eda0db53ec8c5ccc6afa0970b298, 4f22fda1b8750f74b9888362da59a7207f21b3c2321a77ec470f30ada4bbfe62		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PureLogs</u>	<p>PureLogs is a data-stealing malware that extracts a broad spectrum of information from compromised systems, including browser data, cryptocurrency wallets, and PC configuration details. It operates on a subscription model, making it accessible to any threat actor for use in their attacks.</p>	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Information Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
MD5	1e66092482f2738ff808c2fc076185e6		
Domain	ncmomenthv[.]duckdns[.]org		

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>Remcos RAT</u>	Remcos, is often employed by attackers to gain complete control over systems. It operates stealthily, elevates privileges, and persists through reboots. Common methods of delivery include phishing emails, exploit kits, and watering hole attacks.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
			PATCH LINK
			-
TYPE			
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	f60667b9e2a0a25221cdb47844149beb3b1cd08abbc3360e8684fad9d8aaa20e, 2ebf1aed428b35603a907ec88f9172c89eaa08e45070582f4995988f5c6ca8c4, 7cab170002b5372d67add0e7c53e0cf620f33620391efd81c16e1d2000300bbf, 71551d17db59a2ad36d75a15b0b0a84444c2b0e3de1309f14ac8abb305d26b32		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>VenomRAT</u>	VenomRAT is a remote access trojan (RAT) malware designed to exfiltrate data and seize control of infected devices. This highly sophisticated malware is challenging to detect and remove.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
			PATCH LINK
			-
TYPE			
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA1	51179defee9d29718177eb3fd0d0fdd5016165fc		
SHA256	c2278039f0acee06931c3e5f137605c175dab3174c327d9b87842975bf8ca36e		

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>Xworm</u>	XWorm enables unauthorized access to devices, facilitating the theft of sensitive information, including login credentials and passwords. Additionally, it features capabilities for clipboard monitoring and ransomware installation.	Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
			PATCH LINK
			-
		TYPE	
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
IPv4	157[.]20[.]182[.]172		
Domain	welxwrm[.]duckdns[.]org, xwor3july[.]duckdns[.]org		
SHA256	1073ff4689cb536805d2881988b72853b029040f4446af5ced18d1bc08b2266e1		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>MACMA</u>	MACMA was first publicly documented in 2021. It uses a the kNET protocol UDP for communicating with the C2. It also has several components, some of which appear to be configured as modules.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	Windows and macOS
			PATCH LINK
			-
		TYPE	
Backdoor			
ASSOCIATED ACTOR			
StormBamboo			
IOC TYPE	VALUE		
SHA256	d599d7814adbab0f1442f5a10074e00f3a776ce183ea924abcd6154f0d068bb4		

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>POCOSTICK (aka MGBot)</u>	POCOSTICK is a modular backdoor malware framework that is actively maintained and equipped with various plugins, allowing attackers to gather extensive information from compromised machines.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
StormBamboo			-
IOC TYPE	VALUE		
SHA256	003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef, 1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e, dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Cmoon</u>	'CMoon' has been actively distributed in Russia since early July 2024. The worm is capable of stealing account credentials and other sensitive data, posing significant risks to infected systems. Developed using the .NET framework, CMoon is designed to evade detection by modifying file and folder and embedding itself in antivirus directories when possible.	Compromised website	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Stealing Credentials, Espionage	-
Worm			PATCH LINK
ASSOCIATED ACTOR			-
-			-
IOC TYPE	VALUE		
SHA256	a4be526be5359ad2981f439457fe652895731ad56c10c113c22a7836a9591e5d		

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>GoGra</u>	GoGra, written in the Go programming language, interacts with its command-and-control (C&C) server via the Microsoft Graph API, which is hosted on Microsoft's mail services. This malware is believed to be the work of Harvester, a nation-state-backed group known for targeting organizations in South Asia.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure	PATCH LINK
-			-
IOC TYPE		VALUE	
SHA256	d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f, f1ccd604fcdc0034d94e575b3709cd124e13389bbec55c59cbbf7d4f3476e214		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Grager</u>	Grager is capable of executing a range of commands, such as downloading and uploading files, running programs, and collecting file system information. It utilizes the Graph API to interact with a command-and-control (C&C) server hosted on Microsoft OneDrive.	Typosquatted URL	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR		Information Theft, Espionage	PATCH LINK
-			-
IOC TYPE		VALUE	
SHA256	9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9, ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985, 97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824		




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>MoonTag</u>	MoonTag, which seems to be in its early development stages, is based on code discovered in a Google Group. Its use of language and infrastructure suggests a likely association with a Chinese-speaking threat actor.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure	PATCH LINK
-			-
IOC TYPE			VALUE
SHA256	a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcb6, 527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14, fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Onedrivetools</u>	Onedrivetools is a multi-stage backdoor. The initial stage functions as a downloader, authenticating via the Microsoft Graph API to retrieve and execute the second-stage payload from OneDrive. Additionally, this backdoor can download files onto the victim's machine and upload files from the infected system to OneDrive.	Spear Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR		Information Theft, Espionage	PATCH LINK
-			-
IOC TYPE			VALUE
SHA256	f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274, 582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede, 79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6		




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-2024-38856</u>		Apache OFBiz versions up to 18.12.14	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apache:ofbiz:18.12.14:*:*:*:*:*:*	-
Apache OFBiz Incorrect Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1068: Exploitation for Privilege Escalation, T1556: Modify Authentication Process, T1059: Command and Scripting Interpreter	https://ofbiz.apache.org/download.html


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4885</u>		WhatsUp Gold versions released before 2023.1.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*	-
Progress WhatsUp Gold Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter, T1608.001: Upload Malware	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38202		Windows: 10 - 11 23H2 Windows Server: 2016 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_server:*.*.*.*.*.*.*	
Windows Update Stack Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows:*.*.*.*.*.*.*	-
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities	Microsoft is working on a patch to fix flaw, but it has not yet been released.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21302		Windows: 10 - 11 23H2 Windows Server: 2016 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_server:*.*.*.*.*.*.*	
Windows Secure Kernel Mode Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows:*.*.*.*.*.*.*	-
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities	Microsoft is working on a patch to fix flaw, but it has not yet been released.


Adversaries in Action


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Russia	Diplomats	Worldwide
	MOTIVE Information Theft, Espionage		
<u>APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)</u>	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	HeadLace	Windows
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; T1592: Gather Victim Host Information; T1566: Phishing; T1189: Drive-by Compromise; T1132: Data Encoding; T1132.001: Standard Encoding; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1036.007: Double File Extension; T1070: Indicator Removal; T1070.004: File Deletion; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Bloody Wolf</u>	-	All	Kazakhstan
	MOTIVE Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	STRRAT	Windows

TTPs

TA0005: Defense Evasion; TA0007: Discovery; TA0003: Persistence; TA0040: Impact; TA0006: Credential Access; TA0001: Initial Access; TA0009: TTPs; TA0002: Execution; TA0011: Collection; TA0004: Privilege Escalation; T1486: Data Encrypted for Impact: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059.005: Visual Basic; T1053.005: Scheduled Task; T1136.001: Local Account; T1547: Boot or Logon Autostart Execution; T1070: Indicator Removal; T1082: System Information Discovery; T1185: Browser Session Hijacking; T1090.001; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1547.001: Registry Run Keys / Startup Folder; T1134: Access Token Manipulation; T1057: Process Discovery; T1564; T1566.002: Spearphishing Link; T1083: File and Directory Discovery; T1059: Command and Scripting Interpreter; T1055: Process Injection; T1059.003: Windows Command Shell; T1059.007: JavaScript; T1136: Create Account; T1036: Masquerading; T1134.002: Create Process with Token; T1112: Modify Registry; T1056.001: Hide Artifacts; T1113: Screen Capture; T1090: Internal Proxy; T1102: Web Service: Proxy; T1105: Keylogging; T1518: Software Discovery; T1518.001: Security Software Discovery; T1529: Ingress Tool Transfer: System Shutdown/Reboot; T1070.004: File Deletion; T1564.003: Hidden Window; T1056: Input Capture; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Moonstone Sleet (aka Stressed Pungsan, Storm-1789)</u></p>	North Korea	All	Worldwide
	MOTIVE Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0008: Lateral Movement; TA0010: Exfiltration; TA0011: Command and Control; T1189: Drive-by Compromise; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1036: Masquerading; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1070: Indicator Removal; T1070.004: File Deletion; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1071: Application Layer Protocol; T1071.001: Web Protocols			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p>StormBamboo (aka Evasive Panda, StormCloud)</p>	China	All	Worldwide
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	MACMA and POCOSTICK (aka MGBot)	macOS, Windows	

TTPs

TA0001: Initial Access; TA0011: Command and Control; TA0042: Resource Development; T1071.004: DNS; T1588: Obtain Capabilities; T1176; TA0002: Execution; TA0005: Defense Evasion; T1566: Phishing; T1557; TA0009: Collection; TA0003: Persistence; TA0006: Credential Access; TA0010: Exfiltration; T1059: Command and Scripting Interpreter; T1557: Adversary-in-the-Middle T1071: Application Layer Protocol; T1584.001: Domains; T1059.002: Browser Extensions: AppleScript; T1584: Compromise Infrastructure; T1185: Browser Session Hijacking, T1027: Obfuscated Files or Information; T1588.004: Digital Certificates; T1059.007: JavaScript

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 **APT28, Bloody Wolf, Moonstone Sleet, StormBamboo**, and malware **HeadLace, BITSLOTH, SharpRhino, Hunters International, STRRAT, AsyncRAT, GuLoader, PureLogs, Remcos RAT, VenomRAT, Xworm, MACMA, POCOSTICK, Cmoon, GoGra, Grager, MoonTag, Onedrivetools**.

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 **APT28, Bloody Wolf, Moonstone Sleet, StormBamboo**, and malware **HeadLace, BITSLOTH, SharpRhino, STRRAT, AsyncRAT, GuLoader, PureLogs, Remcos, VenomRAT, XWorm, Macma, GoGra, Grager, Onedrivetools, CMoon** in Breach and Attack Simulation(BAS).

Threat Advisories

[Car Sale Scam: APT28 Delivers Malware Instead of the Vehicle](#)

[BITSLOTH Backdoor Leverages BITS for C2](#)

[Hunters International is Redefining RaaS Operations](#)

[Apache OFBiz Flaw Enables Attackers to Execute Remote Code](#)

[Bloody Wolf Targets Kazakhstan with STRRAT Malware](#)

[RATs on the Loose Through Abused Cloudflare Tunnels](#)

[North Korean Hackers Embed Malicious Code in Legitimate npm Packages](#)

[StormBamboo Abuses ISP to Push Malware via Software Updates](#)

[CVE-2024-4885: Active Exploitation of Critical WhatsUp Gold RCE Flaw](#)

[CMoon Worm Emerges: Targets Russia in Data Theft Attacks](#)

[Cloud Services Transformed into Cyber Weapons: New Wave of Espionage](#)

[18 Years of Unresolved Threat: 0.0.0.0 Day Vulnerability in Major Browsers](#)

[Cisco SSM On-Prem Flaw Lets Hackers Hijack User Passwords](#)

[Windows Update Zero-Day Flaws Allow Downgrade Attacks on Patched Systems](#)

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>HeadLace</u>	SHA256	6b96b991e33240e5c2091d092079a440fa1bef9b5aecbf3039bf7c47223bdf96
<u>BITSLOTH</u>	SHA256	4a4356faad620bf12ff53bcfac62e12eb67783bd22e66bf00a19a4c404bf45df, dfb76bcf5a3e29225559ebbd8e8bdd24f69262492eca2f99f7a9525628006d88, 4fb6dd11e723209d12b2d503a9fcf94d8fed6084aceca390ac0b7e7da1874f50, 0944b17a4330e1c97600f62717d6bae7e4a4260604043f2390a14c8d76ef1507, 0f9c0d9b77678d7360e492e00a7fa00af9b78331dc926b0747b07299b4e64afd
<u>SharpRhino</u>	SHA256	223aa5d93a00b41bf92935b00cb94bb2970c681fc44c9c75f245a236d617d9bb, 09b5e780227caa97a042be17450ead0242fd7f58f513158e26678c811d67e264
<u>Hunters International</u>	SHA256	c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e, c83e982448ed1a0a52efa8c87db40f499b052e0495730d3324540bee10ffdb9a
<u>STRRAT</u>	SHA256	e35370cb7c8691b5fdd9f57f3f462807b40b067e305ce30eabc16e0642eca06b, 00172976ee3057dd6555734af28759add7daea55047eb6f627e5491701c3ec83, ab6f8c51d1f15a18cd23e1ad5a34c82c83746befb7d11cce2860c971be35adaa, d634982709d3ebf1641b1160ed6452fa9e3bf2cc8d28f397e56ca9687b28ec84,

Attack Name	TYPE	VALUE
<u>STRRAT</u>	SHA256	a0670c21968e2b1256d72799c22a512e503597ab375d20c49d9ec43428c4c3b2, 3a74d083e1c4e30f1eedcb90c842bf1a7e65a979edab40e37885607bd566bee8, 569f5f6de156bec90f9b0b0e4e707a702c0fea26ab6a0711e32f4a413995ae7c, 176e45016749ec233b8fe1ce32ce2cd47dd5bc8da3663f1c6cf054f6ad58a187, 3094952f4e4c826cdfbc7b146212eec6094f5104b4ba0d70d3b2920a263add27, 4bf781354d02ca0d67a3a180fd6f0d183c6fba763caa660f986752be8b4bb586, 6f7180a451691ee975f516cfc6fb3f0c983bc80aebd1d662a899ff4344e4077e, b364c066e0aa794dd34c7a67ef08e83782c01be225edb5533f3a51f855d5e34, 9714dce49616e48fc4851d05453056939ab08bf140fe9a786616fa914debb4f4
<u>AsyncRAT</u>	SHA256	c2278039f0acee06931c3e5f137605c175dab3174c327d9b87842975bf8ca36e
	Domains	dcxwq1[.]duckdns[.]org, todfg[.]duckdns[.]org
	MD5	c9562d033d5e13674af5b5fdc3e5801c, e618be3fea2925a6637d8fcf05ff5c8a
<u>GuLoader</u>	SHA256	7faedbbd38872ca436e3fd84faaf822ccfee2ce5ffae16b4d7ce5d2552cf61d6, 00efaea983bd75aa20453d6a0807f5f41d8b117ec6fa7e28d8ca58dbd54a441c, 50a240dd81f289babfee552b103ca3a5cb94eda0db53ec8c5ccc6afa0970b298, 4f22fda1b8750f74b9888362da59a7207f21b3c2321a77ec470f30ada4bbfe62, 32ea41ff050f09d0b92967588a131e0a170cb46baf7ee58d03277d09336f89d9
<u>PureLogs</u>	SHA256	32312ed6fc1968c041c331c74760d465897b28ccd939749949d07c23df063823
	MD5	1e66092482f2738ff808c2fc076185e6
	Domain	ncmomenthv[.]duckdns[.]org
<u>VenomRAT</u>	SHA256	b77e4af833185c72590d344fd8f555b95de97ae7ca5c6ff5109a2d204a0d2b8e, c2278039f0acee06931c3e5f137605c175dab3174c327d9b87842975bf8ca36e
	SHA1	51179defee9d29718177eb3fd0d0fdd5016165fc
	MD5	58e6b6b4b7f6849749b6374ffbd7fa2e

Attack Name	TYPE	VALUE
<u>Remcos</u>	SHA256	f60667b9e2a0a25221cdb47844149beb3b1cd08abbc3360e8684fad9d8aaa20e, 2ebf1aed428b35603a907ec88f9172c89eaa08e45070582f4995988f5c6ca8c4, 7cab170002b5372d67add0e7c53e0cf620f33620391efd81c16e1d2000300bbf, 71551d17db59a2ad36d75a15b0b0a84444c2b0e3de1309f14ac8abb305d26b32, 43c39e05ae59835e16df8bd732cd035292db70bc2c2d6d95ac354622bfa376ec, cbf16782202823f4a67679afc49ceada8faaff4f26875f3c5ed48821033b05bc, c06b82a4003da0da508dbad0b63fad050682b8490aefa104f4f9f016abb60fb6, c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2
<u>XWorm</u>	SHA256	1073ff4689cb536805d2881988b72853b029040f446af5ced18d1bc08b2266e1
	Domains	welxwrm[.]duckdns[.]org, xwor3july[.]duckdns[.]org
	IPv4	157[.]20[.]182[.]172
<u>MACMA</u>	SHA1	000830573ff24345d88ef7916f9745aff5ee813d, 07f8549d2a8cc76023acee374c18bbe31bb19d91, 0e7b90ec564cb3b6ea080be2829b1a593fff009f, 2303a9c0092f9b0ccac8536419ee48626a253f94, 31f0642fe76b2bdf694710a0741e9a153e04b485, 734070ae052939c946d096a13bc4a78d0265a3a2, 77a86a6b26a6d0f15f0cb40df62c88249ba80773, 941e8f52f49aa387a315a0238cff8e043e2a7222, b2f0dae9f5b4f9d62b73d24f1f52dcb6d66d2f52, b6a11933b95ad1f8c2ad97afedd49a188e0587d2, c4511ad16564eabb2c179d2e36f3f1e59a3f1346, F7549ff73f9ce9f83f8181255de7c3f24ffb2237
<u>CMoon</u>	SHA256	a4be526be5359ad2981f439457fe652895731ad56c10c113c22a7836a9591e5d
	MD5	132404f2b1c1f5a4d76bd38d1402bdfa
	IPv4:Port	93[.]185[.]167[.]95:9899
<u>Grager</u>	SHA256	9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9, ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985, 97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824

Attack Name	TYPE	VALUE
<u>POCOSTICK</u>	SHA256	<p>003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef, 1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e, dad13b0a9f5fde7bcd3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313, 570cd76bf49cf52e0cb347a68bdcf0590b2eaece134e1b1eba7e8d66261bdbe6, eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0, d8a49e688f214553a7525be96cadddec224db19bae3771d14083a2c4c45f28eb, 955cee70c82bb225ca2b108f987fbb245c48eefe9dc53e804bbd9d55578ea3a4, fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced, 5687b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595, 49079ea789e75736f8f8fad804da4a99db52cbaca21e1d2b6d6e1ea4db56faad, 5c52e41090cdd13e0bfa7ec11c283f5051347ba02c9868b4fddfd9c3fc452191, 4c3b9a568d8911a2a256fdc2ebe9ff5911a6b2b63c7784da08a4daf692e93c1a, ef9aebcd9022080189af8aa2fb0b6594c3dfdc862340f79c17fb248e51fc9929, 0cabb6780b804d4ee285b0ddb00b02468f91b218bd2db2e2310c90471f7f8e74, 3894a8b82338791764524fddac786a2c5025cad37175877959a06c372b96ef05, 3a6605266184d967ab4643af2c73dafb8b7724d21c7aa69e58d78b84ebc06612, 65441ea5a7c0d08c1467e9154312ac9d3fdd3ca9188b4234b5944b767d135074</p>
<u>GoGra</u>	SHA256	<p>d728cdf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f, f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214, ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985, 97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824</p>

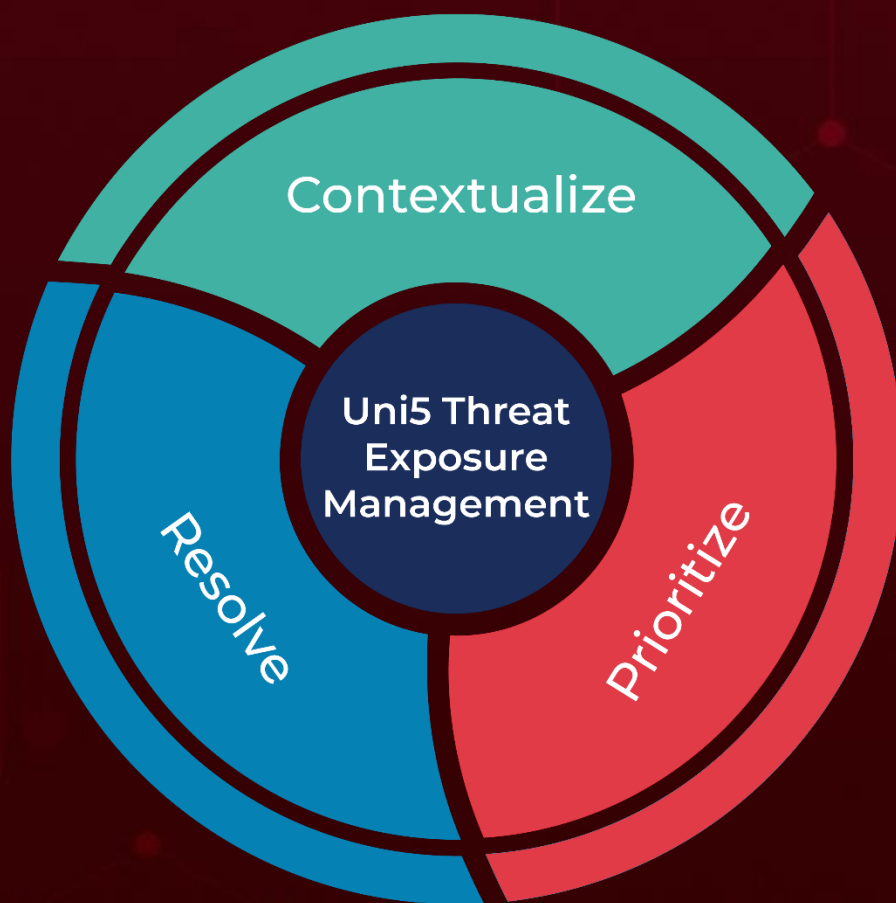
Attack Name	TYPE	VALUE
<u>MoonTag</u>	SHA256	a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcb6, 527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14, fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb
<u>Onedrivetools</u>	SHA256	f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274, 582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede, 79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6, 4057534799993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2

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 12, 2024 • 9:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com