

Date of Publication
February 19, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

12 to 18 FEBRUARY 2024

Table Of Contents

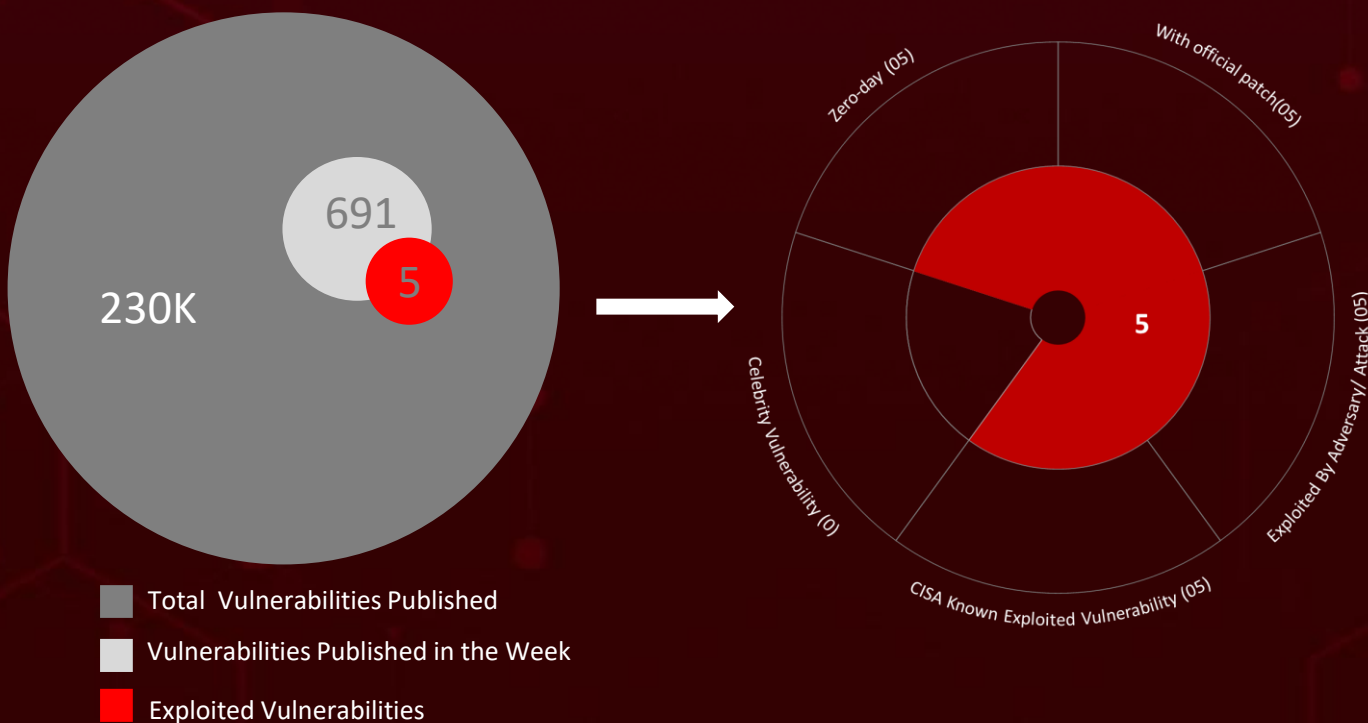
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	18
<u>Threat Advisories</u>	19
<u>Appendix</u>	20
<u>What Next?</u>	23

Summary

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

Furthermore, HiveForce Labs revealed **two zero-day** exploited vulnerabilities has been addressed as part of February 2024 patch Tuesday. One of these vulnerability([CVE-2024-21412](#)) exploited by [Water Hydra APT group](#), to bypass Microsoft Defender SmartScreen, targeting financial traders with DarkMe malware through sophisticated spearphishing tactics..

The [Coyote](#), a new banking trojan is currently targeting more than 60 banking institutions, primarily in Brazil. [Volt Typhoon](#) is actively targeting critical infrastructure in the United States and African countries, employing sophisticated tactics. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

8

Attacks
Executed

5

Vulnerabilities
Exploited

3

Adversaries in
Action

- [Coyote](#)
 - [Zardoor](#)
 - [RustDoor](#)
 - [Rhysida](#)
 - [Ransomware](#)
 - [TinyTurla-NG \(TTNG\)](#)
 - [TurlaPower-NG](#)
 - [DarkMe](#)
 - [Bumblebee](#)
- [CVE-2024-21351](#)
 - [CVE-2024-21412](#)
 - [CVE-2023-36025](#)
 - [CVE-2023-38831](#)
 - [CVE-2024-21410](#)
- [Water Hydra](#)
 - [Volt Typhoon](#)
 - [Turla](#)



Insights

Zardoor

Espionage campaign specifically targeting non-profit organizations in Saudi Arabia

Microsoft Patch Tuesday

Microsoft's February 2024 Patch Tuesday addresses 73 vulnerabilities, including actively exploited zero-days

RustDoor

A Rust-based backdoor currently targeting Apple macOS users

Water Hydra APT

Group exploited **CVE-2024-21412** to bypass Microsoft Defender SmartScreen, targeting financial traders with DarkMe malware through sophisticated spearphishing tactics

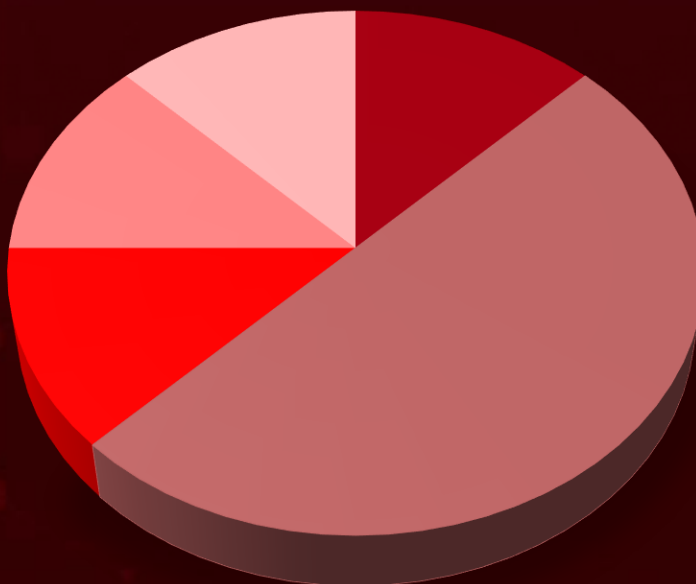
Turla: Russia-affiliated threat actor

Turla employed new malware, named TinyTurla-NG and TurlaPower-NG, to gather sensitive data and maintain access to a targeted network, focusing Polish non-governmental organizations (NGOs)

Coyote

New banking trojan currently targeting more than 60 banking institutions, primarily in Brazil

Threat Distribution



■ Trojan ■ Backdoor ■ Ransomware ■ RAT ■ Loader

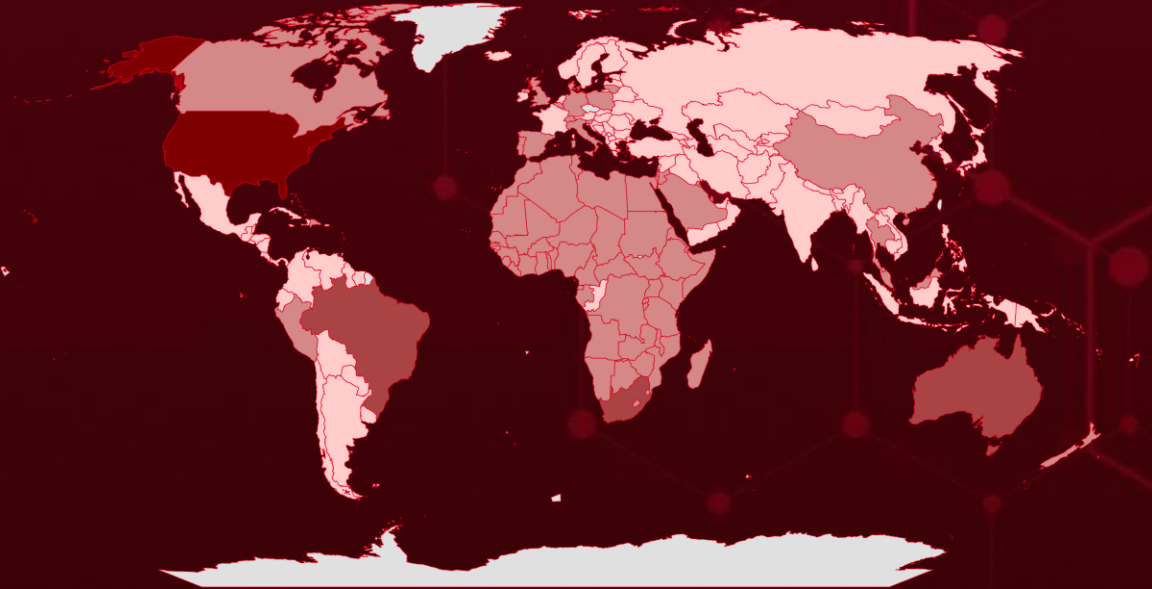


Targeted Countries

Most



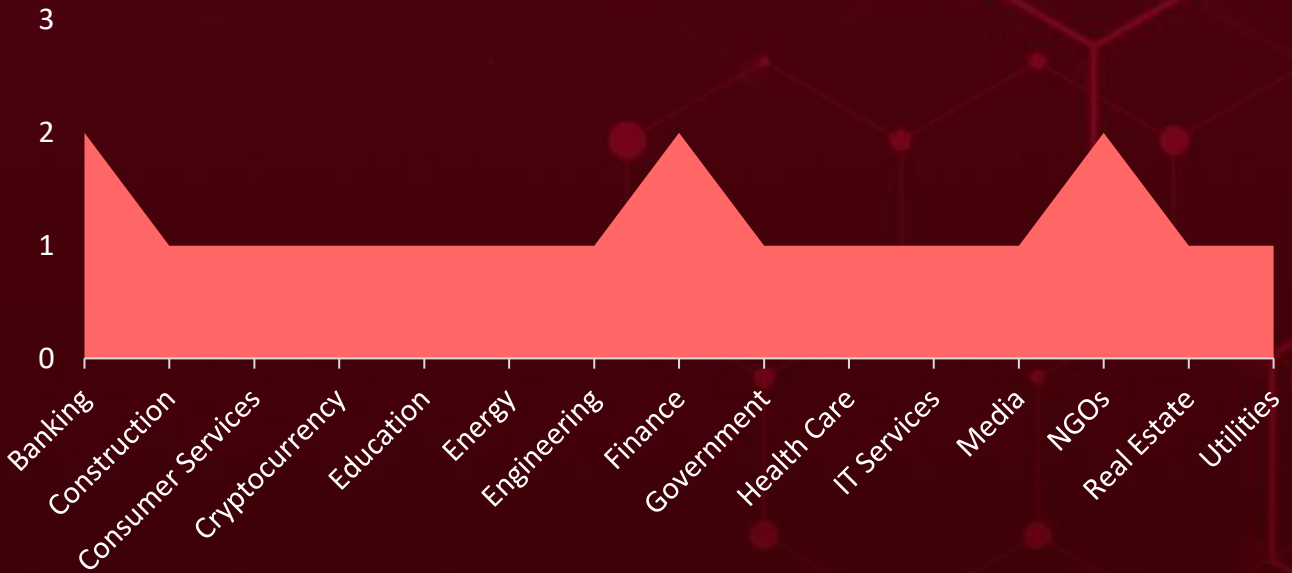
Least



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

Countries	Countries	Countries	Countries
United States	Mozambique	Eswatini	Kenya
Brazil	Chad	Niger	Zambia
Australia	Nigeria	Ethiopia	Kuwait
South Africa	China	Peru	Lesotho
Tanzania	Qatar	Gabon	Libya
New Zealand	Comoros	Portugal	Russia
Malawi	Senegal	Gambia	Timor-Leste
Benin	Congo	Rwanda	Bahrain
Sao Tome & Principe	Belgium	Germany	Ireland
Botswana	Côte d'Ivoire	Saudi Arabia	Venezuela
Zimbabwe	Togo	Ghana	Chile
Angola	Denmark	Seychelles	Azerbaijan
Mauritius	Algeria	Somalia	Belarus
Burkina Faso	Djibouti	Slovenia	Bangladesh
Poland	Liberia	South Sudan	Jamaica
Burundi	Dominican Republic	Sudan	Hungary
Sierra Leone	Madagascar	Guinea	Japan
Cabo Verde	DR Congo	Spain	Andorra
Uganda	Malaysia	Guinea-Bissau	Colombia
Cameroon	Egypt	Switzerland	Samoa
Lithuania	Mauritania	Israel	Kazakhstan
Canada	Equatorial Guinea	Thailand	Singapore
Mali	Morocco	Italy	Albania
Central African Republic	Eritrea	Tunisia	Guatemala
	Namibia	Jordan	Kiribati
		United Kingdom	Syria

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190

Exploit Public-Facing Application

T1059

Command and Scripting Interpreter

T1083

File and Directory Discovery

T1566

Phishing

T1588

Obtain Capabilities

T1082

System Information Discovery

T1588.006

Vulnerabilities

T1498

Network Denial of Service

T1068

Exploitation for Privilege Escalation

T1204

User Execution

T1204.002

Malicious File

T1055

Process Injection

T1211

Exploitation for Defense Evasion

T1105

Ingress Tool Transfer

T1203

Exploitation for Client Execution

T1027

Obfuscated Files or Information

T1218

System Binary Proxy Execution

T1588.005

Exploits

T1071.001

Web Protocols

T1041

Exfiltration Over C2 Channel

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Coyote</u>	Coyote is a new banking trojan and is currently targeting more than 60 banking institutions, primarily in Brazil. The malware distributes itself using the Squirrel installer and executes its infection process using Node.js and Nim, a relatively new multi-platform programming language.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
MD5	03eaccb664d517772a33255dff96020, 071b6efd6d3ace1ad23ee0d6d3eead76, 276f14d432601003b6bf0caa8cd82fec, 5134e6925ff1397fdda0f3b48afec87b, Bf9c9cc94056bcdae6e579e724e8dbbd		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Zardoor</u>	Zardoor is a backdoor malware program that was first discovered in March 2021. It's designed to give attackers remote access to a compromised system, allowing them to steal data, install other malware, or launch further attacks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a60ef585bd2ac2, c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a218e7735561ef74, 73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c5d8cd73083095, a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e3407bc01f661d, 0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b73c208ab723bf		

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>RustDoor</u>	RustDoor is a backdoor malware program that specifically targets macOS devices. It was first discovered in November 2023 and has been linked to the ALPHV/BlackCat and Black Basta ransomware groups.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			MacOS
ASSOCIATED ACTOR			PATCH LINK
-		-	
IOC TYPE	VALUE		
MD5	97cd4fc94c59121f903f2081df1c9981, 28bdd46d8609512f95f1f1b93c79d277, 3e23308d074d8bd4ffdb5e21e3aa8f22, 088779125434ad77f846731af2ed6781, b67f6e534d5cca654813bd9e94a125b9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Rhysida</u>	The Rhysida ransomware-as-a-service (RaaS) group poses a significant global threat, targeting diverse sectors. Recently, researchers developed a decryptor for it, enabling victims of the Rhysida ransomware to recover their encrypted data without any cost.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			PATCH LINK
-		-	
IOC TYPE	VALUE		
SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f, f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab, 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd, 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31efcebf7f6		

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>TinyTurla-NG (TTNG)</u>	TinyTurla-NG (TTNG) is a new backdoor malware developed by the Turla APT group, a Russian cyberespionage group active since at least 2004. It was first discovered in December 2023 targeting a Polish non-governmental organization (NGO).	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Turla			-
IOC TYPE	VALUE		
SHA256	267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b, d6ac21a409f35a80ba9ccfe58ae1ae32883e44ecc724e4ae8289e7465ab2cf40		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>TurlaPower-NG</u>	TurlaPower-NG is a malicious PowerShell script used by the Turla APT group to exfiltrate data from compromised systems. It was discovered in December 2023 and is associated with the TinyTurla-NG backdoor malware. TurlaPower-NG specifically targets files related to password management software, indicating an intent to steal login credentials.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
-			-
	Exfiltrate data and System Compromise		




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>Bumblebee</u>	<p>BumbleBee, a malicious loader discovered in March 2022, resurfaced in the cyber threat landscape on February 8, 2024, after a four-month hiatus.</p> <p>Unlike in previous campaigns, this attack chain diverges from conventional techniques.</p>	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			
ASSOCIATED ACTOR		Data Theft and install other malware	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	c34e5d36bd3a9a6fca92e900ab015aa50bb20d2cd6c0b6e03d070efe09ee689a, 3083ac4480bac3d3b900177ca92afd5ed279279640ac4296cf152e7d30c80d6f, afb75762094c2149d4d5f2312a4b094b34e524747d8d8a8d9e9f132601378a45, e72084687a0e6b9d22bdc51c80870d403645a7e13a1caa2d176acd7a1b10a962, 7140becbc882cab84038ad87e977cd3cb0dc864d2437eb1e2aebab78cc3eb193		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>DarkMe RAT</u>	<p>DarkMe RAT, short for Remote Access Trojan, is a malicious program developed by the Evilnum APT group. It has been in circulation since at least September 2021 and has evolved significantly over time, becoming increasingly sophisticated and dangerous.</p>	Phishing	CVE-2024-21412 CVE-2023-36025
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Data Theft and install other malware	PATCH LINK
Water Hydra (aka DarkCasino)			
IOC TYPE	VALUE		
SHA256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc,		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21351		Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	-
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.002 User Execution: Malicious File, T1553.005 Subvert Trust Controls: Mark-of-the-Web Bypass	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21412		Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	Water Hydra (aka DarkCasino)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	DarkMe RAT
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.001 User Execution: Malicious Link, T1036.008 Masquerading: Masquerade File Type	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-36025</u>		Windows: 10 - 11 23H2 & Windows Server: 2008 - 2022 23H2	Water Hydra (aka DarkCasino)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*	DarkMe RAT and Mispadu infostealer
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.001 User Execution: Malicious Link, T1036.008 Masquerading: Masquerade File Type	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-38831</u>		WinRAR version 6.22 and older versions	APT 28, DarkPink, Konni, APT 40, Sandworm and APT 29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*	BumbleBee, DarkMe, GuLoader, Remcos RAT, SmokeLoader, Nanocore RAT, Crimson RAT, AgentTesla, BOXRAT and Rhadamanthisinfostealer
WinRAR Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1204.001 User Execution: Malicious Link, T1203 : Exploitation for Client Execution	Update WinRAR version to 6.23 or later versions Link: https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21410</u>		Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:2016:cu23:*:*:*:*:*	-
Microsoft Exchange Server Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-668	T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21410


Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Water Hydra (aka DarkCasino)</u>	-	Finance, Cryptocurrency, Forex and Stock trading, Banking, Gambling sites and Casinos	Worldwide
	MOTIVE		
	Financial gain and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DarkMe RAT	Windows
TTPs			
TA0001: Initial Access ; TA0010: Exfiltration ; TA0004: Privilege Escalation ; TA0042: Resource Development ; T1566.002: Spearphishing Link ; T1566: Phishing ; T1204: User Execution ; T1204.001: Malicious Link; T1105: Ingress Tool Transfer ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow ; T1588.006: Vulnerabilities; T1588: Obtain Capabilities ; T1588.005: Exploits ; T1559: Inter-Process Communication ; T1559.001: Component Object Model; T1218: System Binary Proxy Execution; T1218.011: Rundll32 ; T1547.001:Registry Run Keys /Startup Folder; T1547: Boot or Logon Autostart Execution ; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell ; T1585: Establish Accounts ; T1585.001: Social Media Accounts; T1586: Compromise Accounts ; T1586.001: Social Media Accounts ; T1584: Compromise Infrastructure ; T1584.004: Server; T1211: Exploitation for Defense Evasion ; T1218.007 : Msiexec; T1140: Deobfuscate/Decode Files or Information ; T1027: Obfuscated Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Volt Typhoon (aka Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, Insidious Taurus)</u></p>	China	Communications, Energy, Transportation Systems, Water and Wastewater Systems, Emergency management services, Telecommunications, Satellite services, and Defense	United States, Canada, Australia, New Zealand, and African countries
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	TARGETED CVEs		
-	-	-	

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; T1592: Gather Victim Host Information; T1589: Gather Victim Identity Information; T1589.002: Email Addresses; T1590: Gather Victim Network Information; T1591: Gather Victim Org Information; T1593: Search Open Websites/Domains; T1594: Search Victim-Owned Websites; T1583.003: Botnet; T1584.005: Botnet; T1584.004: Server; T1587.004: Exploits; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.004: Unix Shell; T1047: Windows Management Instrumentation; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1006: Direct Volume Access; T1070.009: Clear Persistence; T1070.001: Clear Windows Event Logs; T1070.004: File Deletion; T1036.005: Match Legitimate Name or Location; T1112: Modify Registry; T1027.002: Software Packing; T1218: System Binary Proxy Execution; T1110.002: Password Cracking; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1003.001: LSASS Memory; T1003.003: NTDS; T1552: Unsecured Credentials; T1552.004: Private Keys; T1087.001: Local Account; T1010: Application Window Discovery; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1654: Log Enumeration; T1046: Network Service Discovery; T1120: Peripheral Device Discovery; T1069: Permission Groups Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1082: System Information Discovery; T1614: System Location Discovery; T1016.001: Internet Connection Discovery; T1033: System Owner/User Discovery; T1007: System Service Discovery; T1124: System Time Discovery; T1563: Remote Service Session Hijacking; T1021.007: Cloud Services; T1021.001: Remote Desktop Protocol; T1550: Use Alternate Authentication Material; T1078.004: Cloud Accounts; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1074: Data Staged; T1113: Screen Capture; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1090: Proxy; T1090.001: Internal Proxy; T1090.003: Multi-hop Proxy; T1048: Exfiltration Over Alternative Protocol

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa)</u></p>	Russia	Finance, Cryptocurrency, Forex and Stock trading, Banking, Gambling sites and Casinos	Poland
	MOTIVE		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	TinyTurla-NG (TTNG) and TurlaPower-NG	-
TTPs			
<p>TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1070: Indicator Removal; T1566: Phishing; T1102: Web Service; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1083: File and Directory Discovery; T1056: Input Capture; T1560: Archive Collected: Data; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1552: Unsecured Credentials; T1552.004: Private Keys; T1555: Credentials from Password Stores; T1555.005: Password Managers</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 actors **Water Hydra, Volt Typhoon, Turla** and malware **Coyote, Zardoor, RustDoor, Rhysida Ransomware, TinyTurla-NG (TTNG), TurlaPower-NG, Bumblebee Loader** and **DarkMe 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 **five exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Turla, Volt Typhoon**, and malware **Coyote, Zardoor, RustDoor, Rhysida Ransomware, Bumblebee Loader** in Breach and Attack Simulation(BAS).

Threat Advisories

[Coyote: A Sophisticated Banking Trojan Targeting Financial Information](#)

[The Zardoor Backdoor's Silent Takeover of Saudi Charities](#)

[New Backdoor Masquerading as a Software Update Agent, Targets macOS](#)

[Microsoft's February 2024 Patch Tuesday Addresses Two Zero-day Vulnerabilities](#)

[Rhysida Ransomware's Decryptor is Now in Action](#)

[Critical Flaw in Zoom Windows Apps Allows Privilege Elevation](#)

[Water Hydra Exploits CVE-2024-21412 to Target Financial Traders](#)

[Turla Expands Their Arsenal with Next-Generation Malwares](#)

[A Fresh Look at the Bumblebee's Comeback Strategies](#)

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>Coyote</u>	MD5	03eaccb664d517772a33255dff96020, 071b6efd6d3ace1ad23ee0d6d3eead76, 276f14d432601003b6bf0caa8cd82fec, 5134e6925ff1397fdda0f3b48afec87b, Bf9c9cc94056bcdae6e579e724e8dbbd
<u>Zardoor backdoor</u>	SHA256	f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a6 0ef585bd2ac2, c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a2 18e7735561ef74, 73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c 5d8cd73083095, a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e 3407bc01f661d, 0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b 73c208ab723bf, d267e2a6311fe4e2dfd0237652223add300b9a5233b555e131 325a2612e1d7ef
	Mutexes	3e603a07-7b2d-4a15-afef-7e9a0841e4d5, 6c2711b5-e736-4397-a883-0d181a3f85ae, ThreadMutex12453
	IPv4:Port	70[.]34[.]208[.]197:10086, 140[.]82[.]33[.]130:14443, 70[.]34[.]194[.]185:14443, 139[.]84[.]232[.]245:37135, 208[.]85[.]20[.]130:37135, 139[.]84[.]229[.]192:443,

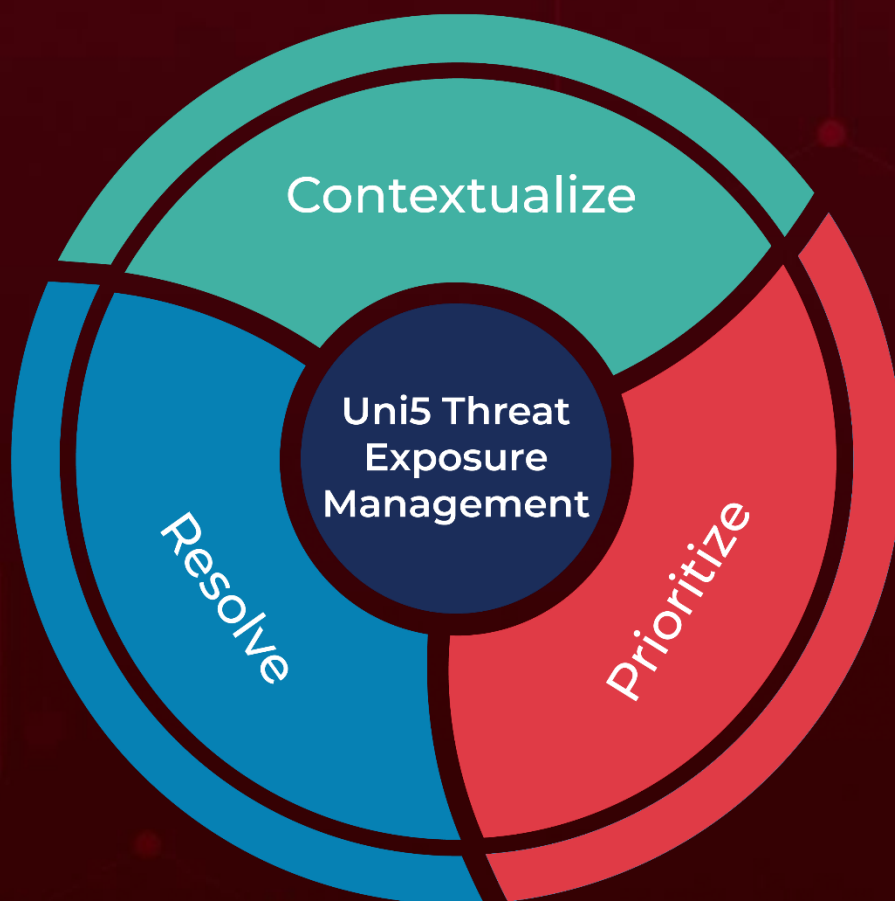
Attack Name	TYPE	VALUE
<u>Zardoor backdoor</u>	IPv4:Port	70[.]34[.]195[.]221:443, 217[.]69[.]1[.]128:14443, 108[.]181[.]20[.]36:443, 108[.]61[.]189[.]125:443
<u>RustDoor</u>	MD5	97cd4fc94c59121f903f2081df1c9981, 28bdd46d8609512f95f1f1b93c79d277, 3e23308d074d8bd4ffdb5e21e3aa8f22, 088779125434ad77f846731af2ed6781, b67f6e534d5cca654813bd9e94a125b9, cf54cba05efee9e389e090b3fd63f89b, 44fcf7253bcf0102811e50a4810c4e41, 690a097b0eea384b02e013c1c0410189, 186be45570f13f94b8de82c98eaa8f4f, 3c780bcfb37a1dfae5b29a9e7784cbf5, 925239817d59672f61b8332f690c6dd6, 9c6b7f388abec945120d95d892314ea7, 85cd1afb026ffdf4cd3eec038c3185, 6aaba581bcef3ac97ea98ece724b9092, bcbbf7a5f7ccff1932922ae73f6c65b7, bde0e001229884404529773b68bb3da0, 795f0c68528519ea292f3eb1bd8c632e, bc394c859fc379900f5648441b33e5fd, 0fe0212fc5dc82bd7b9a8b5d5b338d22, 835ebf367e769eeaaef78ac5743a47ca, bdd4972e570e069471a4721d76bb5efb
<u>TinyTurla-NG</u>	SHA256	267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdc df6e6a453b, d6ac21a409f35a80ba9ccfe58ae1ae32883e44ecc724e4ae8289e74 65ab2cf40
	Domains	anagram[.]jpp, thefinetreats[.]com, caduff-sa[.]ch, jeepcarlease[.]com, buy-new-car[.]com
<u>Bumblebee</u>	SHA256	c34e5d36bd3a9a6fca92e900ab015aa50bb20d2cd6c0b6e03d070ef e09ee689a, 3083ac4480bac3d3b900177ca92afd5ed279279640ac4296cf152e7 d30c80d6f, afb75762094c2149d4d5f2312a4b094b34e524747d8d8a8d9e9f132 601378a45, e72084687a0e6b9d22bdc51c80870d403645a7e13a1caa2d176acd 7a1b10a962, 7140becbc882cab84038ad87e977cd3cb0dc864d2437eb1e2aebab 78cc3eb193, 7f312a38cf00246fafd23684e7c80600f95c191bab7470e54836ce0e 73fa86dd, ecc93d6cab4d59db2a75ba3ce5bbcaac048d44153973df4d13216c5 df74f8d33,

Attack Name	TYPE	VALUE
<u>Bumblebee</u>	SHA256	a5b39fc06464b347af81f13c5994c2bcef15001b35b4e78e4f4677ea b858cb1d, 8695f4936f2942d322e2936106f78144f91602c7acace080e48c97e9 7b888377, f5eb4c8c087cc070b23ebbd5b58c781e843436932a10fae1966c642 a0ef83820
	URL	hxxp[:]://213[.]139.205.131/w_ver.dat
	Domain	q905hr35[.]life
	IPv4:Port	49.13.76[.]144:443
<u>Rhysida Ransomware</u>	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c4 1b8cd3c6, 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3 ae706f, f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724f a06fbab, 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0a d62da71cd, 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31e fceb7f6, 3d2013c2ba0aa1c0475cab186ddf3d9005133fe5f88b5d8604b4667 3b96a40d8, 67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d 9401928ba5, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738 546c2ab1, 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cb a746f05595, 3518195c256aa940c607f8534c91b5a9cd453c7417810de3cd4d262 e2906d24f, d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4 d5320ee
<u>DarkMe RAT</u>	SHA256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e 8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e1989 0b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce37 91bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307 ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c8 39b1d02bc, b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a35 1d40422feb, bf9c3218f5929dfecbbdc0ef421282921d6cbc06f270209b9868fc73 a080b8c, dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f 3f5ecf54

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

February 19, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com