

Date of Publication
March 11, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

4 to 10 MARCH 2024

Table Of Contents

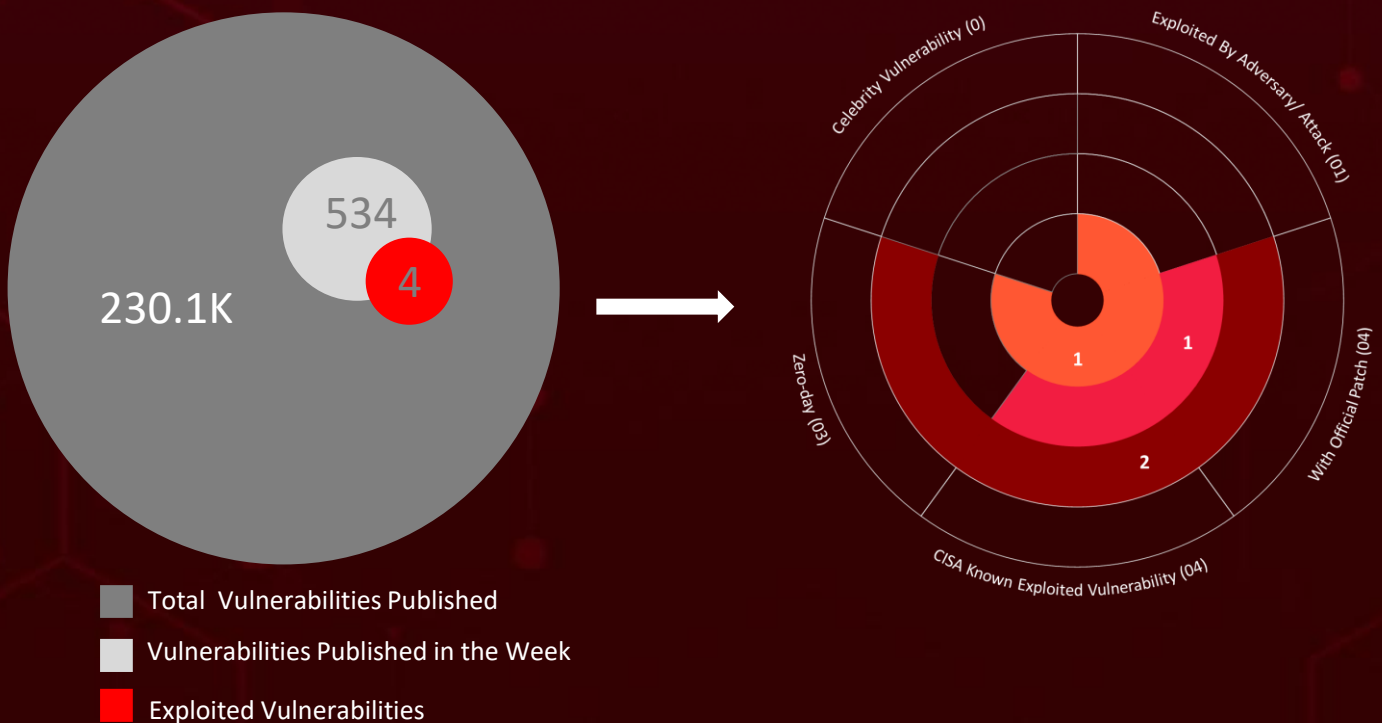
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	21

Summary

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

Furthermore, HiveForce Labs revealed that **two zero-day** exploited vulnerabilities have been addressed by Apple. Two vulnerabilities in the JetBrains TeamCity On-Premises software have been discovered (**CVE-2024-27198** and **CVE-2024-27199**). Threat actors may attempt to take advantage of these vulnerabilities in order to breach and gain control of the impacted systems, leading to system compromise.

The **CHAVECLOAK**, a new banking trojan, is purposefully crafted to target the banking credentials of individuals in Brazil, highlighting the ongoing focus of cybercriminals on the nation's financial sector. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

7

Attacks
Executed

4

Vulnerabilities
Exploited

2

Adversaries in
Action

- [Bifrost](#)
- [Pikabot](#)
- [CHAVECLOAK](#)
- [WogRAT](#)
- [GhostLocker](#)
- [Stormous](#)
- [SapphireStealer](#)

- [CVE-2024-27198](#)
- [CVE-2024-23225](#)
- [CVE-2024-23296](#)
- [CVE-2022-26134](#)

- [TA577](#)
- [TA4903](#)



Insights

Bifrost

Evades detection using a deceptive VMware domain, aiming to compromise systems

JetBrains TeamCity

CVE-2024-27198 and CVE-2024-27199 Threat actors exploiting these vulnerabilities in order to breach and gain control of the impacted systems

WogRAT

A backdoor malware targeting both Windows and Linux, spreads through aNotepad

Apple 0-days

CVE-2024-23225 and CVE-2024-23296 zero-day vulnerabilities were found in iOS, exploited in attacks targeting Mobile devices, providing attackers with arbitrary kernel read and write privileges

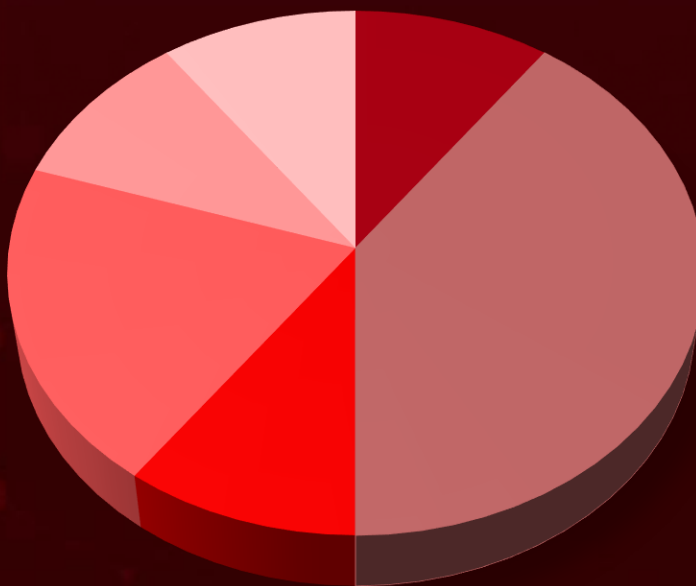
TA577

A significant cyber threat group, has shifted tactics to steal NTLM authentication data, utilizing thread hijacking and customized HTML attachments

CHAVECLOAK

Banking trojan is purposefully crafted to target the banking credentials of individuals in Brazil

Threat Distribution



■ RAT ■ Loader ■ Trojan ■ Backdoor ■ Ransomware ■ Information stealer

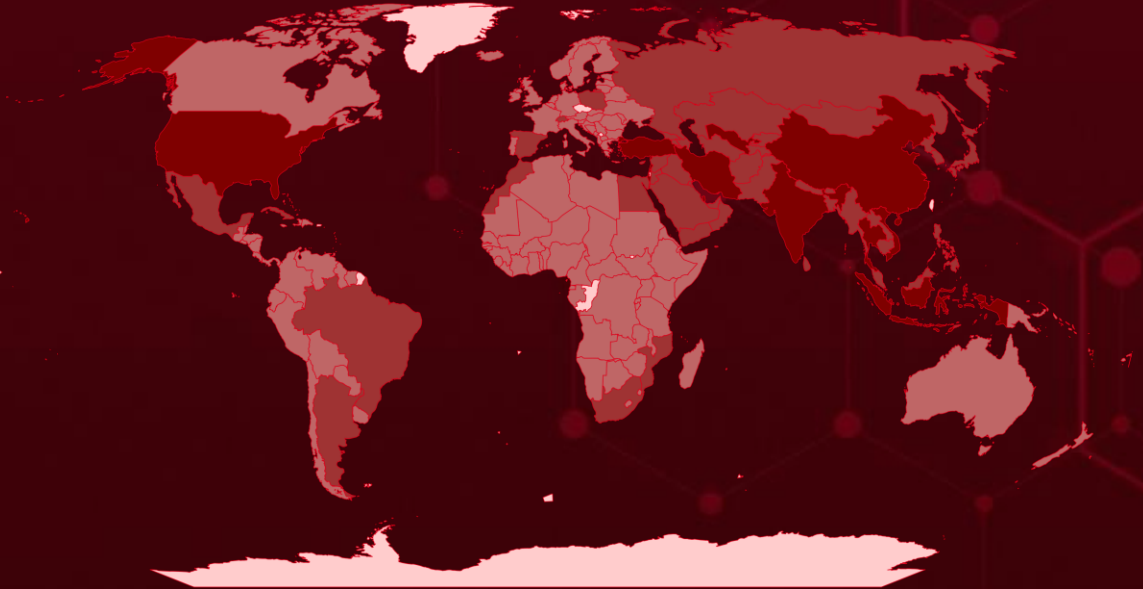


Targeted Countries

Most



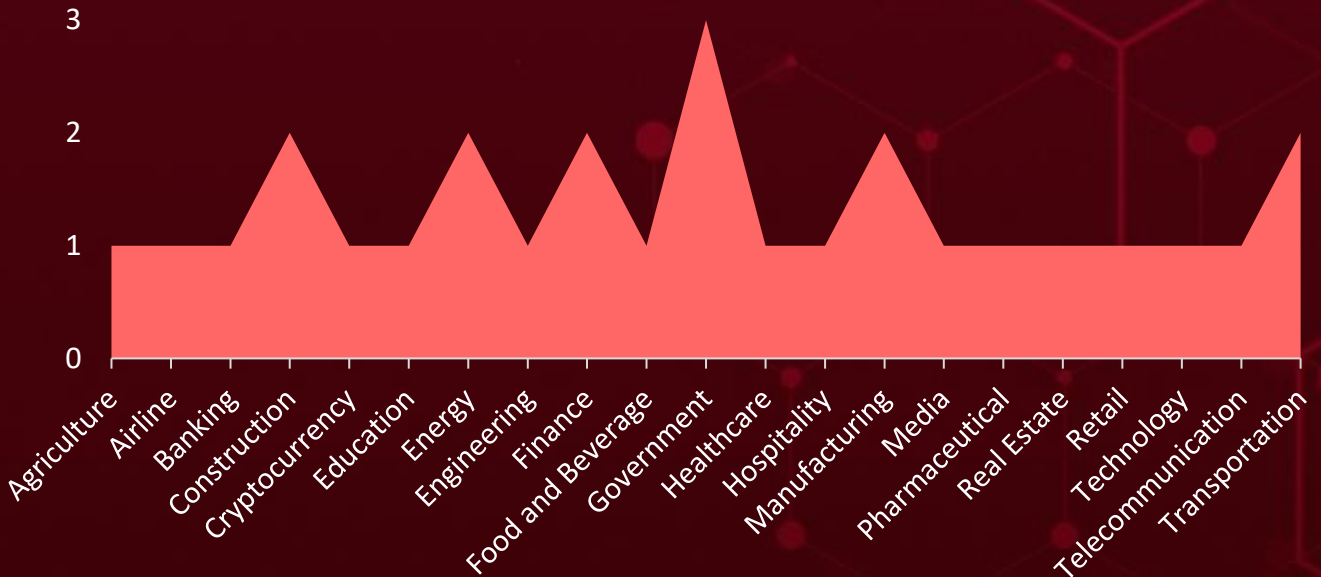
Least



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

Countries	Countries	Countries	Countries
United States	Iraq	Argentina	Estonia
Turkey	South Korea	Morocco	Grenada
Qatar	Bangladesh	Cuba	North Macedonia
China	Switzerland	Mozambique	Guatemala
Lebanon	Japan	United Arab Emirates	Peru
India	Timor-Leste	Myanmar	Guinea
Vietnam	Jordan	Nepal	Saint Kitts & Nevis
Indonesia	Cyprus	Maldives	Guinea-Bissau
Thailand	Kazakhstan	Yemen	Seychelles
Iran	Oman	Mexico	Guyana
Israel	Kuwait	Afghanistan	Denmark
Uzbekistan	Philippines	Fiji	Haiti
Singapore	Kyrgyzstan	Slovenia	Sweden
North Korea	Cambodia	Côte d'Ivoire	Holy See
Tajikistan	Laos	Gambia	Tonga
Egypt	Saudi Arabia	Tanzania	Honduras
Poland	Bhutan	Barbados	Eswatini
Georgia	South Africa	Palau	Hungary
Sri Lanka	Malaysia	Germany	France
Armenia	Spain	Sao Tome & Principe	Iceland
Turkmenistan	Brazil	Ghana	Colombia
Azerbaijan	State of Palestine	St. Vincent & Grenadines	Belarus
Pakistan	Brunei		Papua New Guinea
Bahrain	Syria		Guinea
Russia	Mongolia		Belgium

Targeted Industries



TOP MITRE ATT&CK TTPs

T1036

Masquerading

T1566

Phishing

T1059

Command and Scripting Interpreter

T1204.002

Malicious File

T1204

User Execution

T1083

File and Directory Discovery

T1588.006

Vulnerabilities

T1588

Obtain Capabilities

T1068

Exploitation for Privilege Escalation

T1027

Obfuscated Files or Information

T1574.002

DLL Side-Loading

T1055

Process Injection

T1555

Credentials from Password Stores

T1082

System Information Discovery

T1203

Exploitation for Client Execution

T1498

Network Denial of Service

T1218

System Binary Proxy Execution

T1071.001

Web Protocols

T1041

Exfiltration Over C2 Channel

T1588.005

Exploits

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Bifrost (aka Bifrose)</u>	A new Linux variant of the Bifrost RAT evades detection using a deceptive VMware domain, aiming to compromise systems. This persistent threat spreads through malicious emails and sites, harvesting sensitive data and now includes an ARM version, emphasizing the need for vigilant countermeasures to safeguard against evolving malware.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
RAT				Linux
ASSOCIATED ACTOR				PATCH LINK
-		System Disruption	-	
IOC TYPE	VALUE			
SHA256	8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00250a4a2fe4729, 2aeb70f72e87a1957e3bc478e1982fe608429cad4580737abe58f6d78a626c05			
IPv4	45.91.82[.]127			
Domain	download.vmfare[.]com			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Pikabot</u>	Pikabot is a sophisticated piece of multi-stage malware with a loader and core module within the same file. Pikabot, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Loader				-
ASSOCIATED ACTOR				PATCH LINK
TA577		Data Theft, Downloading other malware	-	
IOC TYPE	VALUE			
SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8			

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>CHAVECLOAK</u>	The CHAVECLOAK banking trojan is purposefully crafted to target the banking credentials of individuals in Brazil, highlighting the ongoing focus of cyber criminals on the nation's financial sector.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Financial gain and Data Theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4, 48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028, 4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006, 131d2aa44782c8100c563cd5feb49fcb4d26952d7e6e2ef22f805664686ffff, 8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>WogRAT</u>	WogRAT, a backdoor malware targeting both Windows and Linux, spreads through aNotepad, an online notepad service. It disguises itself as system tools to trick users into downloading it, mainly targeting users in Asia.	Via aNotepad	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	Windows and Linux
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	290789ea9d99813a07294ac848f808c9, 1aebf536268a9ed43b9c2a68281f0455, 194112c60cb936ed1c195b98142ff49d, 1341e507f31fb247c07beeb14f583f4f, fff21684df37fa7203ebe3116e5301c1		

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>GhostLocker</u>	GhostLocker is ransomware-as-a-Service (RaaS) - developed by the hacktivist group GhostSec, it's now offered to other cybercriminals for a fee. It's features are military-grade encryption, self-deletion to avoid detection, and even attempts to escalate privileges to gain more control over your system.	Phishing	-
TYPE		IMPACT Data Theft and System Disruption	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f, 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f443779e9,		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Stormous</u>	Stormous ransomware primarily known for deploying ransomware attacks, often targeting Western companies and organizations. It has been partnered with other hacking groups like GhostSec, forming the "Five Families" alliance. This collaboration allows them to launch more complex attacks.	Phishing	-
TYPE		IMPACT Data Theft and System Disruption	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f, 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f443779e9,		




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>SapphireStealer</u>	SapphireStealer is a information-stealing malware. It runs on Windows and steals logins, browsing data, screenshots, and specific files. As it's open-source, it's easy to customize and new versions are constantly emerging, making it difficult to detect.	various public malware repositories	-
TYPE		IMPACT	AFFECTED PRODUCTS
Info stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Data Theft	-
IOC TYPE	VALUE		
SHA256	850a99d2039dadb0c15442b40c90aa4dac16319114455ab5904aa51e062fe6e1, c816d0be8d180573d14d230b438a22d7dda6368b1ef1733754eda9804f295a2f		
SHA1	6b44ab6c246c077ee0e6f51300654b3eec2fddc7, b396a8d5e30fb179f3139d28b843b57bb8ae3f47		
MD5	5c025a9e86a125bf2f2ca5c1b29b42a6, 55bb772aea4303ca373fd8940663b6bd		




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-2024-27198		TeamCity On-Premises versions upto 2023.11.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:TeamCity:*:*:*:*:*	-
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1556 : Modify Authentication Process, T1190 : Exploit Public-Facing Application	https://www.jetbrains.com/teamcity/download/


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23225		iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:*:*:*:*:*	-
Apple iOS and iPadOS Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1211 : Exploitation for Defense Evasion, T1106 : Native API	https://support.apple.com/en-us/HT214081 ; https://support.apple.com/en-us/HT214082

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23296		iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Apple iOS and iPadOS Memory Corruption Vulnerability		cpe:2.3:a:apple:*.:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1211 : Exploitation for Defense Evasion, T1106 : Native API	https://support.apple.com/en-us/HT214081 ; https://support.apple.com/en-us/HT214082

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134		Atlassian Confluence Server and Data Center	APT 28, DarkPink, Konni, APT 40, Sandworm and APT 29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*.:*:*:*:*:*	AvosLocker ransomware
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1190 : Exploit Public-Facing Application, T1203 : Exploitation for Client Execution	https://www.atlassian.com/software/confluence/download-archives

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>TA577</u>	-	-	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Pikabot	Windows
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0008: Lateral Movement, TA0003: Persistence, TA0005: Defense Evasion, TA0006: Credential Access, T1021.002: SMB/Windows Admin Shares, T1021: Remote Services, T1566.001: Spearphishing Attachment, T1566: Phishing, T1204.002: Malicious File, T1204: User Execution, T1555: Credentials from Password Stores, T1574: Hijack Execution Flow , T1555.004: Windows Credential Manager			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA4903	-	Government, Construction, Healthcare, Manufacturing, Energy, Finance, Agriculture, Transportation, Commerce, Food and Beverage	United States of America
	MOTIVE		
	Financial gain	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0040: Impact, TA0003: Persistence, TA0005: Defense Evasion, TA0006: Credential Access, T1021.002: SMB/Windows Admin Shares, T1021: Remote Services, T1566.001: Spearphishing Attachment, T1566: Phishing, T1204.002: Malicious File, T1204: User Execution, T1555: Credentials from Password Stores, T1574: Hijack Execution Flow , T1555.004: Windows Credential Manager			

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 **TA577, TA4903** and malware **Bifrost, Pikabot, CHAVECLOAK, WogRAT, GhostLocker, Stormous, SapphireStealer**.

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 **TA577, TA4903** and malware **Bifrost, CHAVECLOAK, WogRAT, GhostLocker, Stormous, SapphireStealer** in Breach and Attack Simulation(BAS).

Threat Advisories

[New Linux Variant of Bifrost RAT Utilizes Deceptive Domain for Evasion](#)

[Critical Vulnerabilities Discovered in TeamCity, Enable Server Takeover](#)

[TA577 Targeting Windows NTLM Hashes in Global Campaigns](#)

[CHAVECLOAK Banking Trojan Sneaks into Brazil's Financial Hub](#)

[Apple Rolls Out Critical Updates to Address Zero-Day Flaws](#)

[WogRAT Backdoor Poses Risk to Windows and Linux Users](#)

[GhostSec and Stormous Join Forces for a Ransomware Blitz](#)

[Misconfigured Servers Targeted with New Golang Malware](#)

[SapphireStealer's Stealthy Invasion via Deceptive Legal Documents](#)

[TA4903 Spoofing Government Entities and SMBs for Financial Gain](#)

[Critical VMware Vulnerabilities Leading To Sandbox Escape](#)

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>Bifrost</u>	SHA256	8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00250a4a2fe4729, 2aeb70f72e87a1957e3bc478e1982fe608429cad4580737abe58f6d78a626c05
	IPv4	45.91.82[.]127
	Domain	download.vmfare[.]com
<u>Pikabot</u>	SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8
<u>CHAVECL OAK</u>	SHA256	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4, 48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028, 4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006, 131d2aa44782c8100c563cd5febfb49fcb4d26952d7e6e2ef22f805664686ffff, 8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c, 634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9, 2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55

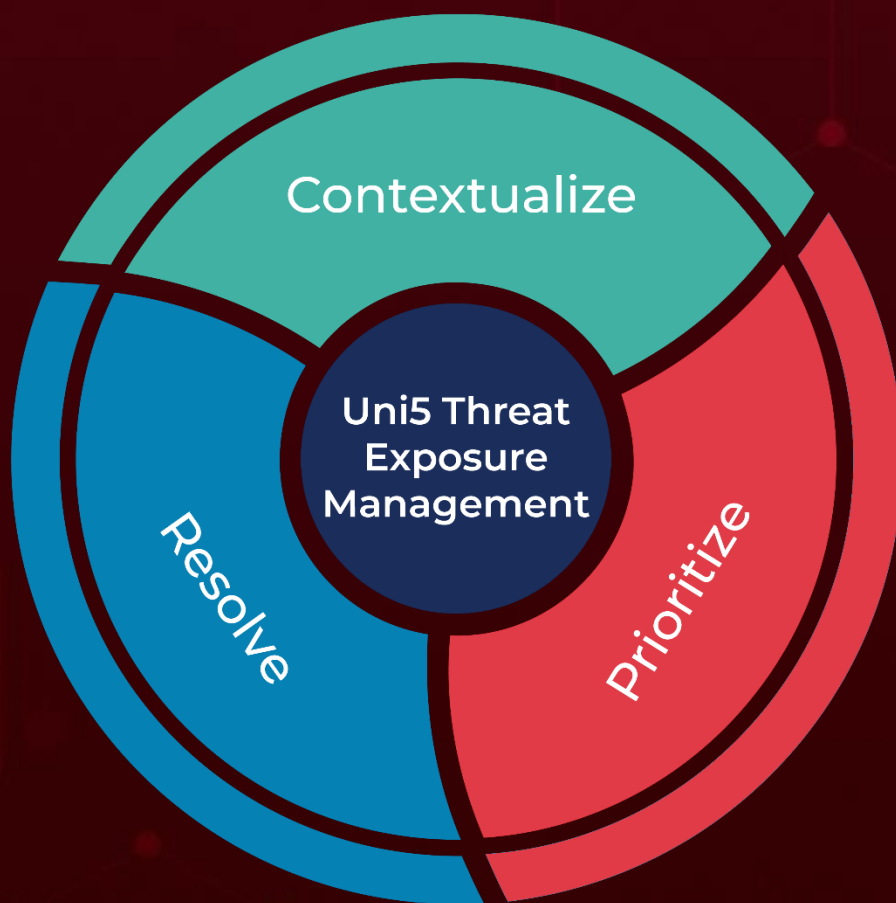
Attack Name	TYPE	VALUE
<u>CHAVECLOAK</u>	URLs	hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrwEWGFG09t5H6854JHGJUUR[.].zip, hxxps://goo[.]su/FTD9owO
	Domains	mariashow[.]ddns[.]net, comunidadebet20102[.]hopto[.]org
<u>WogRAT</u>	Domains	w.linuxwork[.]net, linuxwork[.]net
	MD5	290789ea9d99813a07294ac848f808c9, 1aebf536268a9ed43b9c2a68281f0455, 194112c60cb936ed1c195b98142ff49d, 1341e507f31fb247c07beeb14f583f4f, fff21684df37fa7203ebe3116e5301c1, f97fa0eb03952cd58195a224d48f1124, f271e0ae24a9751f84c5ae02d29f4f0e, e9ac99f98e8fbd69794a9f3c5afdcb52, da3588a9bd8f4b81c9ab6a46e9cddedd, a35c6fbe8985d67a69c918edcb89827e, 929b8f0bdbb2a061e4cf2ce03d0bbc4c, 7bcfea3889f07f1d8261213a77110091, 655b3449574550e073e93ba694981ef4, 5769d2f0209708b4df05aec89e841f31, 3669959fdb0f83239dba1a2068ba25b3
	URLs	hxxps://t0rguard[.]net/c/ hxxps://w.newujs[.]com/c/ hxxps://newujs[.]com/tt.php?fuckyou=1, hxxp://newujs[.]com/ddddd_o, hxxp://newujs[.]com/abc, hxxp://newujs[.]com/a14407a2, hxxps://js.domaiso[.]com/jquery.min-2.js, hxxps://jp.anotepad[.]com/note/read/b896abi9, hxxp://newujs[.]com/cff/wins.jpg
<u>GhostLocker</u>	SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282e b24b7c55f, 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f4 43779e9,
<u>Stormous</u>	SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282e b24b7c55f, 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f4 43779e9,
	MD5	b15a8047abd9a3af013cf6c77ce15acf
	SHA1	aa62afd6a48d3c42ed66d4f5b9189be847ec055b

Attack Name	TYPE	VALUE
<u>SapphireStealer</u>	SHA256	850a99d2039dadb0c15442b40c90aa4dac16319114455ab5904aa51e062fe6e1, c816d0be8d180573d14d230b438a22d7dda6368b1ef1733754eda9804f295a2f
	SHA1	6b44ab6c246c077ee0e6f51300654b3eec2fddc7, b396a8d5e30fb179f3139d28b843b57bb8ae3f47
	MD5	5c025a9e86a125bf2f2ca5c1b29b42a6, 55bb772aea4303ca373fd8940663b6bd

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

March 11, 2024 • 3:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com