Date of Publication
January 29, 2024

Hive Pro®

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

22 to 28 JANUARY 2024

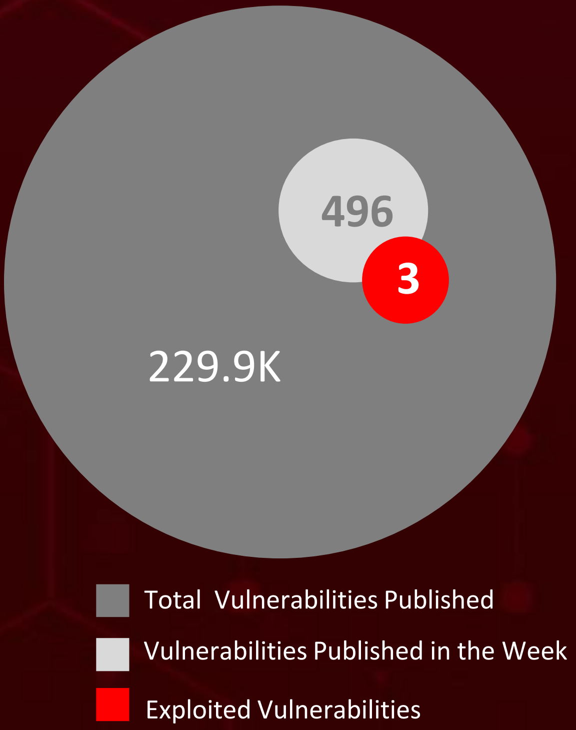
Table Of Contents

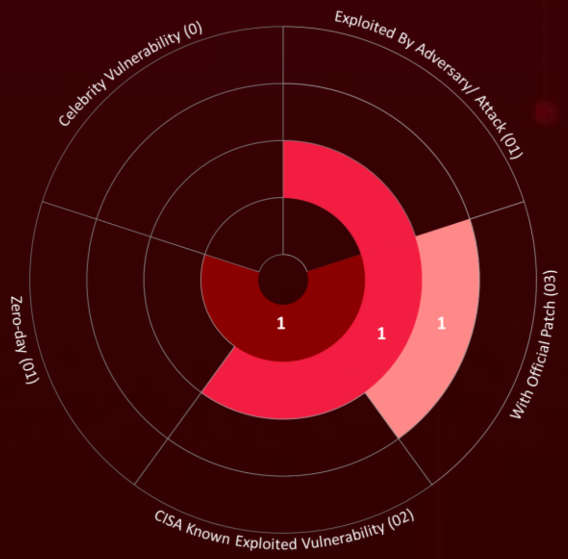
Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **eight** executed attacks, **three** instances of adversary activity, and **three** exploited vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered Financial gain group **TA866**, returned after a hiatus of nine months, launching a new extensive phishing campaign aimed at distributing malwares WasabiSeed and Screenshotter.

Meanwhile, a critical zero-day vulnerability (**CVE-2023-22527**), in Atlassian Confluence that is a critical Remote Code Execution vulnerability which is actively exploited by malicious actors. Nearly 40,000 exploitation attempts have been recorded.





High Level Statistics

8
Attacks Executed

3
Vulnerabilities Exploited

3
Adversaries in Action

- WasabiSeed
- Screenshotter
- Zloader
- RokRAT backdoor
- NS-STEALER
- Kasseika ransomware
- AsyncRAT
- VenomRAT

- CVE-2024-23222
- CVE-2023-22527
- CVE-2024-0204

- TA866
- TA571
- ScarCruft

Insights

Zloader

Resurges after a pause of nearly two years, with fresh iteration that began development in September 2023

Apple's First Zero-Day

CVE-2024-23222 vulnerability in Apple's WebKit is being actively exploited, which results in arbitrary code execution, posing a severe threat to the security and control of multiple Apple Products

CVE-2024-0204

Flaw in Fortra GoAnywhere MFT which allows attackers to become Admins

Kasseika Ransomware

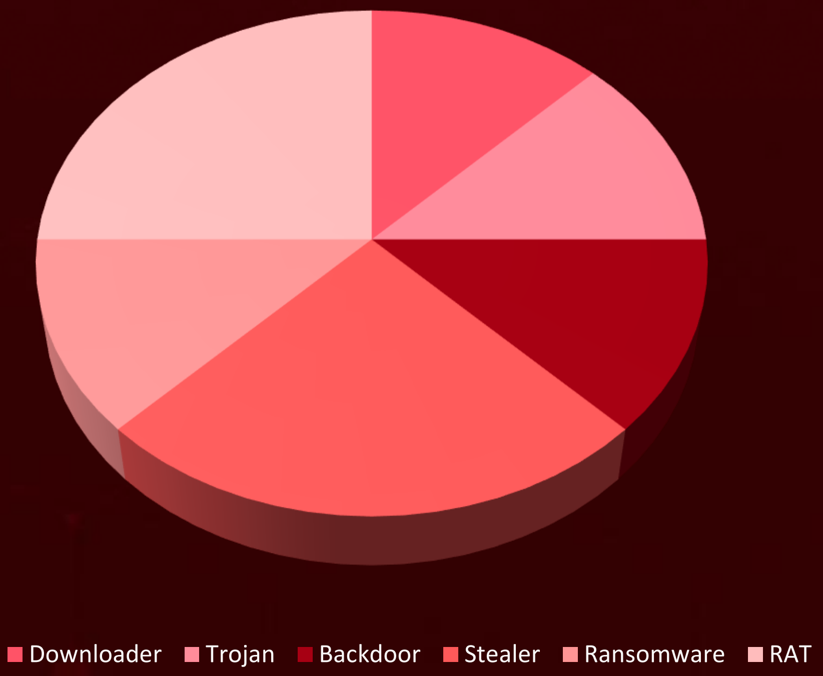
was found leveraging the Martini driver to terminate antivirus related processes on the victim's machine

TA866 Makes a come back after nine months with the email phishing campaigns distributing well-known malware families like WasabiSeed and Screenshotter

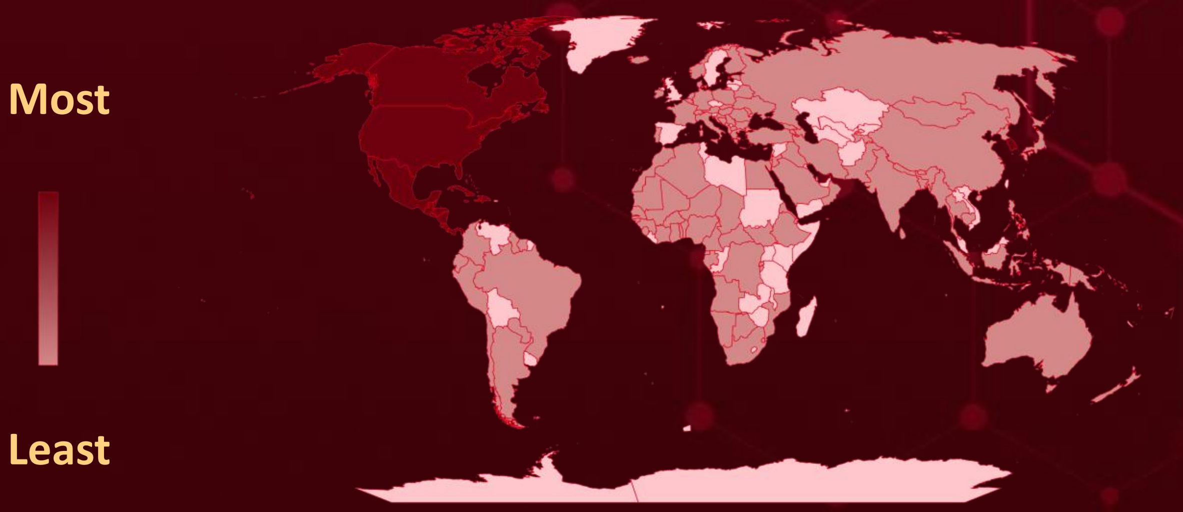
CVE-2023-22527

A critical Remote Code Execution vulnerability in outdated Atlassian Confluence versions, actively exploited by malicious actors

Threat Distribution



Targeted Countries



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

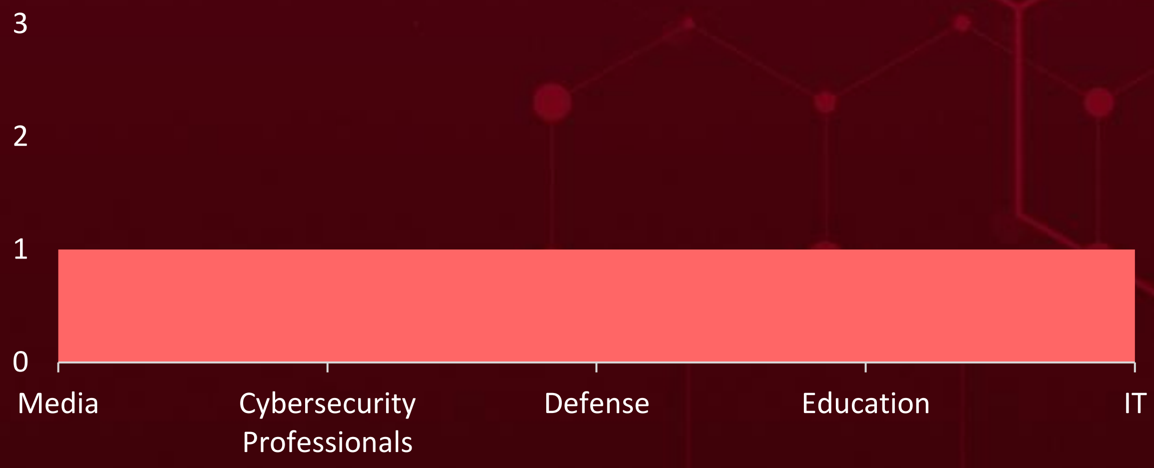
	Countries
■	Jamaica
■	Grenada
■	Saint Lucia
■	Antigua and Barbuda
■	Haiti
■	Bahamas
■	Nicaragua
■	Barbados
■	Trinidad and Tobago
■	Belize
■	Guatemala
■	Canada
■	Honduras
■	Costa Rica
■	Mexico
■	Cuba
■	Panama
■	Dominica
■	South Korea
■	Dominican Republic
■	El Salvador

	Countries
■	United States
□	Saudi Arabia
□	Mozambique
□	Tuvalu
□	Brazil
□	Benin
□	Brunei
□	State of Palestine
□	Bulgaria
□	Mauritius
□	Burkina Faso
□	Niger
□	Burundi
□	Romania
□	Cabo Verde
□	Solomon Islands
□	Cambodia
□	Thailand
□	Cameroon
□	Mali
□	Albania
□	Monaco

	Countries
□	Central African Republic
□	Nepal
□	Chad
□	Norway
□	Chile
□	Philippines
□	China
□	Bhutan
□	Colombia
□	Sierra Leone
□	Comoros
□	South Sudan
□	Congo
□	Switzerland
□	Argentina
□	Bosnia and Herzegovina
□	Côte d'Ivoire
□	Botswana
□	Croatia
□	Marshall Islands
□	Armenia

	Countries
□	Turkey
□	France
□	Ukraine
□	Gabon
□	Maldives
□	Turkey
□	France
□	Ukraine
□	Maldives
□	Turkey
□	France
□	Ukraine
□	Maldives
□	Turkey
□	Iceland
□	India
□	Peru
□	Indonesia
□	Poland
□	Iran
□	Qatar
□	Iraq
□	Russia

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1204** User Execution	**T1041** Exfiltration Over C2 Channel	**T1105** Ingress Tool Transfer
T1036 Masquerading	**T1518** Software Discovery	**T1203** Exploitation for Client Execution	**T1588** Obtain Capabilities	**T1562** Impair Defenses
T1588.005 Exploits	**T1588.006** Vulnerabilities	**T1211** Exploitation for Defense Evasion	**T1059.006** Python	**T1543** Create or Modify System Process
T1057 Process Discovery	**T1204.002** Malicious File	**T1068** Exploitation for Privilege Escalation	**T1083** File and Directory Discovery	**T1190** Exploit Public-Facing Application

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WasabiSeed	WasabiSeed is a simple VBS downloader which repeatedly to connect to the C2 server looking for payload to download and run.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Downloads and executes a MSI file	-
Downloader			
ASSOCIATED ACTOR			PATCH LINK
TA866, TA571			-

IOC TYPE	VALUE
SHA256	29e447a6121dd2b1d1221821bd6c4b0e20c437c62264844e8bcbb9d4be35f013, 292344211976239c99d62be021af2f44840cd42dd4d70ad5097f4265b9d1ce01

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
Screenshotter	Screenshotter has a single purpose of taking a screenshot of the victim's screen and sending it to the command and control (C2) server.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Take Screenshots	-
ASSOCIATED ACTOR			**PATCH LINK**
TA866, TA571			-

IOC TYPE	VALUE
SHA256	02049ab62c530a25f145c0a5c48e3932fa7412a037036a96d7198cc57cef1f40, d0a4cd67f952498ad99d78bc081c98afbef92e5508daf723007533f000174a98, 6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc, 322dccd18b5564ea000117e90dafc1b4bc30d256fe93b7cfd0d1bdf9870e0da6

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Zloader	Zloader is a trojan designed to steal cookies, passwords and sensitive information. The main audience of this piece of malware are users of financial institutions worldwide.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55, 16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d, 25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d, 2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456, 83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3

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
RokRAT backdoor	It is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode. It is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
ScarCruft			-

IOC TYPE	VALUE
SHA256	79c9f770470510034e29ef80d8d7e894ba65bdbff5bdf603c31559b1f0ab67fd, 1fb020554ae92ddc57622e53f61b05cfeab901ed8c4ca80af015eeff7ef59c8e, 48358a167e2697c6c86086505e714f4bc32655fecf59f97d3d34a13f93091e67, 67dd5d076d301e61256bb0558d23c118a71491081a019a88a7aab54c13084af6, 54ea66fc97a35c8bc37bff02bb8c94c28449fe7ee53d6bdb0310a5c5a569d2e7

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NS-STEALER	It is a Java-based information stealer, spreads through cracked software ZIP files. It utilizes JDABuilder Classes to create an instance of an EventListener for easy registration, and the stealer uses a Discord bot channel as part of its EventListener functionality.	ZIP archives that disguise cracked software	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10, 3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4, 3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f, 9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113, 3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Kasseika ransomware</td><td rowspan="6">The Kasseika ransomware is a 32-bit Windows PE file packed by Themida. Before encryption, Kasseika terminates all processes and services that are currently accessing Windows Restart Manager.</td><td>Phishing emails</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Data theft</td><td rowspan="2">-</td></tr>
<tr><td>Ransomware</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7,
63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196,
3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa,
cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37,
c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">AsyncRAT</td><td rowspan="6">AsyncRAT is a remote access trojan released in 2019, primarily as a credential stealer and loader for other malware, including ransomware. AsyncRAT has botnet capabilities and C2 interface allowing operators to control infected hosts remotely.</td><td>Phishing</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Remotely record a target’s screen, Import and execute additional malware, Exfiltrate files on an infected system</td><td rowspan="2">-</td></tr>
<tr><td>RAT</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3,
398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a,
7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e,
da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9,
5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8</td></tr>
</table>

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">VenomRAT</td><td rowspan="7">VenomRAT is a fork of Quasar RAT that is promoted online as a (benevolent) remote access tool for Windows machines. In reality, it's an info-stealing trojan that can be used for malicious purposes. On a technical level, VenomRAT is poorly designed, with hardcoded IPs and misuses of Ngrok tunneling tools.</td><td>Phishing</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="5">Data theft</td><td rowspan="3">-</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>RAT</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">22101f7ae824387a41052dfc0891096efb5ab47859727131465eeadcc1412a58,
cd5a8de963a29d07bb003a8d03fa7ba38e5004641fe8138885c967db46bef0fc,
5b11f30be6e3bfb808c25d07b492cfa12840fd0efa795d8af397feba045d1c59</td></tr>
</table>

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-23222</td><td>✗</td><td rowspan="2">iPhone, iPad, tvOS, Safari and Mac running macOS Monterey, Ventura, Sonoma</td><td rowspan="2">-</td></tr>
<tr><th>ZERO-DAY</th></tr>
<tr><td>✓</td><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*
cpe:2.3:a:apple:tvos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apple Multiple Products Type Confusion Vulnerability</td><td>✓</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-843</td><td>T1588.006: Vulnerabilities
T1203: Exploitation for Client Execution</td><td>https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22527	✗	Atlassian Confluence Data Center and Server: 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.0-8.5.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:* cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*	-
Atlassian Confluence Data Center and Server Template Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1221: Template Injection T1055: Process Injection	https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0204	✗	Fortra GoAnywhere MFT 6.x from 6.0.1 Fortra GoAnywhere MFT 7.x before 7.4.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortra:goanywhere_mft:*:*:*:*:*:*:*:*	-
Fortra GoAnywhere MFT Authentication bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-425	T1588.006: Vulnerabilities T1556: Modify Authentication Process	https://www.fortra.com/security/advisory/fi-2024-001

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA866	Unknown	All	United States and Germany
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	WasabiSeed and Screenshotter	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1218: System Binary Proxy Execution; T1218.007: Msiexec			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">TA571</td><td>Unknown</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Financial gain and espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>WasabiSeed and Screenshotter</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1105: Ingress Tool Transfer; T1113: Screen Capture; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1218: System Binary Proxy Execution; T1218.007: Msiexec</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
ScarCruft (aka Reaper, TEMP.Reaper, APT 37, Ricochet Chollima, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet)	North Korea	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	RokRAT backdoor	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1598.002: Spearphishing Attachment; T1204.002: Malicious File; T1105: Ingress Tool Transfer; T1005: Data from Local System; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1562: Impair Defenses; T1083: File and Directory Discovery; T1041: Exfiltration Over C2 Channel; T1537: Transfer Data to Cloud Account

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actor **TA866, TA571, ScarCruft** and malware **WasabiSeed, Screenshotter, Zloader, RokRAT backdoor, NS-STEALER, Kasseika ransomware, AsyncRAT, VenomRAT.**

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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TA866, TA571, ScarCruft** and malware **WasabiSeed, Screenshotter, Zloader, RokRAT backdoor, NS-STEALER, Kasseika ransomware, AsyncRAT, VenomRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

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
WasabiSeed	SHA256	29e447a6121dd2b1d1221821bd6c4b0e20c437c62264844e8bcbb9d4be35f013, 292344211976239c99d62be021af2f44840cd42dd4d70ad5097f4265b9d1ce01
	URL	hxxp[:]//109[.]107.173.72/%serial%
Screenshotter	SHA256	02049ab62c530a25f145c0a5c48e3932fa7412a037036a96d7198cc57cef1f40, d0a4cd67f952498ad99d78bc081c98afbef92e5508daf723007533f000174a98, 6e53a93fc2968d90891db6059bac49e975c09546e19a54f1f93fb01a21318fdc, 322dccd18b5564ea000117e90dafc1b4bc30d256fe93b7cfd0d1bdf9870e0da6
	URL	hxxp[:]//109[.]107.173.72/screenshot/%serial%
Zloader	URLs	hxxps://adslstickerhi[.]world, hxxps://adslstickerni[.]world, hxxps://dem.businessdeep[.]com

Attack Name	TYPE	VALUE
Zloader	SHA256	038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55, 16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d, 25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d, 2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456, 83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3, 98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2, adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa, b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93, b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378, d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d, eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499, f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb, f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8, fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616, fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75
RokRAT backdoor	SHA256	79c9f770470510034e29ef80d8d7e894ba65bdbff5bdf603c31559b1f0ab67fd, 1fb020554ae92ddc57622e53f61b05cfeab901ed8c4ca80af015eeff7ef59c8e, 48358a167e2697c6c86086505e714f4bc32655fecf59f97d3d34a13f93091e67, 67dd5d076d301e61256bb0558d23c118a71491081a019a88a7aab54c13084af6, 54ea66fc97a35c8bc37bff02bb8c94c28449fe7ee53d6bdb0310a5c5a569d2e7, 3f8ec06a3777d3732c340fe349b922f878ce3a5d9a86938574c7a041e2964b3c, 05024d1e718e904713053563c4ec11dddde928d7e53555c58d54163417e11854, 77f03d83db91b777be49e2badd1be0f4b085bb1c7c1b227dd65bdead4dd54ae6

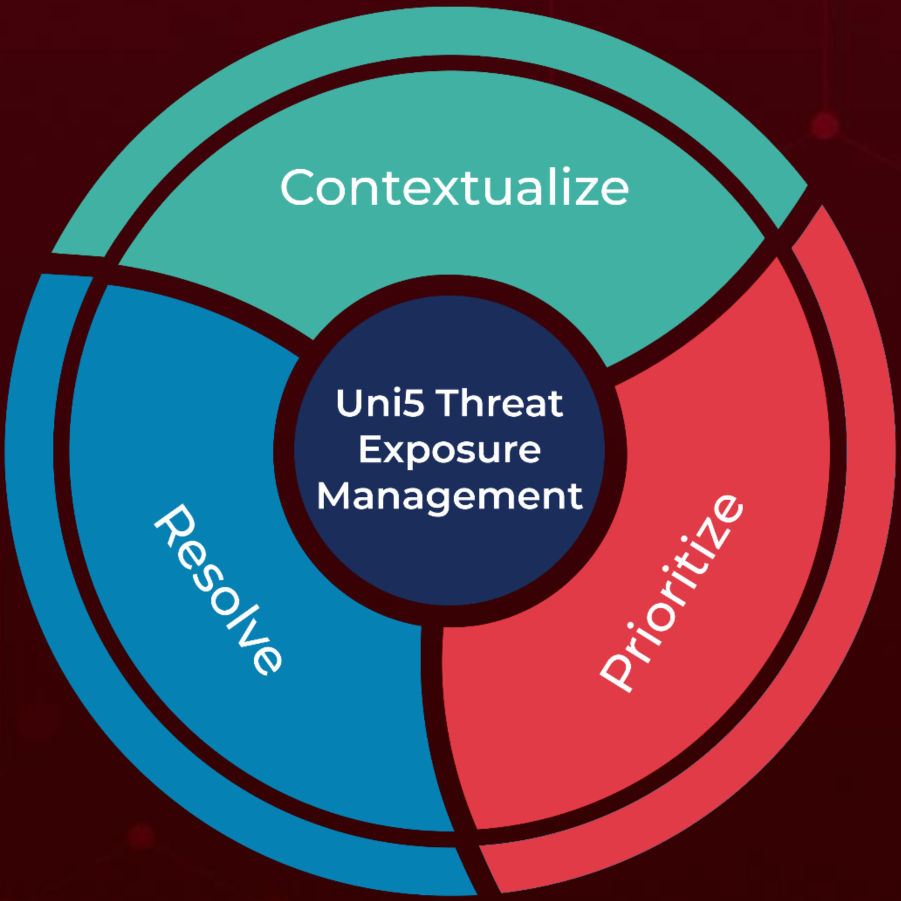
Attack Name	TYPE	VALUE
NS-STEALER	SHA256	85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10, 3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4, 3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f, 9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113, 3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83, eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224, 89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e, bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1
Kasseika ransomware	SHA256	8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7, 63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196, 3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa, cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37, c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0
AsyncRAT	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa,

Attack Name	TYPE	VALUE
AsyncRAT	SHA256	124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99
VenomRAT	SHA256	22101f7ae824387a41052dfc0891096efb5ab47859727131465eeadcc1412a58, cd5a8de963a29d07bb003a8d03fa7ba38e5004641fe8138885c967db46bef0fc, 5b11f30be6e3bfb808c25d07b492cfa12840fd0efa795d8af397feba045d1c59

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

January 29, 2024 • 4:45 AM

More at www.hivepro.com