

Date of Publication  
October 2, 2023



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

25 SEPTEMBER to 01 OCTOBER 2023

# Table Of Contents

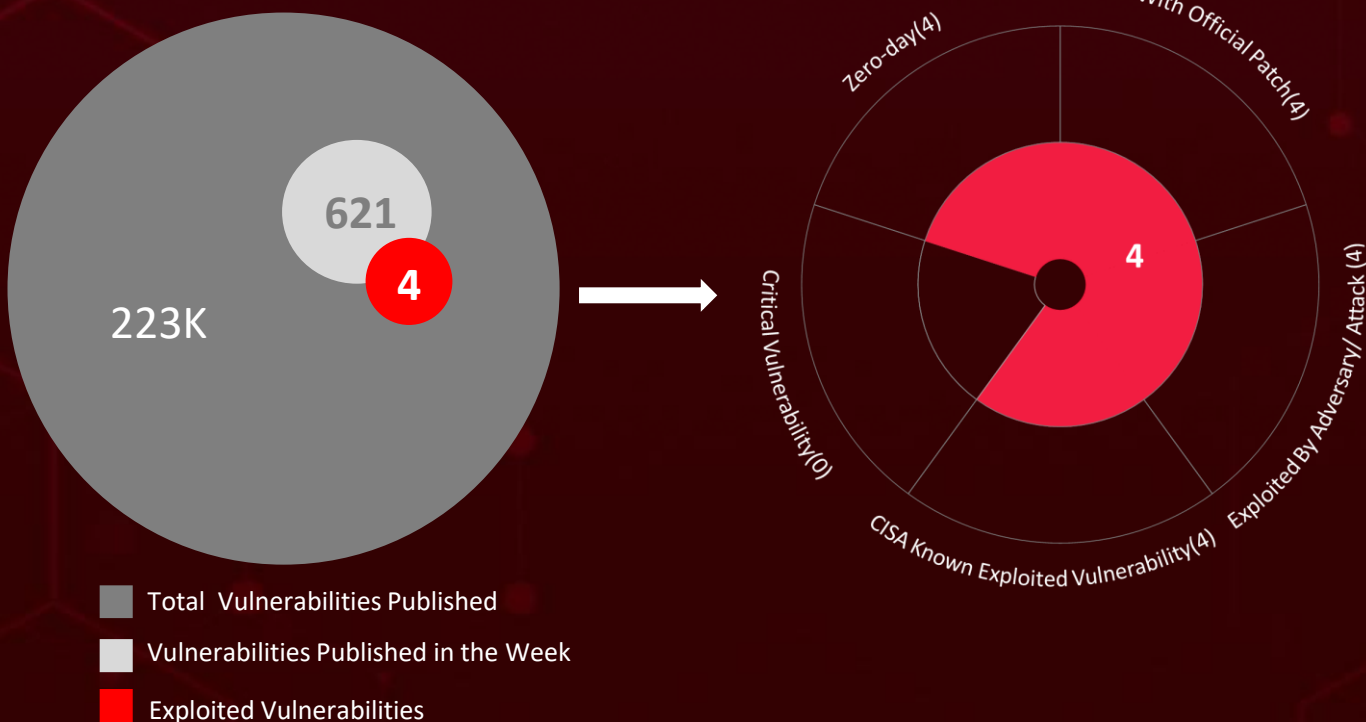
<a href="#"><u>Summary</u></a>	03
<a href="#"><u>High Level Statistics</u></a>	04
<a href="#"><u>Insights</u></a>	05
<a href="#"><u>Targeted Countries</u></a>	06
<a href="#"><u>Targeted Industries</u></a>	07
<a href="#"><u>Top MITRE ATT&amp;CK TTPs</u></a>	07
<a href="#"><u>Attacks Executed</u></a>	08
<a href="#"><u>Vulnerabilities Exploited</u></a>	13
<a href="#"><u>Adversaries in Action</u></a>	17
<a href="#"><u>Recommendations</u></a>	19
<a href="#"><u>Threat Advisories</u></a>	20
<a href="#"><u>Appendix</u></a>	21
<a href="#"><u>What Next?</u></a>	25

# 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 **four** zero-day vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a modular RAT named **ZenRAT**, which is distributed through fake Bitwarden password manager installers, primarily targeting Windows users.

Meanwhile, **BlackTech**, a China-based threat actor, is exploiting router firmware and targeting users in the U.S. and East Asia across various sectors. These observed attacks have been on the rise, posing a significant threat worldwide.



# High Level Statistics

8

Attacks  
Executed

4

Vulnerabilities  
Exploited

3

Adversaries in  
Action

- [RedLine Stealer](#)
- [ZenRAT](#)
- [DangerAds](#)
- [AtlasAgent](#)
- [Deadglyph  
Backdoor](#)
- [Bisonal](#)
- [ReVBSHELL](#)
- [Predator](#)

- [CVE-2023-41991](#)
- [CVE-2023-41992](#)
- [CVE-2023-41993](#)
- [CVE-2023-5217](#)

- [Stealth Falcon](#)
- [TAG-74](#)
- [BlackTech](#)



# Insights

## APT 33

Using Password Spray Campaigns to Infiltrate Organizations

## TAG-74

An espionage group, targets South Korean Organizations by using Bisonal and ReVBSHELL backdoor

## RedLine Stealer

A new variant is being distributed as a batch script

## Stealth Falcon

A cyber espionage group employs "Deadglyph" backdoor to primarily infiltrate Middle Eastern government entities

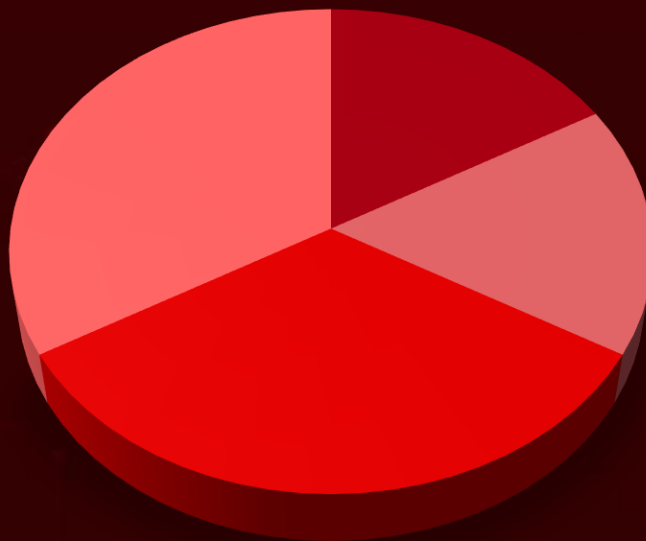
## Apple 0-day

Apple addressed three zero-day vulnerabilities used in an iPhone exploit chain to deliver the Predator spyware

## ZenRAT

A new malware distributed through fake Bitwarden password manager installers, primarily targeting Windows users

## Threat Distribution



■ Info Stealer ■ RAT ■ Trojan ■ Backdoor

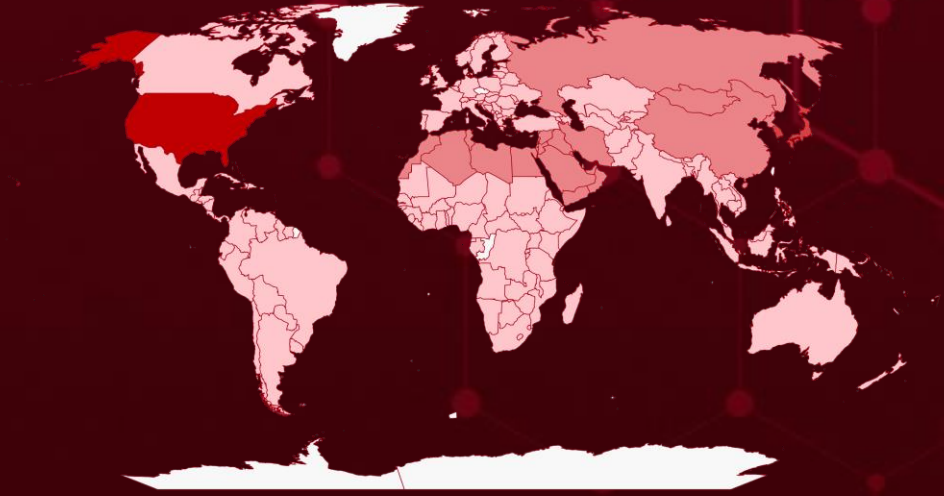


# Targeted Countries

Most



Least



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

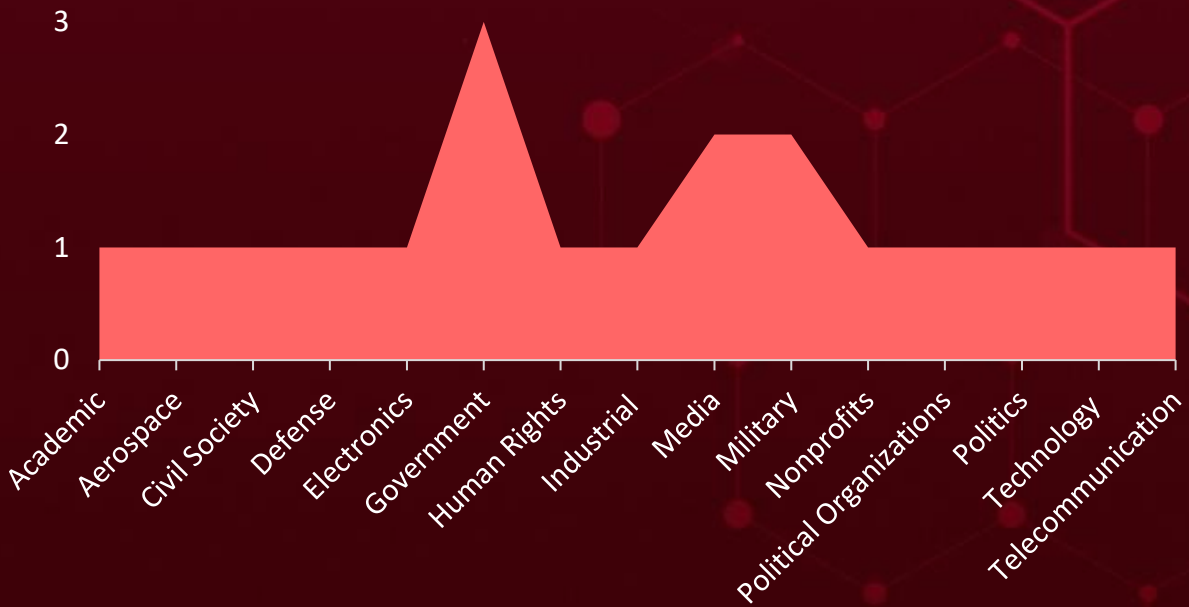
Countries
United States
Japan
South Korea
Oman
Lebanon
China
Russia
Egypt
United Arab Emirates
Iran
Mongolia
Iraq
Qatar
Israel
Saudi Arabia
Syria
Taiwan
Turkey
Jordan
United States
Kuwait
Yemen

Countries
Montenegro
Bhutan
Brazil
Palau
Brunei
Sudan
Bulgaria
Marshall Islands
Burkina Faso
New Zealand
Burundi
Barbados
Cabo Verde
Slovakia
Cambodia
Tanzania
Cameroon
Uruguay
Canada
Micronesia
Central African Republic
Namibia
South Africa

Countries
Ukraine
Côte d'Ivoire
Venezuela
Croatia
Mauritius
Cuba
Monaco
Cyprus
Mozambique
Czech Republic
Nepal
Denmark
Niger
Djibouti
Bangladesh
Dominica
Papua New Guinea
Dominican Republic
Poland
East Timor (Timor-Leste)
Belarus

Countries
El Salvador
Sierra Leone
Equatorial Guinea
Solomon Islands
Eritrea
Spain
Estonia
Suriname
Eswatini
Benin
Ethiopia
The Bahamas
Fiji
Trinidad and Tobago
Finland
Tuvalu
France
United Kingdom
Gabon
Vanuatu
Georgia
Malta
Germany
Mauritania
Ghana

# Targeted Industries



# TOP MITRE ATT&CK TTPS

**T1204.002**

Malicious File

**T1204**

User Execution

**T1566**

Phishing

**T1059**

Command and Scripting Interpreter

**T1059.001**

PowerShell

**T1059.003**

Windows Command Shell

**T1082**

System Information Discovery

**T1090**

Proxy

**T1518**

Software Discovery

**T1620**

Reflective Code Loading

**T1588**

Obtain Capabilities

**T1588.006**

Vulnerabilities

**T1041**

Exfiltration Over C2 Channel

**T1562.001**

Disable or Modify Tools

**T1587.001**

Malware

**T1087**

Account Discovery

**T1555.003**

Credentials from Web Browsers

**T1016**

System Network Configuration Discovery

**T1569**

System Services

**T1105**

Ingress Tool Transfer

# 🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">RedLine Stealer</a>	RedLine Stealer is one of the emerging stealer malwares distributed under the guise of fake documents or software. RedLine stealer was first discovered in March 2020 and is one of the most popular stealer malwares. It is designed to steal sensitive information from compromised systems.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Info Stealer			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	ddb7185f7da4beef972a1188d55c722a924862eb97c2fd42e5bbbd8d9074055b, d8c681f4bde8e5a20849ec21389d6592229e995fbb0155952b93d7e792df7cca, de2949c25878b7849a5fe7e6f7820005ab07c370c4754a6284d11162573145bf, 8fb369b47a2e6046a68026aea6c6f1198dcc6bfe9418d0f75118d24d37a68abb, bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">ZenRAT</a>	The ZenRAT malware is a modular remote access trojan (RAT) with information stealing capabilities. ZenRAT has emerged in the wild that's distributed via bogus installation packages of the Bitwarden password manager.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Modular remote access trojan (RAT)			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	60098db9f251bca8d40bf6b19e3defa1b81ff3bdc13876766988429a2e922a06, 8378c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12, 986aa8e20962b28971b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76, ba36d9d6e537a1c1ecdf1ace9f170a3a13c19e77f582a5cae5c928a341c1be8d, D7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536		

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>DangerAds</u>	DangerAds is a loader Trojan. Its main function is to detect the host environment and execute a built-in shellcode in its own process, and then the shellcode loads and runs subsequent Trojan programs.	Phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Trojan			-
<b>ASSOCIATED ACTOR</b>		Obtain host information, execute shellcode, download and execute	<b>PATCH LINK</b>
AtlasCross			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>MD5</b>	F8bafe2ce6f11a32109abbab1c42e2cf		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AtlasAgent</u>	AtlasAgent is Trojan horse program developed by AtlasCross. The main functions of the Trojan are to obtain host information, process information, prevent opening of multi-programs, inject specified shellcode and download files from CnC servers.	Phishing emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Trojan			-
<b>ASSOCIATED ACTOR</b>		Obtain host information, execute shellcode, download and execute	<b>PATCH LINK</b>
AtlasCross			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>MD5</b>	ca48431273dfcd2bd025e55f2de30635, ba85467ceff628be8b4f0e2da2a5990c		

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
<a href="#"><u>Deadglyph Backdoor</u></a>	Deadglyph backdoor's architecture is unusual as it consists of cooperating components one a native x64 binary, the other a .NET assembly. The backdoor has a range of counter detection mechanisms	Unknown	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Data Theft and Financial loss	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Stealth Falcon			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA1</b>	c40f1f46d230a85f702daa38cfa18d60481ea6c2, 740d308565e215eb9b235cc5b720142428f540db, 1805568d8362a379af09fd70d3406c6b654f189f, 9cb373b2643c2b7f93862d2682a0d2150c7aec7e, f47cb40f6c2b303308d9d705f8cad707b9c39fa5,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Bisonal</u></a>	Bisonal is a long-running customized backdoor that, because of its added capability, is likely meant to be used as a follow-up malware family loaded after initial access is established. Bisonal has been spotted assisting with the TAG-74 infrastructure.	Visual Basic Script backdoor	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Information Theft and Financial loss	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
TAG-74			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd, 01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd, a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5, 89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893bec1a9bc, 0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514		

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
<b>ReVBSHELL</b>	<p>TAG-74 utilizes social engineering attacks, employing Microsoft Compiled HTML Help (CHM) files as lures. These CHM files are used to deliver a modified version of an open-source Visual Basic Script backdoor known as "ReVBSHELL." ReVBSHELL is configured to enter a sleep mode for a specified duration, a command that can be issued remotely and edited as needed from a server.</p>	Social Engineering	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Information Theft and Financial loss	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
TAG-74			-
<b>IOC TYPE</b>	<b>VALUE</b>		
<b>SHA256</b>	aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71, 8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34, ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c, 465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c, 6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a		

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>Predator</u>	<p>Predator malware is a type of spyware developed and sold by Israeli company Intellexa. It is a very dangerous virus that can steal information from victims, including passwords, browser data, and the contents of cryptocurrency wallets. It can also take photos using the infected victim's webcam.</p>	Social Engineering	CVE-2023-41991 CVE-2023-41992 CVE-2023-41993 CVE-2023-5217
TYPE		IMPACT	AFFECTED PRODUCTS
Spyware		Information Theft and Financial loss	iPhone, iOS, iPadOS, macOS, watchOS, Safari, Google Chrome, Firefox, FirefoxESR, Firefox Focus for Android, Firefox for Android
ASSOCIATED ACTOR			PATCH LINK
-			<a href="https://support.apple.com/en-us/HT213927">https://support.apple.com/en-us/HT213927</a> ; <a href="https://support.apple.com/en-us/HT213931">https://support.apple.com/en-us/HT213931</a> ; <a href="https://support.apple.com/en-us/HT213932">https://support.apple.com/en-us/HT213932</a> ; <a href="https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html">https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html</a> ; <a href="https://www.mozilla.org/en-US/security/advisories/mfsa-2023-44/">https://www.mozilla.org/en-US/security/advisories/mfsa-2023-44/</a>
IOC TYPE	VALUE		
SHA256	df9c1ed19c6bd78d9813bb2b9b084b16781f9dd64b5236f77622f632d98b9a9f, 93488594d1b33bd64a0c5568a54e8f23f4aef6b6ae1b498c10b114a18c18a4ec, edbcfe1171767f6e2a18266e14039c5fecfd0922fd5eca64971a901ea2d9d8aa, 09780015b2aeb7e82bdd67973f45d5eea247ff19057ed8be1c61d8c434983977, 896e102087175cb5b690b21e3395b77d0db05e7ded7c6dd62a50494630b420fe		

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



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-41992</a>		iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*	Predator
Apple Multiple Products Kernel Privilege Escalation Vulnerability		cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*	
		cpe:2.3:o:apple:watchos:*:*:*:*:*:*	
		cpe:2.3:o:apple:macos:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-754	T1068: Exploitation for Privilege Escalation	<a href="https://support.apple.com/en-us/HT213927">https://support.apple.com/en-us/HT213927</a> ; <a href="https://support.apple.com/en-us/HT213931">https://support.apple.com/en-us/HT213931</a> ; <a href="https://support.apple.com/en-us/HT213932">https://support.apple.com/en-us/HT213932</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-5217</u></a>		Google Chrome, Firefox, Firefox ESR, Firefox Focus for Android, Firefox for Android	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:google_chrome:117.0.5938.92:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_focus_for_android:118.0:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_ESR:115.3.0:*:*:*:*:*:* cpe:2.3:a:mozilla:mozilla_firefox:118.0:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_for_android:118.0:*:*:*:*:*:*	Predator
Google Chrome libvpx Heap Buffer Overflow Vulnerability			
	CWE ID		
	CWE-122	T1189:Drive-by Compromise	<a href="https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html">https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html</a> , <a href="https://www.mozilla.org/en-US/security/advisories/mfsa-2023-44/">https://www.mozilla.org/en-US/security/advisories/mfsa-2023-44/</a>





# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b>Stealth Falcon (aka FruityArmor, Project Raven)</b></p>	UAE	Media, Civil Society, Human Rights, Government, Politics, and Nonprofits	Middle East
	<b>MOTIVE</b>		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	Deadglyph Backdoor	-


## TTPs

TA0042 Resource Development; TA0002 Execution; TA0003 Persistence; TA0005 Defense Evasion; TA0007 Discovery; TA0009 Collection; TA0011 Command and Control; TA0010 Exfiltration; T1583.001 Domains; T1583.003 Virtual Private Server; T1587.001 Malware; T1588.003 Code Signing Certificates; T1047 Windows Management Instrumentation; T1059.003 Windows Command Shell; T1106 Native API; T1204.002 Malicious File; T1546.003 Windows Management Instrumentation Event Subscription; T1027 Obfuscated Files or Information; T1070.004 File Deletion; T1112 Modify Registry; T1134 Access Token Manipulation; T1140 Deobfuscate/Decode Files or Information; T1218.011 Rundll32; T1480.001 Environmental Keying; T1562.001 Disable or Modify Tools; T1620 Reflective Code Loading; T1007 System Service Discovery; T1012 Query Registry; T1016 System Network Configuration Discovery; T1033 System Owner/User Discovery; T1057 Process Discovery; T1082 System Information Discovery; T1518.001 Security Software Discovery; T1005 Data from Local System; T1071.001 Web Protocols; T1090 Proxy; T1573.001 Symmetric Cryptography; T1041 ExfiltrationOver C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>TAG-74</b>	China	Academic, aerospace, defense, government, military, and political organizations	South Korea, Japan, and Russia
	<b>MOTIVE</b>		
	Cyber-espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	Bisonal, ReVBSHELL	-	

**TTPs**

TA0001 Initial Access; TA0002 Execution; TA0003 Persistence; TA0005 Defense Evasion; TA0007 Discovery; TA0011 Command and Control; TA0010 Exfiltration; T1566 Phishing; T1566.001 Spearphishing Attachment; T1059 Command and Scripting Interpreter; T1059.005 Visual Basic; T1204 User Execution; T1204.002 Malicious File; T1547 Boot or Logon Autostart Execution; T1547.001 Registry Run Keys / Startup Folder; T1574 Hijack Execution Flow; T1574.001 DLL Search Order Hijacking; T1218 System Binary Proxy Execution; T1218.001 Compiled HTML File; T1480 Execution Guardrails; T1518 Software Discovery; T1518.001 Security Software Discovery; T1132 Data Encoding; T1132.001 Standard Encoding; T1071 Application Layer Protocol; T1071.001 Web Protocols; T1573 Encrypted Channel; T1573.001 Symmetric Cryptography; T1041 Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda)</b>	China	Government, industrial, technology, media, electronics, telecommunication, military	U.S. and East Asia
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	-	-	

**TTPs**

TA0042 Resource Development; TA0001 Initial Access; TA0003 Persistence; TA0004 Privilege Escalation; TA0005 Defense Evasion; TA0007 Discovery; TA0008 Lateral Movement; TA0011 Command and Control; T1588 Obtain Capabilities; T1588.003 Code Signing Certificates; T1199 Trusted Relationship; T1205 Traffic Signaling; T1542.004 ROMMONkit; T1112 Modify Registry; T1562 Impair Defenses; T1562.003 Impair Command History Logging; T1601.001 Patch System Image; T1021.001 Remote Desktop Protocol; T1021.004 SSH; T1071.002 File Transfer Protocols; T1090 Proxy

# 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 actor **Stealth Falcon, TAG-74, BlackTech and RedLine Stealer, ZenRAT, DangerAds, AtlasAgen, Bisonal, ReVBSHELL, Deadglyph Backdoor, Predator** malware.

## 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 **Stealth Falcon, TAG-74, BlackTech and RedLine Stealer, ZenRAT, DangerAds, AtlasAgent, Bisonal, ReVBSHELL, Deadglyph Backdoor, Predator** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Apple Addresses Zero-Day Flaws Exploited in the Wild](#)

[New Variant of RedLine Stealer Uses Batch Script to Evade Detection](#)

[Critical Security Vulnerabilities Discovered in Atlassian Products](#)

[Deadglyph Malware Emerges as a Game Changer for Stealth Falcon](#)

[ZenRAT Targeting Windows Users Through Fake Bitwarden Installs](#)

[TAG-74's Multi-Year Campaign Targets South Korean Organizations](#)

[AtlasCross Exploits Organizations with DangerAds and AtlasAgent Trojans](#)

[Google and Firefox fixes Zero-Day Flaw Exploited in the Wild](#)

[BlackTech: China-Linked Cyber Actors Exploit Router Firmware](#)

# Appendix

**Known Exploited Vulnerabilities (KEV):** Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

**Celebrity Vulnerabilities:** Software vulnerabilities that have gained significant attention and been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

## ✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<a href="#"><u>RedLine Stealer</u></a>	SHA256	ddb7185f7da4beef972a1188d55c722a924862eb97c2fd42e5bbbd8d9074055b, d8c681f4bde8e5a20849ec21389d6592229e995fbb0155952b93d7e792df7cca, de2949c25878b7849a5fe7e6f7820005ab07c370c4754a6284d11162573145bf, 8fb369b47a2e6046a68026aea6c6f1198dcc6bfe9418d0f75118d24d37a68abb, bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466, 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4, 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4, bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466, 9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0, 6cbe9be190f521408438262d0c7f2ccbfb32a6df558cec2a264285fdfffe5c2, 53af2c266c7f18e7c1ab16460d3c09d773fe93ac0a840fa83a30cc1020d1019a, 4f1c1565afc782e688945c07a486205c59d43a98ae577c5d065bfed9a47a983d, b5d8caa15cbf53d002edc6194abd0de43e4a139cc04f9703ae7bfc397bca66c8,

Attack Name	TYPE	VALUE
<u>RedLine Stealer</u>	SHA256	9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0, 43328f774db70b98c4cbe83cc3be18de20a29b073b483eec49c64c6c301e4079, 1b5f1e505e57b9915418f251f9c2343302f0737bdd85126666db56a27f0142f2, b83e50fa2c5c54e027f3bfe859e2a69e883bbb0080fed20aca176f77ad120fa1
<u>Deadglyph Backdoor</u>	SHA1	c40f1f46d230a85f702daa38cfa18d60481ea6c2, 740d308565e215eb9b235cc5b720142428f540db, 1805568d8362a379af09fd70d3406c6b654f189f, 9cb373b2643c2b7f93862d2682a0d2150c7aec7e, f47cb40f6c2b303308d9d705f8cad707b9c39fa5, 3d4d9c9f2a5aceff9e45538f5ebe723acaf83e32, 3d2accea98dbdf95f0543b7c1e8a055020e74960, 4e3018e4fd27587bd1c566930ae24442769d16f0
	IPv4	135.125.78[.]187, 185.25.50[.]60
<u>ZenRAT</u>	SHA256	60098db9f251bca8d40bf6b19e3defa1b81ff3bdc13876766988429a2e922a06, 8378c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12, 986aa8e20962b28971b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76, ba36d9d6e537a1c1ecd1ace9f170a3a13c19e77f582a5cae5c928a341c1be8d, d7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536, e0c067fc8e10a662c42926f6cdadfa5c6b8c90d5dff3f0e9f381210180d47d37, e318b2c1693bc771dfe9a66ee2cebcc2b426b01547bb0164d09d025467cb9ee3, f7573ad27ff407e84d3ebf173cbeaaa6aba62eb74b4b2b934bc0433df3d9e066
	Domains	bitwariden[.]com, crazygameis[.]com, geogebraa[.]com, obsploject[.]com
	IPv4:Port	185.156.72[.]8:9890, 185.186.72[.]14:9890
<u>Bisonal</u>	SHA256	11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd, 01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd, a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5,

Attack Name	TYPE	VALUE
<b><u>Bisonal</u></b>	SHA256	89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893becec1a9bc, 0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514
	File Name	SearchFilterHost.exe, msfltr32.exe, MySnake.EXE
	Domains	formsgle.freedynamicdns[.]net, satreci.bounceme[.]net, hanseo1.hopto[.]org, sarang.serveminecraft[.]net
<b><u>ReVBSHell</u></b>	SHA256	aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71, 8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34, ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c, 465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c, 6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a, df7d584d56af6fcf3cca31ed0d3a4d34abd2c1019b8d223a230f8a78075a7d9a, 078a8026f32b8d05258285dc527408388c651f6c3eaebc45f8bb3f4b42248631
<b><u>DangerAds</u></b>	MD5	f8bafe2ce6f11a32109abbab1c42e2cf
	SHA256	9c2f990f2d23f380f1cf8f83e9e23749f7ef097bda5b530c7d43fbf5feb3ba99
<b><u>AtlasAgent</u></b>	MD5	ca48431273dfcd2bd025e55f2de30635, ba85467ceff628be8b4f0e2da2a5990c
	Domains	activequest[.]goautodial[.]com, ops-ca[.]mioying[.]com, app[.]basekwt[.]com, secure[.]poliigon[.]com, engage[.]adaptqe[.]com, chat[.]thedresscodeapp[.]com, superapi-staging[.]mlmprotec[.]com, search[.]allaccountingcareers[.]com, order[.]staging[.]photobookworldwide[.]com, crm[.]cardabel[.]com, public[.]pusulait[.]com

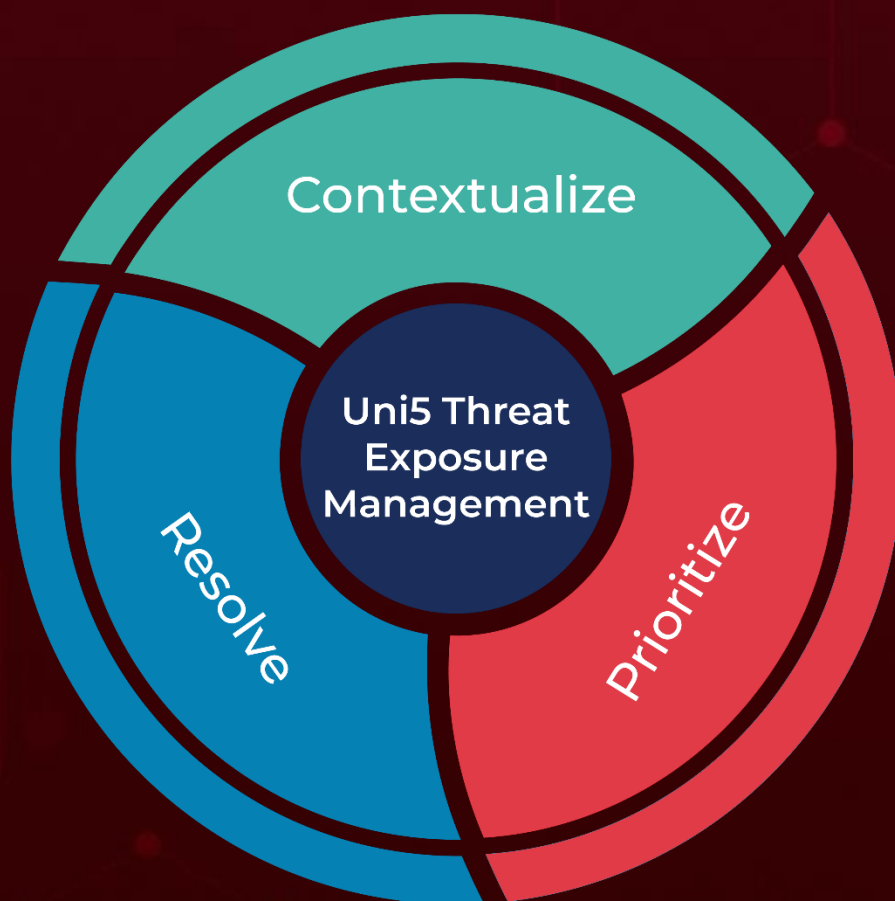
Attack Name	TYPE	VALUE
<u>Predator</u>	SHA256	df9c1ed19c6bd78d9813bb2b9b084b16781f9dd64b5236f77622f632d98b9a9f, 93488594d1b33bd64a0c5568a54e8f23f4aef6b6ae1b498c10b114a18c18a4ec, edbcfe1171767f6e2a18266e14039c5fecfd0922fd5eca64971a901ea2d9d8aa, 09780015b2aeb7e82bdd67973f45d5eea247ff19057ed8be1c61d8c434983977, 896e102087175cb5b690b21e3395b77d0db05e7ded7c6dd62a50494630b420fe



# 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

**October 2, 2023 • 11:30 PM**

© 2023 All Rights are Reserved by Hive Pro®



More at [www.hivepro.com](http://www.hivepro.com)