

Date of Publication  
October 1, 2024



HiveForce Labs

MONTHLY

# THREAT DIGEST

**Vulnerabilities, Attacks, and Actors**

SEPTEMBER 2024

# Table Of Contents

- [Summary](#)..... 03
- [Insights](#)..... 04
- [Threat Landscape](#)..... 05
- [Celebrity Vulnerabilities](#) ..... 06
- [Vulnerabilities Summary](#)..... 09
- [Attacks Summary](#)..... 12
- [Adversaries Summary](#)..... 15
- [Targeted Products](#)..... 17
- [Targeted Countries](#)..... 19
- [Targeted Industries](#)..... 20
- [Top MITRE ATT&CK TTPs](#)..... 21
- [Top Indicators of Compromise \(IOCs\)](#)..... 22
- [Vulnerabilities Exploited](#)..... 25
- [Attacks Executed](#)..... 38
- [Adversaries in Action](#)..... 58
- [MITRE ATT&CK TTPS](#)..... 70
- [Top 5 Takeaways](#)..... 75
- [Recommendations](#)..... 76
- [Hive Pro Threat Advisories](#)..... 77
- [Appendix](#)..... 78
- [Indicators of Compromise \(IoCs\)](#)..... 79
- [What Next?](#)..... 93

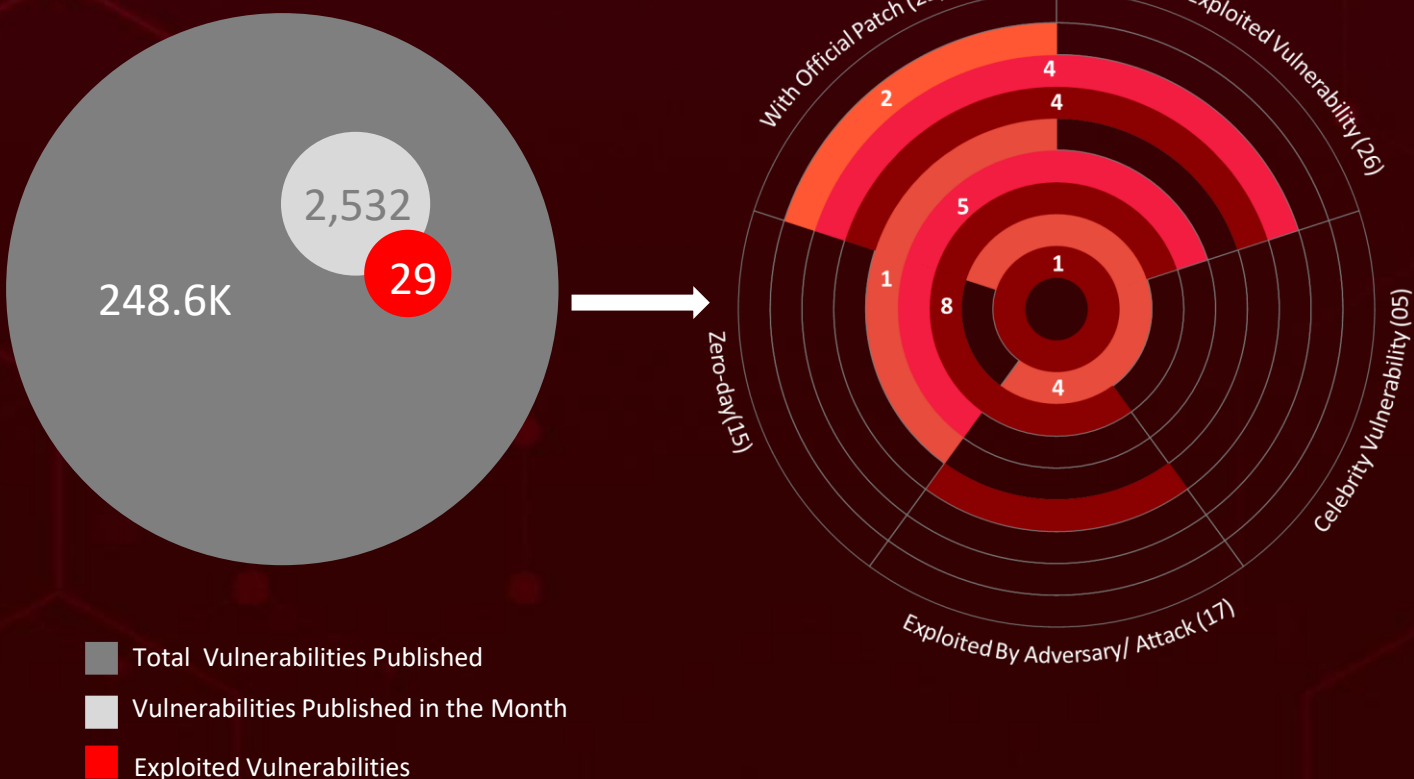
# Summary

In **September**, the cybersecurity arena garnered significant attention following the discovery of **fifteen zero-day** vulnerabilities. North Korean hackers leveraged a recently patched Google Chrome zero-day, **CVE-2024-7971**, to deploy the **FudModule rootkit**, further escalating concerns.

At the same time, ransomware incidents surged, with aggressive variants such as **Meow**, **RansomHub**, **LockBit**, **Babuk**, and **INC ransomware** targeting numerous victims. As ransomware tactics become increasingly sophisticated, organizations must strengthen their defenses by adopting robust backup and disaster recovery solutions.

Meanwhile, **Mustang Panda**, a notorious advanced persistent threat (APT) group, has ramped up its operations, deploying new malware variants and refining its attack methods. The group has orchestrated complex worm-based attacks aimed at high-value targets.

Additionally, **CVE-2024-43461**, a spoofing vulnerability in Microsoft Windows MSHTML, has been actively exploited in zero-day campaigns by the **Void Banshee APT** group. This vulnerability facilitated the deployment of malware, including the **Atlantida info-stealer**. As the threat landscape continues to evolve, it is crucial for organizations to remain vigilant and proactively address emerging risks.



**In September 2024**, a geopolitical cybersecurity landscape unfolds, revealing **Australia, Japan, Taiwan, Singapore, and China** as the top-targeted countries

Highlighted in **September 2024** is a cyber battleground encompassing the **Manufacturing, Government, IT, Financial, and Energy** sectors, designating them as the top industries

**Meow Ransomware Strikes Again:**  
Resurfaces Stronger After 2023 Halt.  
Focusing Extortion Over Encryption

**AnyDesk and MEGA:** Tools of Choice for **Vanilla Tempest** in Data Exfiltration

**Microsoft's September Patch Tuesday**  
Tackles 79 Vulnerabilities, Including 4 Zero-Days Across Key Products

**DragonRan k's Malware Arsenal:**  
Using Web Shells to Manipulate Search Engine Results

**Geopolitical Espionage Escalates:** Tropic Trooper Targets Human Rights in the Middle East

**200+ Victims in 2024:**  
RansomHub's Affiliates Push Double Extortion Tactics

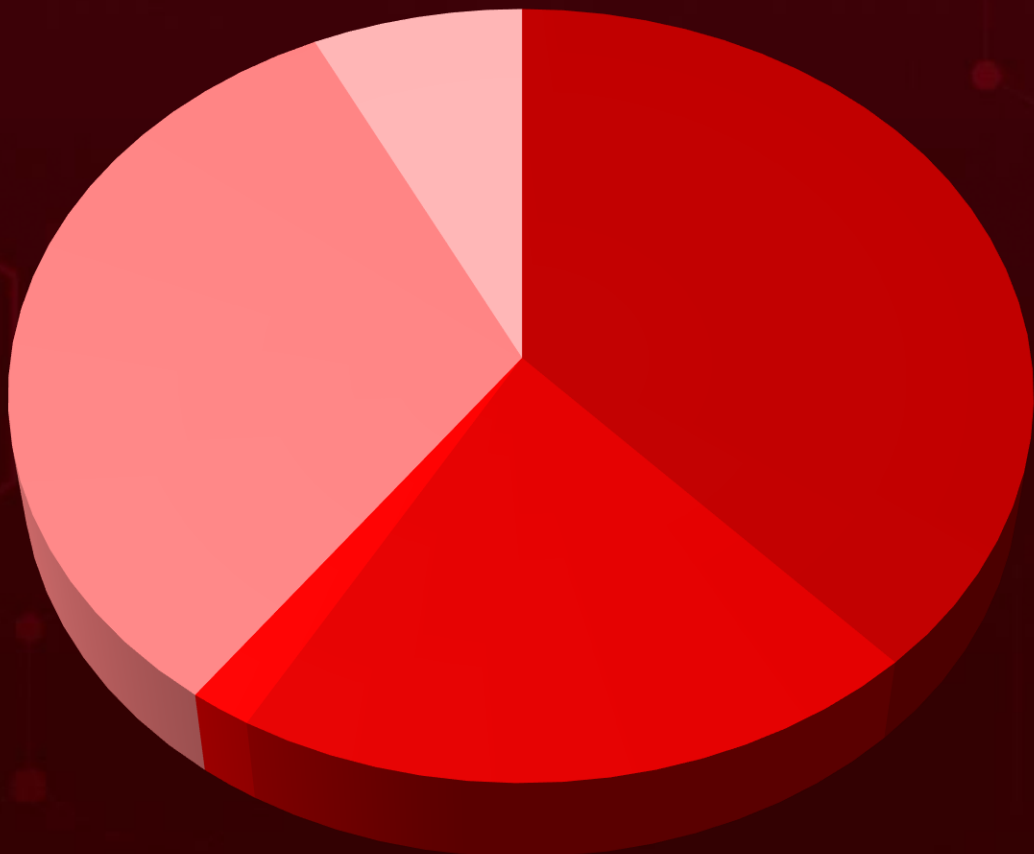
**FudModule Rootkit Gains**

**Control:**

Chrome Zero-Day Fuels North Korean Attacks

**CVE-2024-20469:**  
Command Injection Flaw Puts Cisco ISE at Risk of Root Compromise

# Threat Landscape



■ Malware Attacks

■ Social Engineering

■ Denial-of-Service Attack

■ Injection Attacks



■ Password Attack







# Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2020-1472</a>		Microsoft Netlogon	-
	CISA KEY		
<b>NAME</b>		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
			cpe:2.3:o:microsoft:windows_server:*.:*:*:*:*:*
ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH DETAILS</b>
	CWE-330	T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472</a>

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2017-0144</a>		Microsoft SMBv1	-
	CISA KEY		
<b>NAME</b>		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
			cpe:2.3:a:microsoft:server_message_block:1.0:*.:*:*:*:*:*
EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH DETAILS</b>
	CWE-94	T1059 : Command and Scripting Interpreter, T1210 : Exploitation of Remote Services	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213</a>

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2021-31207</u></a>		Microsoft Exchange Server	-
	CISA KEV		
NAME		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.:*:*:*:*	RansomHub Ransomware
PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-434	T1190 : Exploit Public-Facing Application, T1588.006: Vulnerabilities	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207</a>





































CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2021-34473</u></a>		Microsoft Exchange Server	-
	CISA KEV		
NAME		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.:*:*:*:*	RansomHub Ransomware
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1190 : Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473</a>














CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34523</u>		Microsoft Exchange Server	-
	CISA KEY		
<b>NAME</b>		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.*.*.*.*.*	RansomHub Ransomware
		<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>
	CWE-287	T1190 : Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523</a>



# Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-7971	Google Chromium V8 Type Confusion Vulnerability	Google Chrome, Microsoft Edge	✓	✓	✓
CVE-2024-20469	Cisco Identity Services Engine Command Injection Vulnerability	Cisco Identity Services Engine	✗	✗	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-27997	Fortinet heap-based buffer overflow Pre-Auth Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN	✓	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	✗	✓	✓
CVE-2023-22515	Atlassian Confluence Privilege Escalation Vulnerability	Atlassian Confluence Data Center and Server	✓	✓	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✓	✓	✓
CVE-2023-48788	Fortinet FortiClientEMS SQL Injection Vulnerability	Fortinet FortiClient EMS	✗	✓	✓
CVE-2017-0144	EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	Microsoft SMBv1	✓	✓	✓
CVE-2020-1472	Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability	Microsoft Windows	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server			
CVE-2021-34523	PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	Microsoft Exchange Server			
CVE-2021-31207	PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	Microsoft Exchange Server			
CVE-2023-26360	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion			
CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	Microsoft Windows			
CVE-2024-38226	Microsoft Publisher Security Feature Bypass Vulnerability	Microsoft Windows			
CVE-2024-43491	Microsoft Windows Update Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows			
CVE-2024-41869	Adobe Acrobat and Reader Use After Free Vulnerability	Adobe Acrobat and Reader			
CVE-2024-8190	Ivanti Cloud Services Appliance OS Command Injection Vulnerability	Cloud Service Appliance (CSA)			
CVE-2024-8963	Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability	Cloud Services Appliance (CSA)			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-29847	Ivanti Endpoint Manager Deserialization of Untrusted Data Vulnerability	Ivanti Endpoint Manager			
CVE-2024-38112	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows			
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR			
CVE-2024-6670	Progress WhatsUp Gold SQL Injection Vulnerability	Progress WhatsUp Gold			
CVE-2024-36401	OSGeo GeoServer GeoTools Eval Injection Vulnerability	GeoServer			
CVE-2024-7593	Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability	Ivanti Virtual Traffic Manager			

# Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
FudModule	Rootkit	CVE-2024-7971	Google Chrome, Microsoft Edge		Exploit vulnerabilities
Meow Ransomware	Ransomware	-	-	-	Phishing
Emansrepo Stealer	Stealer	-	Microsoft Windows	-	Phishing
RansomHub Ransomware	Ransomware	CVE-2023-3519 CVE-2023-27997 CVE-2023-46604 CVE-2023-22515 CVE-2023-46747 CVE-2023-48788 CVE-2017-0144 CVE-2020-1472 CVE-2020-0787	-		Phishing, Exploiting vulnerabilities
China Chopper	Web shell	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360	-		-
Crowdoor	Loader	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360	-		-
BlotchyQuasar	RAT	-	-	-	Phishing
CXCLNT	Backdoor	-	Windows	-	-
CLNTEND	Backdoor	-	-	-	-
Fog ransomware	Ransomware	-	-	-	Compromised Virtual Private Network (VPN) credentials
DOWNBAIT	Downloader	-	-	-	Spear Phishing Emails

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PULLBAIT	Downloader	-	-	-	DOWNBAIT deploys
CBROVER	Backdoor	-	-	-	PULLBAIT deploys
PLUGX	RAT	-	-	-	Deployed by other malware, or via exploited vulnerabilities in web applications
PUBLOAD	Downloader	-	-	-	HIUPAN spreads through removable drives
BadIIS	Backdoor	-	-	-	Exploit vulnerabilities in web applications
Atlantida	Information stealer	CVE-2024-43461 CVE-2024-38112	Microsoft Windows		Exploiting Vulnerabilities
Gomorrah Stealer	Information stealer	-	Windows	-	-
PhantomDL	Backdoor	CVE-2023-38831	WinRAR		Phishing, Exploiting Vulnerability
PhantomCore	RAT	CVE-2023-38831	WinRAR		Phishing, Exploiting Vulnerability
LockBit	Ransomware	CVE-2023-38831	WinRAR		Phishing, Exploiting Vulnerability
Babuk	Ransomware	CVE-2023-38831	WinRAR		Phishing, Exploiting Vulnerability
SambaSpy	RAT	-	-	-	Phishing
Gootloader	Loader	-	-	-	-
Supper backdoor	Backdoor	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
INC Ransomware	Ransomware	-	-	-	Phishing
Diamorphine	Rootkit	-	CentOS	-	Exploit vulnerabilities
EAGLEDOOR	Backdoor	CVE-2024-36401	GeoServer		Exploit vulnerabilities and Spear-phishing
PondRAT	Backdoor	-	Linux and macOS	-	Python software packages
POOLRAT	Backdoor	-	Linux and macOS	-	Python software packages
BURNBOOK	Loader	-	-	-	Phishing
TEARPAGE	Loader	-	-	-	Phishing
MISTPEN	Backdoor	-	-	-	Through BURNBOOK and TEARPAGE
SnipBot	RAT	-	Windows	-	Phishing
RomCom	RAT	-	Windows	-	Phishing
KLogExe	Keylogger	-	-	-	Phishing
FPSpy	Backdoor	-	-	-	Phishing
RIPCOY	Trojan	CVE-2024-36401	GeoServer		Phishing

# Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Citrine Sleet	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2024-7971	FudModule, PondRAT, POOLRAT, BURNBOOK, TEARPAGE, MISTPEN	Google Chrome, Microsoft Edge, Linux and macOS
Tropic Trooper	Information theft and espionage	China	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360	China Chopper, Crowdoor	-
Blind Eagle	Information theft, Espionage, Financial crime	Colombia	-	BlotchyQuasar RAT	-
TIDRONE	Information Theft, Espionage	Chinese-speaking threat actor	-	CXCLNT, CLNTEND	-
Mustang Panda	Information Theft, Espionage	China	-	DOWNBAIT, PULLBAIT, CBROVER, PLUGX, PUBLOAD (aka ClaimLoader)	-
DragonRank	Information Theft, Espionage	China	-	PlugX and BadIIS	Windows
Void Banshee APT	Financial Gain, Information Theft	-	CVE-2024-43461 CVE-2024-38112	Atlantida	Microsoft Windows
Head Mare	Information Theft, Espionage, Financial Gain, Hacktivism	Linked to Russian-speaking	CVE-2023-38831	PhantomDL, PhantomCore, LockBit ransomware, Babuk ransomware	WinRAR










ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Vanilla Tempest	Financial Gain	-	-	INC Ransomware, Gootloader, Supper backdoor	-
TeamTNT	Information theft and Financial gain	Germany	-	-	CentOS
Earth Baxia	Information theft and espionage	China	CVE-2024-36401	EAGLEDOOR	GeoServer
Sparkling Pisces	Information theft and espionage	North Korea	-	KLogEXE and FPSpy	-





# Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Application	F5 BIG-IP Configuration Utility
	Plugin	WordPress LiteSpeed Cache Plugin Versions Prior to 6.5.0.1, Houzez Theme Versions 3.2.4 and Prior, Houzez Login Register Plugin Versions 3.2.5 and Prior
	Browser	Google Chromium V8
	Server	Atlassian Confluence Data Center and Server
	Browser	Microsoft Edge
	Application	Microsoft Netlogon, Microsoft Exchange Server, Microsoft Publisher 2016, Microsoft Office LTSC 2021, Microsoft Office 2019, Microsoft SharePoint Server: 2019, Microsoft SharePoint Server Subscription Edition: All versions, Microsoft SharePoint Enterprise Server: 2016
	OS	Windows: 10 - 11 23H2, Windows Server: 2008 – 2022 23H2
	Security appliances	Fortinet FortiOS and FortiProxy SSL-VPN, Fortinet FortiClient EMS
	Application delivery controller, Virtualization Software	Citrix NetScaler ADC, XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR
	Remote access solution	Citrix NetScaler Gateway
	Open-source enterprise resource planning (ERP) system, message broker, application server	Apache OFBiz: Version Prior to 18.12.16, Apache ActiveMQ, Apache Tomcat

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Application	Adobe ColdFusion, Acrobat DC Versions 24.003.20054 and earlier versions (Windows, MacOS)
	Wi-Fi system, router	D-link COVR-X1870 v1.02 and below, DIR-X4860 v1.04B04_Hot-Fix and below, DIR-X5460 v1.11B01_Hot-Fix and below
	Cloud Service Appliance, Endpoint Manager	Ivanti CSA 4.6 (All versions before Patch 519), Ivanti Endpoint Manager 2022 SU5 and prior, Ivanti Endpoint Manager 2024
	Application	WinRAR version 6.22 and older versions
	DevOps lifecycle tool	GitLab CE/EE All versions starting from 8.14 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2
	Load balancing solution, Network monitoring solution	Progress LoadMaster 7.2.60.0 and all prior versions, Multi-Tenant Hypervisor 7.1.35.11 and all prior versions, Progress WhatsUp Gold versions released before 2024.0.0
	Identity management platform, Cloud-based licensing management	Cisco Identity Services Engine (ISE) versions: 3.2 and 3.3, Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0
	APs and Security router	NWA50AX: 7.00(ABYW.1)and earlier,NWA50AX PRO: 7.00(ACGE.1)and earlier,NWA55AXE: 7.00(ABZL.1)and earlier,NWA90AX: 7.00(ACCV.1)and earlier,NWA90AX PRO: 7.00(ACGF.1)and earlier, NWA110AX: 7.00(ABTG.1)and earlier, WAC500: 6.70(ABVS.4) and earlier, USG LITE 60AX: 2.00(ACIP.2)
	Application	SolarWinds ARM 2024.3 and prior versions
	Application	Microchip Advanced Software Framework: through 3.52.0.2574

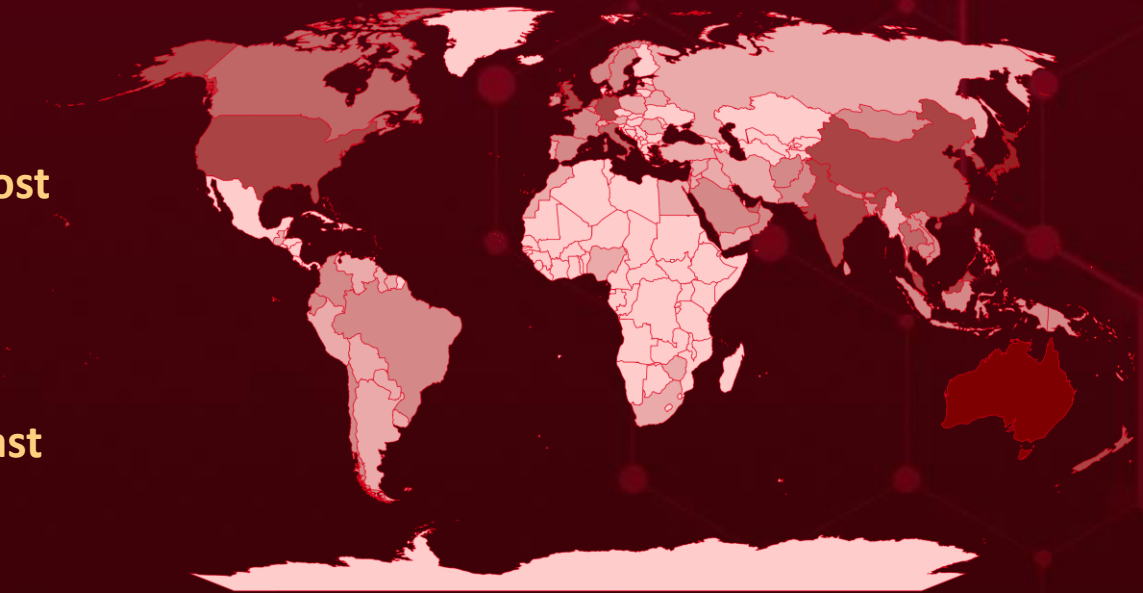


# Targeted Countries

Most



Least



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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
Dark Red	Australia	Dark Red	Bangladesh	Dark Red	Nepal	Dark Red	Nigeria	Dark Red	Yemen
Dark Red	Japan	Dark Red	Brunei	Dark Red	Spain	Dark Red	Falkland Islands	Dark Red	Belarus
Dark Red	Taiwan	Dark Red	Indonesia	Dark Red	Cyprus	Dark Red	Djibouti	Dark Red	Zimbabwe
Dark Red	Singapore	Dark Red	Tuvalu	Dark Red	Sweden	Dark Red	Poland	Dark Red	Latvia
Dark Red	China	Dark Red	Ireland	Dark Red	Ecuador	Dark Red	Argentina	Dark Red	Gabon
Dark Red	Germany	Dark Red	Palau	Dark Red	France	Dark Red	Portugal	Dark Red	Samoa
Dark Red	South Korea	Dark Red	Israel	Dark Red	Chile	Dark Red	Guatemala	Dark Red	Dominica
Dark Red	India	Dark Red	Brazil	Dark Red	Tonga	Dark Red	Qatar	Dark Red	Haiti
Dark Red	United Kingdom	Dark Red	Cook Islands	Dark Red	Niue	Dark Red	Syria	Dark Red	Ethiopia
Dark Red	United States	Dark Red	Sri Lanka	Dark Red	Bahrain	Dark Red	Romania	Dark Red	Honduras
Dark Red	New Zealand	Dark Red	Belgium	Dark Red	Colombia	Dark Red	Guyana	Dark Red	Greenland
Dark Red	Malaysia	Dark Red	Timor-Leste	Dark Red	New Caledonia	Dark Red	Russia	Dark Red	Botswana
Dark Red	Netherlands	Dark Red	Kiribati	Dark Red	Afghanistan	Dark Red	Burma	Dark Red	Benin
Dark Red	North Korea	Dark Red	Norway	Dark Red	Bhutan	Dark Red	Kuwait	Dark Red	Hungary
Dark Red	United Arab Emirates	Dark Red	Laos	Dark Red	Maldives	Dark Red	Austria	Dark Red	Sint Eustatius
Dark Red	Fiji	Dark Red	Pakistan	Dark Red	Marshall Islands	Dark Red	Bolivia	Dark Red	Iceland
Dark Red	Thailand	Dark Red	Vanuatu	Dark Red	Iraq	Dark Red	Iran	Dark Red	Svalbard
Dark Red	Italy	Dark Red	Papua New Guinea	Dark Red	Morocco	Dark Red	Lebanon	Dark Red	Bouvet Island
Dark Red	Canada	Dark Red	Vietnam	Dark Red	Suriname	Dark Red	Uruguay	Dark Red	Antigua and Barbuda
Dark Red	Cambodia	Dark Red	Saudi Arabia	Dark Red	Egypt	Dark Red	South Africa	Dark Red	Åland
Dark Red	Philippines	Dark Red	Mongolia	Dark Red	Turkey	Dark Red	Venezuela	Dark Red	Western Sahara
Dark Red	Oman	Dark Red	Solomon Islands	Dark Red	Palestine	Dark Red	Akrotiri and Dhekelia	Dark Red	British Virgin Islands
Dark Red		Dark Red		Dark Red	Dominican Republic	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Jordan	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Switzerland	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Paraguay	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Hong Kong	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Peru	Dark Red		Dark Red	

# Targeted Industries

Most



Least

# TOP 25 MITRE ATT&CK TTPS

## T1059

Command and Scripting Interpreter

## T1588

Obtain Capabilities

## T1588.006

Vulnerabilities

## T1566

Phishing

## T1068

Exploitation for Privilege Escalation

## T1036

Masquerading

## T1190

Exploit Public-Facing Application

## T1027

Obfuscated Files or Information

## T1041

Exfiltration Over C2 Channel

## T1588.005

Exploits

## T1204

User Execution

## T1574

Hijack Execution Flow

## T1082

System Information Discovery

## T1204.002

Malicious File

## T1083

File and Directory Discovery

## T1071

Application Layer Protocol

## T1203

Exploitation for Client Execution

## T1070

Indicator Removal

## T1105

Ingress Tool Transfer

## T1057

Process Discovery

## T1059.001

PowerShell

## T1071.001

Web Protocols

## T1078

Valid Accounts

## T1574.002

DLL Side-Loading

## T1547

Boot or Logon Autostart Execution



# Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>FudModule</u>	Domains	voyagorclub[.]space, weinsteinfrog[.]com
<u>Meow Ransomware</u>	SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9, 7f6421cdf6355edfdbcddadd26bcd9bf984def301df3c6c03d71af8e30bb781f, 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099, 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f, 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec
	SHA1	59e756e0da6a82a0f9046a3538d507c75eb95252, 987ad5aa6aee86f474fb9313334e6c9718d68daf, 94a9da09da3151f306ab8a5b00f60a38b077d594, 5949c404aee552fc8ce29e3bf77bd08e54d37c59, 578b1b0f46491b9d39d21f2103cb437bc2d71cac, 4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b
	MD5	8f154ca4a8ee50dc448181afbc95cfd7, 4dd2b61e0ccf633e008359ad989de2ed, 3eff7826b6eea73b0206f11d08073a68, 1d70020ddf6f29638b22887947dd5b9c, 033acf3b0f699a39becdc71d3e2dddcc, 0bbb9b0d573a9c6027ca7e0b1f5478bf
	TOR Address	meow6xanhzfcizgbkn3lmbqq7xjjufskkdfocqdngt3ltvzqgpg5mid[.]onion, totos7fqprkecvcs12jwy72v32glgkp2ejeqlnx5ynnxbvbebnletqd[.]onion
<u>RansomHub Ransomware</u>	SHA256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fabcc14801a, 342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b, 56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763
	TOR Address	ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
<u>DOWNBAIT</u>	SHA256	3b9ef9701ea2b2c1a89489ed0ed43ffabec9e22b587470899c0d5aca1a1e4302
<u>PULLBAIT</u>	SHA256	9dd62afdb4938962af9ff1623a0aa5aaa9239bcb1c7d6216f5363d14410a3369

Attack Name	TYPE	VALUE
<b><u>CBROVER</u></b>	SHA256	d8747574251c8b4ab8da4050ba9e1f6e8dbbaa38f496317b23da366e25d3028a, 7c520353045a15571061c3f6ae334e5f854d441bab417ebf497f21f5a8bc6925
	IPv4	18[.]163[.]112[.]181
<b><u>PLUGX</u></b>	SHA256	b37b244595cac817a8f8dba24fbeat08205e1d1321651237fe24fdcfac4f8ffc, de08f83a5d2421c86573dfb968293c776a830d900af2bc735d2ecd7e77961aaf, d32d7e86ed97509289fff89a78895904cf07a82824c053bfaf1bc5de3f3ba791, 046a03725df3104d02fa33c22e919cc73bed6fd6a905098e98c07f0f1b67fadb, 785d92dc175cb6b7889f07aa2a65d6c99e59dc1bbc9edb8f5827668fd249fa2e, f748b210677a44597a724126a3d97173d97840b59d6deaf010c370657afc01f8, ffa94d76d4423e43a42c7944c512e1a71827a89ad513d565f82eb8fe374ef74d
	Domain	www[.]ynsins[.]com, www[.]jaihkstore[.]com, www[.]bcller[.]com
<b><u>PUBLOAD</u></b>	MD5	7103a25d591a051aa37424bc3a9d0733
	SHA1	3e716409192e5023328920e67512185fea89b3b1
	SHA256	a062fafaff556b17a5ccb035c8c7b9d2015722d86a186b6b186a9c63eeb4308a, 14a9a74298408c65cb387574ffa8827abd257aa2b76f87efbaa1ee46e8763c57, 2e44ebe8d864ae19446d0853c51e471489c0893fc5ae2e042c01c7f232d2a2c2
	IPv4	103[.]15[.]29[.]17, 47[.]253[.]106[.]177
<b><u>Atlantida</u></b>	SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0
<b><u>Gootloader</u></b>	SHA256	b939ec9447140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988, c853d91501111a873a027bd3b9b4dab9dd940e89cfec51efbb6f0db0ba6687b
<b><u>Supper backdoor</u></b>	MD5	0b175136f48d88e094318cc78792b876, 032bf67c14d00b5468ce0aeab927c86c, 7ca12616c3e964dcf3dcc30f8ee6a18, f176d8ee8c58223c3a1ca5b1dff274b8, c1cd52785f2ca5ef177e259c7ae3596f

Attack Name	TYPE	VALUE
<u>Supper backdoor</u>	SHA267	4cd01348769bffa6623e9871ff2169de2f5e15f4c5128b232b666e0c62398cff
<u>INC Ransomware</u>	SHA256	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced
<u>EAGLEDOOR</u>	SHA256	b3b8efcaf6b9491c00049292cdf8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4bfa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7
	Domain	msa.hinet[.]ink
	IPv4	167[.]172[.]89[.]142, 167[.]172[.]84[.]142














# Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2024-7971</a></u>		Google Chrome V8 prior to 128.0.6613.84, Microsoft Edge	Citrine Sleet
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:google:chrome :*:*:*:*:*:*:*	FudModule
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1189: Drive-by Compromise T1204: User execution	<a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2024-20469</a></u>		Cisco Identity Services Engine (ISE) versions: 3.2 and 3.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:3.2.0:*:*:*:*:*	-
Cisco Identity Services Engine Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1068 : Exploitation for Privilege Escalation, T1059.008 Command and Scripting Interpreter: Network Device CLI	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-6kn9tSxm">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-6kn9tSxm</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-3519</a>		Citrix NetScaler ADC and NetScaler Gateway	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:adc:*:*:*:*:*:*:*	RansomHub Ransomware
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability		cpe:2.3:a:citrix:gateway:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<a href="https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467?language=en_US">https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467?language=en_US</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-27997</a>		Fortinet FortiOS and FortiProxy SSL-VPN	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*	RansomHub Ransomware
Fortinet heap-based buffer overflow Pre-Auth Vulnerability		cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1005: Data from Local System	<a href="https://www.fortiguard.com/psirt/FG-IR-23-097">https://www.fortiguard.com/psirt/FG-IR-23-097</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2023-46604</u></b>		Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	<b>ZERO-DAY</b>		
		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:a:apache:activemq.*.*.*.*.*.*	RansomHub Ransomware
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability		cpe:2.3:a:apache:activemq_legacy_openwire_module.*.*.*.*.*.*	
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-502	T1059: Command and Scripting Interpreter	<a href="https://activemq.apache.org/security-advisories.data/CVE-2023-46604">https://activemq.apache.org/security-advisories.data/CVE-2023-46604</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2023-22515</a></u>		Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*:*	RansomHub Ransomware
Atlassian Confluence Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	<a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2023-46747</a></u>		F5 BIG-IP Configuration Utility	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*	RansomHub Ransomware
F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306 CWE-288	T1190: Exploit Public-Facing Application	<a href="https://my.f5.com/manage/s/article/K000137353">https://my.f5.com/manage/s/article/K000137353</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2023-48788</u></b>		FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*	RansomHub Ransomware
Fortinet FortiClientEMS SQL Injection Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-89	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	<a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-007">https://fortiguard.fortinet.com/psirt/FG-IR-24-007</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2020-0787</u></b>		Microsoft Windows	-
	ZERO-DAY		
		AFFECTED CPE	
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:o:microsoft:windows:-*:*:*:*:*:*	RansomHub Ransomware
Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-59	T1068 : Exploitation for Privilege Escalation, T1059 : Command and Scripting Interpreter	<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0787">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0787</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-26360</a>		ColdFusion: 2016 update 15 and earlier versions ColdFusion: 2021 Update 5 and earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:2021:Update 5:*:*:*:*:*	RansomHub Ransomware
Adobe ColdFusion Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities	<a href="https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/">https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38014</a>		Windows: 10 - 11 23H2 Windows Server: 2008 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*	-
Windows Installer Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38217</a>		Windows: 10 - 11 23H2 Windows Server: 2008 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Windows Mark of the Web Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553.005: Mark-of-the-Web Bypass, T1204: User Execution	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38226</a>		Microsoft Publisher 2016 Microsoft Office LTSC 2021 Microsoft Office 2019	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:publisher:*:*:*:*:*	
Microsoft Publisher Security Feature Bypass Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553: Subvert Trust Controls, T1204: User Execution	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-43491</a>		Windows 10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Update Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting, T1562.010: Downgrade Attack	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-43461</a>		Windows: 10 - 11 23H2, Windows Server: 2008 – 2022 23H2	Void Banshee
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	Atlantida
Windows MSHTML Platform Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-451	T1059: Command and Scripting, T1204: User Execution	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461</a>









CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2024-41869</u></b>		Acrobat DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat Reader DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat 2024 Versions 24.001.30159 and earlier versions, Acrobat 2020 Versions 20.005.30655 and earlier versions, Acrobat Reader 2020 Versions 20.005.30655 and earlier versions	-
	<b>ZERO-DAY</b>		
		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RAN SOMWARE</b>
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:a:adobe:acrobat:*:*:*:*:*:* cpe:2.3:a:adobe:reader:*:*:*:*:*:*	-
Adobe Acrobat and Reader Use After Free Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-416	T1203: Exploitation for Client Execution, T1204: User Execution	<a href="https://helpx.adobe.com/security/products/acrobat/apsb24-70.html">https://helpx.adobe.com/security/products/acrobat/apsb24-70.html</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-8190</u>		CSA 4.6 (All versions before Patch 519)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6-:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*	-
Ivanti Cloud Services Appliance OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE- 78	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	<a href="https://forums.ivanti.com/s/article/CSA-4-6-Patch-519">https://forums.ivanti.com/s/article/CSA-4-6-Patch-519</a> , <a href="https://forums.ivanti.com/s/article/CSA-5-0-Download">https://forums.ivanti.com/s/article/CSA-5-0-Download</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-8963</u>		CSA 4.6 (All versions before Patch 519)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6-:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*	-
Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter	<a href="https://forums.ivanti.com/s/article/CSA-4-6-Patch-519">https://forums.ivanti.com/s/article/CSA-4-6-Patch-519</a> , <a href="https://forums.ivanti.com/s/article/CSA-5-0-Download">https://forums.ivanti.com/s/article/CSA-5-0-Download</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-38112</a>		Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	Void Banshee APT
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	Atlantida
Microsoft Windows MSHTML Platform Spoofing Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-451	T1059: Command and Scripting, T1204: User Execution	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-29847</a>		Ivanti Endpoint Manager 2022 SU5 and prior Ivanti Endpoint Manager 2024	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*	-
Ivanti Endpoint Manager Deserialization of Untrusted Data Vulnerability		*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	<a href="https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022">https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-38831</u></a>		WinRAR version 6.22 and older versions	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*	PhantomDL, PhantomCore, LockBit ransomware, Babuk ransomware
RARLAB WinRAR Code Execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions
	CWE-20		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-6670</u></a>		Progress WhatsUp Gold versions released before 2024.0.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:progress:what sup_gold:*:*:*:*:*:*	-
Progress WhatsUp Gold SQL Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	<a href="https://community.progress.com/s/article/WhatsApp-Gold-Security-Bulletin-August-2024">https://community.progress.com/s/article/WhatsApp-Gold-Security-Bulletin-August-2024</a>
	CWE-89		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-36401</u></a>		GeoServer	Earth Baxia
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:geoserver:geoserver:*.~.*.*.*.*.*.*.*	EAGLEDOOR, RIPCOY
OSGeo GeoServer GeoTools Eval Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	<a href="https://geoserver.org/download/">https://geoserver.org/download/</a> ; <a href="https://sourceforge.net/projects/geotools/files/">https://sourceforge.net/projects/geotools/files/</a>
	CWE-95		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-7593</u></a>		Ivanti Virtual Traffic Manager Versions: 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:vtm:*:*:*:*.*.*.*	-
Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability			
	CWE ID	T1068 : Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593</a>
	CWE-287, CWE-303		

# 🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">FudModule</a></u>	<p>FudModule is an advanced rootkit malware developed by the North Korean threat actor group Citrine Sleet. FudModule is designed to gain admin-to-kernel access on Windows systems, enabling the attackers to read and write arbitrary kernel memory. This allows FudModule to disable various security monitoring features by modifying kernel variables and removing kernel callbacks, affecting security products like EDRs, firewalls, and antimalware tools.</p>	Exploit vulnerabilities	CVE-2024-7971
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Rootkit			
<b>ASSOCIATED ACTOR</b>			
Citrine Sleet	System compromise	<b>PATCH LINK</b>	<a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">Meow Ransomware</a></u>	<p>The Meow ransomware variant emerged in late 2022, originating from the leak of Conti's ransomware strain. Despite a temporary halt following the release of a free decryptor in March 2023, Meow resurfaced in 2024, swiftly claiming new victims. It is suspected that the latest version may now operate primarily as an extortion group.</p>	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			
<b>ASSOCIATED ACTOR</b>			
-	Encrypt files, System compromise	<b>PATCH LINK</b>	-

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>Emansrepo Stealer</u></a>	Emansrepo is a Python-based infostealer, first observed in November 2023, that spreads via phishing emails disguised as purchase orders and invoices. This malware primarily targets browser directories and specific file paths, collecting sensitive data from victims.	Phishing	-	
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
Stealer				Microsoft Windows
<b>ASSOCIATED ACTOR</b>			Data theft	<b>PATCH LINK</b>
-				-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<a href="#"><u>BlotchyQuasar</u></a>	BlotchyQuasar malware is a variant of QuasarRAT. It enables keylogging, browser data theft, and surveillance of financial transactions.	Phishing	-	
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
RAT				-
<b>ASSOCIATED ACTOR</b>			Information Theft, Compromise Infrastructure, Financial Gains	<b>PATCH LINK</b>
Blind Eagle				-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<a href="#"><u>CXCLNT</u></a>	CXCLNT acts as a backdoor, enabling communication between the compromised system and the command-and-control (C&C) server. It supports basic file upload and download capabilities, as well as features for erasing traces, gathering victim information, and downloading additional portable executable (PE) files for further execution.	-	-	
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
Backdoor				Windows
<b>ASSOCIATED ACTOR</b>			Information Theft, Compromise Infrastructure	<b>PATCH LINK</b>
TIDRONE				-

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>RansomHub Ransomware</u></a>	<p>RansomHub, a ransomware-as-a-service (RaaS) platform, has rapidly gained prominence in the cybercriminal landscape since February 2024. Responsible for targeting over 200 victims across various industries, RansomHub's affiliates employ a 'double extortion' tactic, encrypting and exfiltrating sensitive data to pressure victims into paying a ransom.</p>	Phishing, Exploiting vulnerabilities	CVE-2023-3519 CVE-2023-27997 CVE-2023-46604 CVE-2023-22515 CVE-2023-46747 CVE-2023-48788 CVE-2017-0144 CVE-2020-1472 CVE-2020-0787
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Data Theft	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			<a href="https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467">https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467</a> ; <a href="https://www.fortiguard.com/psirt/FG-IR-23-097">https://www.fortiguard.com/psirt/FG-IR-23-097</a> ; <a href="https://activemq.apache.org/security-advisories.data/CVE-2023-46604">https://activemq.apache.org/security-advisories.data/CVE-2023-46604</a> ; <a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a> ; <a href="https://my.f5.com/manage/s/article/K000137353">https://my.f5.com/manage/s/article/K000137353</a> ; <a href="https://www.fortiguard.com/psirt/FG-IR-24-007">https://www.fortiguard.com/psirt/FG-IR-24-007</a> ; <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144</a> ; <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472</a> ; <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0787">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0787</a>

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>China Chopper</u>	<p>China Chopper is a malicious web shell, a type of software that allows attackers to remotely access and control compromised web servers. It's a popular tool among cybercriminals due to its versatility and ease of use. It allows attackers to steal data, compromise systems, and persist on networks.</p>	-	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360
TYPE		IMPACT	AFFECTED PRODUCTS
Web shell		Data Theft, System compromise	-
ASSOCIATED ACTOR			PATCH LINK
Tropic Trooper			<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473;</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523;</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207;</a> <a href="https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html">https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html</a>

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>Crowdoor</u>	<p>Crowdoor is a loader tool, a type of malware that is used to download and install other malicious software onto compromised systems. It is associated with the SparrowDoor backdoor, a persistent threat that provides attackers with remote access to infected systems. Crowdoor is known for its ability to evade detection by traditional security measures, making it a challenging threat to address.</p>	-	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft, System compromise	-
ASSOCIATED ACTOR			PATCH LINK
Tropic Trooper			<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473;</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523;</a> <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207;</a> <a href="https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html">https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html</a>

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>CLNTEND</u>	CLNTEND serves as a remote shell, providing attackers with full control over the infected system. It communicates with the C&C server using multiple protocols.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Information Theft, Compromise Infrastructure	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
TIDRONE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Fog ransomware (aka Lost in the Fog)</u>	Fog ransomware utilizes techniques such as 'pass-the-hash' attacks to escalate privileges, enabling it to access administrator accounts. Encrypted files typically receive the extensions .FOG or .FLOCKED.	Compromised Virtual Private Network (VPN) credentials	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Sensitive Information Theft, Financial Loss, Compromised Infrastructure, Exfiltration of data	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-

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><u>DOWNBAIT</u></b>	DOWNBAIT is a multi-stage downloader that retrieves a decoy document from an attacker-controlled server, while the server simultaneously delivers other malware.	Spear Phishing Emails	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Downloader		Information Theft, Compromise Infrastructure, Remote Control	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Mustang Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>PULLBAIT</u></b>	PULLBAIT is a lightweight shellcode that operates directly in memory. It performs further downloads and executions of additional malware.	DOWNBAIT deploys	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Downloader		Information Theft, Compromise Infrastructure	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Mustang Panda			-

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><u>CBROVER</u></b>	CBROVER is a first-stage backdoor that supports file download and remote shell execution. It is spawned using DLL side-loading techniques.	PULLBAIT deploys	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Information Theft, Remote Control, Infrastructure Compromise	-
Backdoor			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
Mustang Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>PLUGX</u></b>	PLUGX is a second-stage payload protected with RC4 and DPAPI. It injects its code into other processes that are launched with varying arguments.	Deployed by other malware, or via exploited vulnerabilities in web applications	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Information Theft, Espionage, Remote Control, Infrastructure Compromise	-
RAT			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
Mustang Panda, DragonRank			-

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><u>PUBLOAD (aka ClaimLoader)</u></b>	The variant of HIUPAN spreads through removable drives to deliver PUBLOAD. PUBLOAD was used as the main control tool for most of the campaign and to perform various tasks, including executing tools such as RAR for collection and curl for data exfiltration. PUBLOAD was also used to introduce supplemental tools into the targets' environments.	HIUPAN spreads through removable drives	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Information Theft, Espionage, Exfiltration	-
Downloader			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
Mustang Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>BadIIS</u></b>	BadIIS is malware used to manipulate search engine crawlers and disrupt the SEO of affected sites. The proxy feature of BadIIS is configured to permit access to certain URL paths and to impose restrictions on specific file types based on their extensions.	Exploit vulnerabilities in web applications	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Information Theft, Compromise Infrastructure	-
Backdoor			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
DragonRank			-

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><a href="#">Atlantida</a></u>	<p>Atlantida stealer is an info-stealer malware targeting sensitive information from various applications, including Telegram, Steam, FileZilla, cryptocurrency wallets, and web browsers. This malware extracts stored sensitive and potentially valuable data, such as passwords and cookies, and collects files with specific extensions from the infected system's desktop. Additionally, Atlantida stealer captures the victim's screen and gathers comprehensive system information, enhancing its ability to exploit compromised systems.</p>	Exploiting Vulnerabilities	CVE-2024-43461 CVE-2024-38112
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information stealer			
<b>ASSOCIATED ACTOR</b>		Microsoft Windows	<b>PATCH LINK</b>
Void Banshee APT			
	Data theft		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">LockBit ransomware</a></u>	<p>LockBit is a prominent ransomware-as-a-service (RaaS) operation known for its aggressive tactics. It employs data encryption and exfiltration, demanding high ransoms. The group has evolved through multiple versions, each with enhanced capabilities, making it a persistent and sophisticated threat to organizations worldwide.</p>	Phishing, Exploiting Vulnerability	CVE-2023-38831
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			
<b>ASSOCIATED ACTOR</b>		Data encryption	<b>PATCH LINK</b>
Head Mare			
	Upgrade to WinRAR version 6.23 or later		

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>Gomorrah Stealer</u></a>	Gomorrah Stealer is an advanced piece of malware designed to steal sensitive information from compromised systems. It uses various evasion techniques to avoid detection while gathering data from multiple sources, including the Windows registry, web browsers, VPNs, cryptocurrency wallets, and configuration files. Its primary functions include stealing passwords, accessing cryptocurrency wallets, and loading additional tasks and payloads.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information stealer			
<b>ASSOCIATED ACTOR</b>		Data theft	Windows
-			<b>PATCH LINK</b>
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>PhantomDL</u></a>	PhantomDL is a Go-based backdoor malware designed for delivering additional payloads and exfiltrating files to a command-and-control (C2) server. This backdoor enables attackers to maintain persistent access to compromised systems, allowing them to deploy further malicious software and steal sensitive data.	Phishing, Exploiting Vulnerability	CVE-2023-38831
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		Remote access	WinRAR
-			<b>PATCH LINK</b>
Head Mare	Upgrade to WinRAR version 6.23 or later		

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>PhantomCore</u></a>	PhantomCore, also known as PhantomRAT, is the predecessor to PhantomDL. PhantomCore was a remote access trojan (RAT) that provided attackers with control over compromised systems, enabling them to steal data, execute commands, and deploy additional malware.	Phishing, Exploiting Vulnerability	CVE-2023-38831
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			WinRAR
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Head Mare			Upgrade to WinRAR version 6.23 or later
		Remote control	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Babuk ransomware</u></a>	Babuk is a ransomware strain that emerged in 2021, targeting large enterprises. Initially focusing on data encryption for ransom, the group later shifted to data theft and extortion. Known for its aggressive tactics and leaked source code.	Phishing, Exploiting Vulnerability	CVE-2023-38831
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			WinRAR
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Head Mare			Upgrade to WinRAR version 6.23 or later
		Data encryption	

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>SambaSpy RAT</u>	SambaSpy is a sophisticated, Java-based remote access trojan (RAT) obfuscated with Zelix KlassMaster, featuring encrypted strings and obfuscated class names to evade detection, with capabilities that include file and process management, webcam control, keystroke logging, clipboard control, screenshot capture, remote desktop management, password stealing, plugin loading at runtime, remote shell access, and victim interaction.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Remote control	-
-			<b>PATCH LINK</b>
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Supper backdoor</u>	Supper backdoor is a malicious software used by cyber threat actors like Vanilla Tempest to gain persistent access to compromised systems. It allows attackers to remotely control infected devices, execute commands, and exfiltrate sensitive data. Supper is often deployed in conjunction with other malware, such as ransomware, to maximize the impact of attacks.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		Remote access	-
Vanilla Tempest, Storm-0494			<b>PATCH LINK</b>
-	-		

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><u>INC Ransomware</u></b>	Inc. ransomware is an extortion operation that emerged in July 2023, positioning itself as a "service" to victims. This ransomware group employs a multi-extortion approach, stealing sensitive data and threatening to leak it online if their demands are not met.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			-
<b>ASSOCIATED ACTOR</b>		Data encryption	<b>PATCH LINK</b>
Vanilla Tempest, Storm-0494			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>Gootloader</u></b>	Gootloader is a JScript-based malware family known for using SEO poisoning and compromised websites to trick victims into downloading a ZIP archive that appears to be a legitimate document. Once executed, Gootloader checks if the infected system is connected to an Active Directory domain before deploying multiple stages of JScript and PowerShell payloads, which can lead to various threats.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Loader			-
<b>ASSOCIATED ACTOR</b>		Loads malware/ Malware execution	<b>PATCH LINK</b>
Vanilla Tempest, Storm-0494			-

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>Diamorphine</u>	Diamorphine is a Linux rootkit that allows attackers to hide processes, files, and network connections from system monitoring tools. It operates at the kernel level, making it difficult to detect and remove. Often used to maintain covert access, it grants attackers elevated privileges and can manipulate logs.	Exploit vulnerabilities	-	
<b>TYPE</b>		<b>IMPACT</b>	AFFECTED PRODUCTS	
Rootkit				CentOS
<b>ASSOCIATED ACTOR</b>			Stealthy access and System control	PATCH LINK
TeamTNT				-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>EAGLEDOOR</u>	EAGLEDOOR is a backdoor malware linked to Earth Baxia, used in their cyberespionage campaigns. It allows attackers to remotely execute commands on compromised systems, enabling them to control infected devices and steal sensitive data. EAGLEDOOR is deployed through spear-phishing attacks and exploits vulnerabilities, including in platforms like GeoServer.	Exploit vulnerabilities and Spear-phishing	CVE-2024-36401	
<b>TYPE</b>		<b>IMPACT</b>	AFFECTED PRODUCTS	
Backdoor				GeoServer
<b>ASSOCIATED ACTOR</b>			Unauthorized access	PATCH LINK
Earth Baxia				<a href="https://geoserver.org/download/">https://geoserver.org/download/</a>

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><u>PondRAT</u></b>	PondRAT is a lightweight Linux and macOS remote access trojan (RAT) discovered in a campaign using poisoned Python packages. It shares significant code similarities with POOLRAT, malware attributed to the North Korean threat actor Gleaming Pisces. PondRAT facilitates file uploads, downloads, command execution, and system control for attackers.	Python software packages	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>			Unauthorized access
Gleaming Pisces	--		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>POOLRAT</u></b>	POOLRAT, also known as SIMPLESEA, is a macOS backdoor attributed to the North Korean hacking group Gleaming Pisces, specifically used in sophisticated supply chain attacks. This malware enables attackers to gain remote access to infected systems, allowing for file manipulation, command execution, and data exfiltration. Recent analyses reveal that POOLRAT shares significant code similarities with newer malware variants like PondRAT.	Python software packages	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>			Unauthorized access
Gleaming Pisces	--		

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><u>BURNBOOK</u></b>	BURNBOOK is a malware loader designed to download and execute additional malicious payloads onto infected systems. It acts as an intermediary, facilitating the launch of more harmful malware like ransomware or spyware. BURNBOOK typically operates covertly, evading detection while delivering its secondary payloads to targets.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Loads other malware and espionage	-
Loader			
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Lazarus Group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>TEARPAGE</u></b>	TEARPAGE is a malicious loader used by North Korean Lazarus cyber espionage group. It operates through DLL search order hijacking, facilitating the execution of the MISTPEN backdoor by decrypting an encrypted payload from a file located in the user's AppData directory.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Loads other malware and espionage	-
Loader			
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Lazarus Group			-

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><u>MISTPEN</u></b>	MISTPEN is a lightweight backdoor written in C, primarily designed to download and execute Portable Executable (PE) files from command-and-control (C2) servers. MISTPEN employs sophisticated evasion techniques, including encrypted communications and stealthy operations, making it particularly dangerous for critical sectors like energy and aerospace.	Through BURNBOOK and TEARPAGE	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		-	
Backdoor			
<b>ASSOCIATED ACTOR</b>		<b>PATCH LINK</b>	
Lazarus Group	--		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>SnipBot</u></b>	SnipBot, a newly identified variant from the RomCom malware family, employs advanced infection and evasion techniques. Typically delivered via phishing emails posing as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. This malware showcases capabilities for remote command execution and data exfiltration while using anti-sandbox methods to evade detection.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Windows	
RAT			
<b>ASSOCIATED ACTOR</b>		<b>PATCH LINK</b>	
-	-		

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><u>RomCom</u></b>	RomCom malware is a sophisticated cyber threat that emerged in 2022, used primarily for cyber espionage and ransomware campaigns. It typically involves phishing emails or malicious software disguised as legitimate programs to infiltrate systems. Once inside, it steals sensitive information and can manipulate network configurations to expand its reach.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Remote control and data theft	<b>PATCH LINK</b>
-			--

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>KLogEXE</u></b>	KLogEXE is a keylogger used by the Kimsuky group, designed to capture keystrokes and steal sensitive information like credentials. It operates stealthily, using anti-detection and anti-analysis techniques to evade cybersecurity defenses. This tool is a critical part of Sparkling Pisces's espionage campaigns, particularly against South Korean targets.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Keylogger			
<b>ASSOCIATED ACTOR</b>		Data theft and Keystroke recording	<b>PATCH LINK</b>
Sparkling Pisces			-

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><u>FPSpy</u></b>	FPSpy is a malware variant associated with the North Korean threat group Sparkling Pisces, primarily delivered through spear-phishing emails containing malicious ZIP file attachments. It functions as a backdoor, capable of gathering system information, executing arbitrary commands, and enumerating files on compromised machines.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Remote control and data theft	-
Backdoor			
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Sparkling Pisces			--


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>RIPCOY</u></b>	RIPCOY is a malware variant employed by the Earth Baxia threat group, typically distributed via spear-phishing emails with ZIP file attachments. RIPCOY employs the GrimResource technique to download malicious files from a public cloud service, typically AWS, after tricking users into executing an obfuscated VBScript within a decoy MSC or Ink file.	Phishing	CVE-2024-36401
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Unauthorized access	GeoServer
Trojan			
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Baxia			<a href="https://geoserver.org/download/">https://geoserver.org/download/</a>


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

# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b>Citrine Sleet</b> (aka Lazarus, Labyrinth Chollima, Group 77, Hastati Group, Who is Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</p>	North Korea	Cryptocurrency, Financial, Energy, Aerospace	Worldwide
	<b>MOTIVE</b>		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-7971	FudModule, PondRAT, POOLRAT, BURNBOOK, TEARPAGE, MISTPEN Backdoor	Google Chrome, Microsoft Edge, Linux and macOS
<b>TTPs</b>			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0040: Impact; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1189: Drive-by Compromise; T1566: Phishing; T1014: Rootkit; T1036: Masquerading; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1176: Browser Extensions; T1553: Subvert Trust Controls; T1565: Data Manipulation			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Tropic Trooper (aka Pirate Panda, APT 23, KeyBoy, Iron, Bronze Hobart, Earth Centaur)</u>	China	Government	The Middle East, and Malaysia
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360	China Chopper, Crowdoor	-	
<b>TTPs</b>			
TA0002: Execution; TA0042: Resource Development; TA0004: Privilege Escalation; TA0001: Initial Access; TA0006: Credential Access; T1218: System Binary Proxy Execution; T1059: Command and Scripting Interpreter; TA0003: Persistence; TA0007: Discovery; T1068: Exploitation for Privilege Escalation; TA0043: Reconnaissance; TA0005: Defense Evasion; TA0011: Command and Control; T1588.006: Vulnerabilities; T1588.005: Exploits; T1059.007: JavaScript; T1027: Obfuscated Files or Information; T1218.007: Msiexec; T1218.011: Rundll32; T1055: Process Injection; T1505.003: Web Shell; T1547.001: Registry Run Keys /Startup Folder; T1046: Network Service Discovery; T1574.001: DLL Search Order Hijacking; T1547: Boot or Logon Autostart Execution; T1574: Hijack Execution Flow; T1543; T1543.003: Windows Service; T1090: Create or Modify System Process; T1003.001: LSASS Memory; T1190: Exploit Public-Facing Application; T1588: Obtain Capabilities; T1003: OS Credential Dumping; T1090: Proxy; T1018: Remote System Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b><u>Blind Eagle (aka AguilasCiega, APT-C-36, APT-Q-98)</u></b></p>	Colombia	Insurance, Banking Services, Financial	Colombia, Ecuador
	<b>MOTIVE</b>		
	Information theft, Espionage, Financial crime		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	BlotchyQuasar RAT	-
<b>TTPs</b>			
<p>TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1056.002: GUI Input Capture; T1095: Non-Application Layer Protocol; T1583: Acquire Infrastructure; T1583.001: Domains; T1586: Compromise: Accounts; T1586.002: Email Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1608: Stage Capabilities; T1608.001: Upload Malware; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053.005: Scheduled Task; T1562.001: Disable or Modify Tools; T1564.001: Hidden Files and Directories; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1553.005: Mark-of-the-Web Bypass; T1027.002: Software Packing; T1140: Deobfuscate/Decode Files or Information; T1056.001: Keylogging; T1056: Input Capture; T1539: Steal Web Session Cookie; T1041: Exfiltration Over C2 Channel; T1490: Inhibit System Recovery; T1036: Masquerading</p>			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
 <b>TIDRONE</b>	Chinese-speaking threat actor	Military, Satellite, Drone Manufacturing Sector	Taiwan
	<b>MOTIVE</b>		
	Information Theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	CXCLNT, CLNTEND	-

### TTPs


TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1203: Exploitation for Client Execution; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1040: Network Sniffing; T1212: Exploitation for Credential Access; T1083: File and Directory Discovery; T1012: Query Registry; T1057: Process Discovery; T1119: Automated Collection; T1021.001: Remote Desktop Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1082: System Information Discovery; T1070: Indicator Removal; T1543: Create or Modify System Process; T1055: Process Injection; T1560: Archive Collected Data; T1071.002: File Transfer Protocols; T1071: Application Layer Protocol; T1021: Remote Services; T1105: Ingress Tool Transfer

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Void Banshee APT</u>	-	All	All
	<b>MOTIVE</b> Financial Gain, Information Theft		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSO MWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-43461 CVE-2024-38112	Atlantida	Microsoft Windows
	<b>TTPs</b>		
TA0004: Privilege Escalation; TA0042: Resource Development; TA0005: Defense Evasion; TA0002: Execution; T1068: Exploitation for Privilege Escalation; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits; T1204: User Execution; T1204.002: Malicious File; T1036: Masquerading; T1059: Command and Scripting Interpreter; T1587.001: Malware; T1587: Develop Capabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <b>Mustang Panda</b> <b>(aka Earth Preta, Stately Taurus, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG)</b>	China	Government, Military, Foreign Affair, Education	Asia-Pacific (APAC)
	<b>MOTIVE</b> Information Theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	DOWNBAIT, PULLBAIT, CBROVER, PLUGX, PUBLOAD (aka ClaimLoader)	-

### TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1091: Replication Through Removable Media; T1566: Phishing; T1566.001: Spearphishing Attachment; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053.005: Scheduled Task; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1480.001: Environmental Keying; T1553.002: Code Signing; T1055: Process Injection; T1518: Software Discovery; T1518.001: Security Software Discovery; T1049: System Network Connections Discovery; T1016: System Network Configuration Discovery; T1005: Data from Local System; T1560.001: Archive via Utility; T1567.002: Exfiltration to Cloud Storage; T1048: Exfiltration Over Alternative Protocol; T1071.001: Web Protocols


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>DragonRank</b>	China	Jewelry, media, research services, healthcare, video and television production, manufacturing, transportation, religious and spiritual organizations, IT services, international affairs, agriculture, sports, and even niche markets	Thailand, India, Korea, Belgium, Netherlands and China
	<b>MOTIVE</b>		
	Information Theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	PlugX and BadIIIS	Windows
<b>TTPs</b>			
<p>TA0007: Discovery; TA0008: Lateral Movement; TA0042: Resource Development; TA0003: Persistence; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0011: Command and Control; TA0009: Collection; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1016: System Network Configuration Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1069.001: Local Groups; T1082: System Information Discovery; T1555 : Credentials from Password Stores; T1505.003: Web Shell; T1505: Server Software Component; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1055: Process Injection; T1608.006: SEO Poisoning; T1608: Stage Capabilities; T1547: Boot or Logon Autostart Execution; T1090: Proxy; T1584.004: Server; T1584: Compromise Infrastructure; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1059: Command and Scripting Interpreter; T1218.011: Rundll32; T1218.007: Msiexec T1218: System Binary Proxy Execution; T1547.001: Registry Run Keys / Startup Folder; T1113: Screen Capture</p>			




NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Head Mare</u></p>	Linked to Russian-speaking	Government, Transportation, Energy, Manufacturing, Entertainment	Russia and Belarus
	<b>MOTIVE</b>		
	Information Theft, Espionage, Financial Gain, Hacktivism		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSO MWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2023-38831	PhantomDL, PhantomCore, LockBit ransomware, Babuk ransomware	WinRAR

**TTPs**


TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1012: Query Registry; T1105: Ingress Tool Transfer; T1497.001: System Checks; T1566: Phishing; T1203: Exploitation for Client Execution; T1071: Application Layer Protocol; T1219: Remote Access Software; T1486: Data Encrypted for Impact; T1003: OS Credential Dumping; T1562: Impair Defenses; T1543: Create or Modify System Process; T1571: Non-Standard Port; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1041: Exfiltration Over C2 Channel


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
  <u>Vanilla Tempest (DEV-0832, Vice Society)</u>	-	Education, Healthcare, IT, and Manufacturing	United States, United Kingdom, Canada, Australia, Germany, China
	<b>MOTIVE</b>		
	Financial Gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSO MWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	INC Ransomware, Gootloader, Supper backdoor	-
<b>TTPs</b>			
TA0004: Privilege Escalation; TA0042: Resource Development; TA0002: Execution; TA0005: Defense Evasion; TA0003: Persistence; TA0008: Lateral Movement; TA0040: Impact; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1068: Exploitation for Privilege Escalation T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1047: Windows Management Instrumentation; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b>TeamTNT</b> (aka <b>Adept Libra</b>)</p>	Germany	Cryptocurrency, Financial	Worldwide
	<b>MOTIVE</b>		
	Information theft and Financial gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	-	CentOS

### TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1110: Brute Force; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1083: File and Directory Discovery; T1490: Inhibit System Recovery; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1222: File and Directory Permissions Modification; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1562.003: Impair Command History Logging; T1562.004: Disable or Modify System Firewall; T1562.012: Disable or Modify Linux Audit System; T1070: Indicator Removal; T1070.006: Timestomp; T1014: Rootkit; T1609: Container: Administration Command; T1053: Scheduled Task/Job; T1053.003: Cron; T1583.003: Virtual Private Server; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>Earth Baxia</b>	China	Government, Telecommunication, and Energy	Asia–Pacific
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-36401	EAGLEDOOR	GeoServer
<b>TTPs</b>			
TA0007: Discovery; TA0011: Command and Control; T1566.001: Spearphishing Attachment; T1574.002: DLL Side-Loading; TA0005: Defense Evasion; TA0010: Exfiltration; T1566: Phishing; TA0001: Initial Access; T1071.001: Web Protocols: TTPs; TA0002: Execution; T1071.004: DNS; T1574.014: AppDomainManager; T1574: Hijack Execution Flow; T1027.010: Command Obfuscation; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1082: System Information Discovery; T1620; T1190: Reflective Code Loading Exploit Public-Facing Application; T1001: Data Obfuscation; T1071: Application Layer Protocol; T1027.013: Encrypted/Encoded File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Sparkling Pisces (aka Kimsuky, Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394)</u></p>	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks	South Korea and Japan
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	KLogEXE and FPSpy	-	
<b>TTPs</b>			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1070: Indicator Removal; T1070.006: Timestomp; T1041: Exfiltration Over C2 Channel; T1056: Input Capture; T1056.001: Keylogging; T1105: Ingress Tool Transfer; T1048: Exfiltration Over Alternative Protocol; T1082: System Information Discovery; T1083: File and Directory Discovery; T1074: Data Staged; T1057: Process Discovery; T1027: Obfuscated Files or Information			

# MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
<b>TA0043: Reconnaissance</b>	T1595: Active Scanning	
	T1592: Gather Victim Host Information	
	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1598.003: Spearphishing Link	
<b>TA0042: Resource Development</b>	T1584: Compromise Infrastructure	T1584.008: Network Devices T1584.004: Server
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities T1588.005: Exploits T1588.003: Code Signing Certificates
	T1583: Acquire Infrastructure	T1583.001: Domains T1583.003: Virtual Private Server
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1608: Stage Capabilities	T1608.001: Upload Malware T1608.006: SEO Poisoning
	T1566: Phishing	T1566.002: Spearphishing Link T1566.001: Spearphishing Attachment
	T1189: Drive-by Compromise	
<b>TA0001: Initial Access</b>	T1133: External Remote Services	
	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
	T1078.001: Default Accounts	
	T1091: Replication Through Removable Media	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
	T1129: Shared Modules	
<b>TA0002: Execution</b>	T1059: Command and Scripting Interpreter	T1059.001: PowerShell T1059.005: Visual Basic T1059.006: Python T1059.008: Network Device CLI T1059.003: Windows Command Shell T1059.004: Unix Shell T1059.007: JavaScript
	T1204: User Execution	T1204.002: Malicious File
	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1204.001: Malicious Link	
	T1203: Exploitation for Client Execution	
	T1609: Container Administration Command	

Tactic	Technique	Sub-technique
<b>TA0003: Persistence</b>	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1136: Create Account	
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1137: Office Application Startup	
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking T1574.002: DLL Side-Loading T1574.014: AppDomainManager
	<b>TA0004: Privilege Escalation</b>	T1055: Process Injection
T1053: Scheduled Task/Job		T1053.003: Cron T1053.005: Scheduled Task
T1078: Valid Accounts		T1078.001: Default Accounts
T1484: Domain or Tenant Policy Modification		T1484.002: Trust Modification
T1068: Exploitation for Privilege Escalation		
T1098: Account Manipulation		
T1543: Create or Modify System Process		T1543.003: Windows Service
T1547: Boot or Logon Autostart Execution		T1547.001: Registry Run Keys / Startup Folder
T1548: Abuse Elevation Control Mechanism		T1548.002: Bypass User Account Control
T1574: Hijack Execution Flow		T1574.001: DLL Search Order Hijacking T1574.002: DLL Side-Loading T1574.014: AppDomainManager
<b>TA0005: Defense Evasion</b>		T1014: Rootkit
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.003: Steganography
		T1027.005: Indicator Removal from Tools
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
	T1027.013: Encrypted/Encoded File	
	T1036.005: Match Legitimate Name or Location	
T1036: Masquerading		
T1055: Process Injection		

Tactic	Technique	Sub-technique
<b>TA0005: Defense Evasion</b>	T1078: Valid Accounts	T1078.001: Default Accounts
	T1140: Deobfuscate/Decode Files or Information	
	T1480.001: Environmental Keying	
	T1550.002: Pass the Hash	
	T1550: Use Alternate Authentication Material	
	T1070: Indicator Removal	T1070.004: File Deletion T1070.006: Timestomp
	T1218: System Binary Proxy Execution	T1218.007: Msiexec T1218.011: Rundll32
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1564.001: Hidden Files and Directories	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.003: Impair Command History Logging
		T1562.004: Disable or Modify System Firewall
		T1562.012: Disable or Modify Linux Audit System
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
		T1574.014: AppDomainManager
	T1622: Debugger Evasion	
	T1620: Reflective Code Loading	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
		T1553.002: Code Signing
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1484: Domain or Tenant Policy Modification	T1484.002: Trust Modification
T1556: Modify Authentication Process		
<b>TA0006: Credential Access</b>	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1040: Network Sniffing	
	T1556: Modify Authentication Process	
	T1110.003: Password Spraying	
	T1110: Brute Force	
	T1539: Steal Web Session Cookie	
	T1212: Exploitation for Credential Access	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers



Tactic	Technique	Sub-technique	
<b>TA0007: Discovery</b>	T1010: Application Window Discovery		
	T1012: Query Registry		
	T1016: System Network Configuration Discovery		
	T1018: Remote System Discovery		
	T1033: System Owner/User Discovery		
	T1040: Network Sniffing		
	T1046: Network Service Discovery		
	T1049: System Network Connections Discovery		
	T1057: Process Discovery		
	T1069.001: Local Groups		
	T1082: System Information Discovery		
	T1083: File and Directory Discovery		
	T1135: Network Share Discovery		
	T1217: Browser Information Discovery		
	T1622: Debugger Evasion		
	T1518: Software Discovery	T1518.001: Security Software Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks	
<b>TA0008: Lateral Movement</b>	T1021: Remote Services	T1021.001: Remote Desktop Protocol	
	T1080: Taint Shared Content		
	T1210: Exploitation of Remote Services		
	T1091: Replication Through Removable Media		
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash	
<b>TA0009: Collection</b>	T1560: Archive Collected Data	T1560.001: Archive via Utility	
	T1056: Input Capture	T1056.001: Keylogging	
		T1056.002: GUI Input Capture	
	T1005: Data from Local System		
	T1115: Clipboard Data		
	T1119: Automated Collection		
	T1213: Data from Information Repositories		
	T1074: Data Staged		
T1113: Screen Capture			
<b>TA0011: Command and Control</b>	T1001: Data Obfuscation		
		T1071.001: Web Protocols	
	T1071: Application Layer Protocol	T1071.004: DNS	
		T1071.002: File Transfer Protocols	
	T1090: Proxy		
	T1095: Non-Application Layer Protocol		
	T1105: Ingress Tool Transfer		
	T1219: Remote Access Software		
	T1571: Non-Standard Port		
T1573: Encrypted Channel			
<b>TA0010: Exfiltration</b>	T1048: Exfiltration Over Alternative Protocol	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
		T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol	

Tactic	Technique	Sub-technique
<b>TA0010: Exfiltration</b>	T1537: Transfer Data to Cloud Account	
	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1567.002: Exfiltration to Cloud Storage	
<b>TA0040: Impact</b>	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1499: Endpoint Denial of Service	
	T1498: Network Denial of Service	
	T1561: Disk Wipe	T1561.001: Disk Content Wipe
	T1565: Data Manipulation	

# Top 5 Takeaways

## #1

In **September**, there were **fifteen zero-day** vulnerabilities, with the 'Three Celebrity Vulnerabilities' taking center stage. These featured flaws such as **ZeroLogon, EternalBlue, and PROXYSHELL**.

## #2

Over the course of the month, a variety of ransomware variants, including **Meow, RansomHub, Fog, LockBit, Babuk, and INC Ransomware**. **RansomHub**, a ransomware-as-a-service (RaaS) platform, rapidly gained traction, affecting over **200** victims through double extortion attacks, making it a significant player in the cybercriminal space.

## #3

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These malicious malware include the Rootkit like FudModule, Diamorphine and Backdoors namely CXCLNT, CLNTEND, CBROVER, BadIIS, PhantomDL, Supper backdoor, EAGLEDOOR, PondRAT, POOLRAT, MISTPEN, and FPSpy.

## #4

Twelve active threat actors were detected across various campaigns, targeting critical industries including **Manufacturing, Government, IT, Financial, and Energy**. Notably, Citrine Sleet, also known as Lazarus, and the Void Banshee APT emerged as prominent adversaries during the month.

## #5

Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of 38 attacks significantly targeting the following nations: **Australia, Japan, Taiwan, Singapore, and China**

# Recommendations

## Security Teams



This digest can be used as a guide to help security teams prioritize the **29 significant vulnerabilities** and block the indicators related to the **12 active threat actors**, **38 active malware**, and **174 potential MITRE TTPs**.

## Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **29 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors**, **active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

# Hive Pro Threat Advisories (SEPTEMBER 2024)

MONDAY		TUESDAY		WEDNESDAY		THURSDAY		FRIDAY		SATURDAY		SUNDAY	
													1
	2		3		4		5		6		7		8
													
	9		10		11		12		13		14		15
													
	16		17		18		19		20		21		22
													
	23		24		25		26		27		28		29
													
	30												

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

# 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 malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

**Social engineering:** is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

**Supply chain attack:** Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

**Eavesdropping:** Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

## Glossary:

**CISA KEV** - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities

**CVE** - Common Vulnerabilities and Exposures

**CPE** - Common Platform Enumeration

**CWE** - Common Weakness Enumeration

# ✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<a href="#"><u>FudModule</u></a>	Domains	voyagorclub[.]space, weinsteinfrog[.]com
<a href="#"><u>Meow Ransomware</u></a>	SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d044444 76416f9, 7f6421cdf6355edfdcbddadd26bcdbf984def301df3c6c03d71af8e30b b781f, 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310 a645099, 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda54434 81922f, 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d 8e9b853, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c6 4283ec
	SHA1	59e756e0da6a82a0f9046a3538d507c75eb95252, 987ad5aa6aee86f474fb9313334e6c9718d68daf, 94a9da09da3151f306ab8a5b00f60a38b077d594, 5949c404aee552fc8ce29e3bf77bd08e54d37c59, 578b1b0f46491b9d39d21f2103cb437bc2d71cac, 4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b
	MD5	8f154ca4a8ee50dc448181afbc95cfd7, 4dd2b61e0ccf633e008359ad989de2ed, 3eff7826b6eea73b0206f11d08073a68, 1d70020ddf6f29638b22887947dd5b9c, 033acf3b0f699a39becdc71d3e2dddcc, 0bbb9b0d573a9c6027ca7e0b1f5478bf
	TOR Address	meow6xanhzfc12gbkn3lmbqq7xjjufskkdfoqcdngt3ltvzgqpsg5mid[.]onion, totos7fqprkecvsl2jwy72v32glgkp2ejeqlnx5ynnxbbebnletqd[.]onion
<a href="#"><u>Emansrepo</u></a>	SHA256	e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb 04ff28e5 8e43c97e5bc62211b3673dee13e376a1f5026502ebe9fd9f7f455dc17 c253b7f
<a href="#"><u>RansomHub Ransomware</u></a>	SHA256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fab c14801a, 342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7 853ca2b, 56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307 a82e6763
	TOR Address	ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
<a href="#"><u>China Chopper</u></a>	MD5	3F15C4431AD4573344AD56E8384EBD62, 78B47DDA664545542ED3ABE17400C354, 3B7721715B2842CDFF0AB72BD605A0CE, 868B8A5012E0EB9A48D2DAF7CB7A5D87

Attack Name	TYPE	VALUE
<u>Crowdoor</u>	SHA256	9dff4c8f403338875d009508c64a0e4d4a5eeac191d7654a7793c823fb8e3018, 98af7888655b8bcac49b76c074fc08877807ac074fb4e81a6cacf1566d52f12
	MD5	Fd8382efb0a16225896d584da56c182c, 1dd03936baf0fe95b7e5b54a9dd4a577, c10643b3fb304972c650e593b69faaa1
<u>BlotchyQuasar</u>	MD5	b83f6c57aa04dab955fadcef6e1f4139
	SHA1	a68cac786b47575a0d747282ace9a4c75e73504d
	SHA256	ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2ebd
	URL	hxxps[:]//pastebin[.]com/raw/XAfbmb6xp
	Domain	edificiobaldeares[.]linkpc[.]net, equipo[.]linkpc[.]net, perfect5[.]publicvm[.]com, perfect8[.]publicvm[.]com
<u>CXCLNT</u>	SHA256	f13869390dda83d40960d4f8a6b438c5c4cd31b4d25def7726c2809ddc573dc7, 19bbc2daa05a0e932d72ecfa4e08282aa4a27becaabad03b8fc18bb85d37743a, 0d91dfd16175658da35e12cafc4f8aa22129b42b7170898148ad516836a3344f, 1f22be2bbe1bfcda58ed6b29b573d417fa94f4e10be0636ab4c364520cda748e,
<u>CLNTEND</u>	SHA256	db600b0ae5f7bfc81518a6b83d0c5d73e1b230e7378aab70b4e98a32ab219a18, f3897381b9a4723b5f1f621632b1d83d889721535f544a6c0f5b83f6ea3e50b3
<u>Fog ransomware</u>	File Name	advanced_port_scanner_2.5.3869(1).exe, advanced_port_scanner_2.5.3869(1).tmp, advanced_port_scanner.exe, locker.exe, rclone.exe, SharpShares.exe, vssadmin.exe
	TOR Address	Xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid[.]onion
	File Path	C:\programdata\advanced_port_scanner_2.5.3869 (1).exe, C:\programdata\locker.exe, C:\ProgramData\SharpShares.exe, C:\users\xxxxx\appdata\local\temp\advanced_port_scanner_2.5.3869 (1).tmp,



Attack Name	TYPE	VALUE
<u>Fog ransomware</u>	File Path	C:\users\xxxxx\appdata\local\temp\advanced_port_scanner.exe, C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
	IPV4	85[.]209[.]11[.]227, 85[.]209[.]11[.]254, 85[.]209[.]11[.]27
<u>DOWNBAIT</u>	SHA256	3b9ef9701ea2b2c1a89489ed0ed43ffabec9e22b587470899c0d5aca1a1e4302
<u>PULLBAIT</u>	SHA256	9dd62afdb4938962af9ff1623a0aa5aaa9239bcb1c7d6216f5363d14410a3369
<u>CBROVER</u>	SHA256	d8747574251c8b4ab8da4050ba9e1f6e8dbbaa38f496317b23da366e25d3028a, 7c520353045a15571061c3f6ae334e5f854d441bab417ebf497f21f5a8bc6925
	IPv4	18[.]163[.]112[.]181
<u>PLUGX</u>	SHA256	b37b244595cac817a8f8dba24fba208205e1d1321651237fe24fdcfac4f8ffc, de08f83a5d2421c86573dfb968293c776a830d900af2bc735d2ecd7e77961aaf, d32d7e86ed97509289fff89a78895904cf07a82824c053bfaf1bc5de3f3ba791, 046a03725df3104d02fa33c22e919cc73bed6fd6a905098e98c07f0f1b67fadb, 785d92dc175cb6b7889f07aa2a65d6c99e59dc1bbc9edb8f5827668fd249fa2e, f748b210677a44597a724126a3d97173d97840b59d6deaf010c370657afc01f8, ffa94d76d4423e43a42c7944c512e1a71827a89ad513d565f82eb8fe374ef74d
	Domain	www[.]ynsins[.]com, www[.]aihkstore[.]com, www[.]bccler[.]com
<u>PUBLOAD</u>	MD5	7103a25d591a051aa37424bc3a9d0733
	SHA1	3e716409192e5023328920e67512185fea89b3b1
	SHA256	a062fafaff556b17a5ccb035c8c7b9d2015722d86a186b6b186a9c63eeb4308a, 14a9a74298408c65cb387574ffa8827abd257aa2b76f87efbaa1ee46e8763c57, 2e44ebe8d864ae19446d0853c51e471489c0893fc5ae2e042c01c7f232d2a2c2
	IPv4	103[.]15[.]29[.]17, 47[.]253[.]106[.]177

Attack Name	TYPE	VALUE
<p><b><u>BadIIS</u></b></p>	<p>SHA256</p>	<p>3f17c66aab154212fb02fc7e329296c233aeb4abd9248204fa99c490c113a6e,  875239000f22cff75f62f9a1aa9924a8c3fea72124b0c4b31c7b3814f9dc0601,  157174f0b9be66e3c9090c95efdd1dd23b19e42aa671758ebac5540a173f760c,  716c14edbd08658fc72a7641913cbab451c3f947d2473fd36488b1a228d1e340,  e733b9444106ca37c3ef9e207ac6c813b787614496b275c1a455fcc3aca1c4a,  6da823fa4950b95f9ada74e6899fb0a17c90e8f64c75be43f037461f3eee3d02,  138a48279b17d4f04368096a6f2de5d16cf3d4c4472342d3263468a69399b9b8,  0644b3ffc856eb54b53338ab8ecd22dd005ee5aacfe321f4e61b763a93f82aea,  9f7de916e513f89e8b7192bfc1daadf927110f3eafa836d036fad2b3db1a93d7,  40384f574e4ea0a1dd0876cf4af60f79a4a0b37d2a8287a795b8ab5e3427521e,  12f6b72cdf8660d94eb5d915d4eddc0ee3ae4adaa719cacad60c6f7d44e90486,  01830ea1e8bcfa8307d1d271982ef40c3451a21f7b109835b524f7a2f5f50dcc,  497e6965120a7ca6644da9b8291c65901e78d302139d221fcf0a3ec6c5cf9de3,  f8eeb8a8e336eaa8723d483fd3dec802c504a7121976477a3a1d6baf44f19a12,  41cd5131c323ed643bebb245da7ec39f49efe1014bce2f3b4031ba5903fb97db,  507b77ab91f1b9c792210d7e38f4d43f16ab652f2b3008f1361cacc81817f992,  feeea74325d2f389e9325a8113f185bc823dc0681b86a82982c3a3f2951750c8,  fde34c06dff9a5304c394097047233930da199cce90d5a2ded3a1634dea42470,  7353030af3274ea1ab9756aad8130fb01bcacd82fb6c6d2358ddcd060257275,  82b107aa1791a58c65e3a266981e886e24e7d6abcf076750f3e72bf4e3697aa4,  a19144fad371a7fb476e5c109e1ca943245c41ea833c5e10ad4ff0db0e045869,  64a2785b41c0864cb630f54d749371e4ae6d916d421b96f0e394d203c066c883,  9793ea98b7fbd43f0a7273594d7b4e53338048c651c33fbfdbeb1cc275957996,  241cce3bde9379fcb18c81a856e8b67582b44e48f2134b3e750a9370bd87d707,  819500f6d820bffd4290b172eb84721eee9f4d3a5814d58a65d5a321ce3e51ab,</p>

Attack Name	TYPE	VALUE
<b><u>BadIIS</u></b>	SHA256	bbdada0149cd4833a32e9f0d981e36ed13685b1f00233e7196b843 2ec1589b3d, c79086813d0c846deecb7eeca238f78a662f0aec1ded892c3561522 cbb39a24a, 46644577e1d6f748a7c10667eed8255de711b95018a4a75234f070 409ba8bd8d, 05d2fde8b6141318a97cb0044c2494f009761351af9b6633ecc7e7f 089879998, 4fbda60f74a4003bc93e75acffbd55520c99236052b527f920c67c18 673e6bbb, 56715f3e15e8d39125e0b8cb46aaac1788fa46df4eed6881ddc5beb 805679506, e3ace9e5b9a71a6a2e98daa33fd19e536d2a520a0160495b4b77ec 98ad0f71d9, 611a41a2856b907abd2ebc627369aebfe0156864f2927bb1a124a3 dc1e8463a0, 68a57727aa0097cfe65782961fd10c8f6fc8766c7a816f85098c3ddcf 7a681be, b8e15597e1b137274f36c5e5f6f0811f041dbd5c2cd0784a2a928f6e eb68cba2, a62734619ec889e7c80bb2edc3497cd4139ebd5646db30c20e0928 b264b53435, cb816863576b982fb7f14a41c63282d8f6f7a635e555353f5a751107 94196f87, aa34ecb2922ce8a8066358a1d0ce0ff632297037f8b528e3a37cd53 477877e47, 0b7fed82d2594b8a30772eec6eb6bf2db6a23404504535bb78c828 ec1fc870f5, d52ebfa1ea0366ffbce967a652190e3eb0206e47319a19df630d374 43e7d0d69, 44d95ff98bc70dca8c9bae7b7cdb2e6f94685f5fc65f2ec5cd27d069c 4e4797d, d15d07add8f4f27ac87127c7d98d287f7cd0a4e5d480119dab62aa6 488a70d59, 3ae3ae44712a4cc7645bbce3b54f6a431ea08d33105f78cd8f33002 7aa15b8cc, 4d4bcf6be29b3074d01f839d81a78880be7afc5df366d65006a5d07 fc9d11fea, 00142e46c997fe7051af5667953908cc876268be30d61cd985f6265 514639251, 6a9e2cb9592bee7dda6165fc5f8c26e6be5eb49d9de58b3251327c1 d02d858b3, f0e95504b127dc1477cc1d89aac29edb8b7578ce21224ddb4d67c3 b81ab19e52, c6847600910ab196652a38e94ecf592e645d43025d1d61b3710b2f 715238307b, 4f8775e26d6e291905f49a2766b804c6fe8398d8acc26c11ec6a2fa9 6a02b3de, f5615c120aaab860b279e095a68ea0ae2ca556929395f118ad7b63a f53d61f21,

Attack Name	TYPE	VALUE
<p><b><u>BadIIS</u></b></p>	<p>SHA256</p>	<p>2f708f00f6c2743f61b662dcc82ac908f5d86c6a87d72cc7061311d267d36e56,  cefd1c9abbfe0dd44d923a24a568b3531d067ef821f40ca64c471a8a  a1ff33d3,  cfaec2a27dc9667443bc5be81b66e01c42ad5d83a90393e4dff396e  46f99ee7,  7553767046f15e37550f3d26a779a7e8ec3704842b97b928092602  d725528a4d,  28b4c4f001517ac4a682b728fd4b9d1364da6698a84d2f1f6016937  e8240219e,  ad1c768f5f6bba0110be23c36ad6aaffca7f122cf3a5624934af6cf871  f58bee,  80e327564d00167a6eb4ecf5a6fa0526d5261b390c46ef442673c2e  69173e470,  08ee575b9cda0ea5f12c8d5132469c99cd1deebfc9514f7b8cb5203  48d3a9abc,  91bb5a365478de474d938690f4ee9bcd6413ef59d331829da93c9c  1c88fcb771,  4995992852f5c5066581e4d63bcb9b2655d7458534c27102765871  59c234e135,  2a2c1447a24fca304815b8de8b546276e37a866f0bb9390a69f92ec  150855a1f,  9abc210de663efa287e09adfb6fe4196d46d4f3f4541fd4d64439adc  220709ae,  bcde2ee839d6bc2e18bd150f4fc21beb369f7877425efeb6e721bf95  4f54679d,  a11626d55ee9c958d86e8c77dfe19f66cdf545fbd8743126081f46dc  24446767,  95795de242b0b42d4ad0bb66ef8d9baa0c2e9e35f419fb515f023e9  a33ed271e,  307f905981965afc33bc17e5053d877deb2eb4fe7b88b892d59dbae  96992c161,  fb07c5b6e8f0ae482d9c571611f5868179227938e1e23de3d09dcbc  b14fb7972,  7c61c37356a2486cb39eef47ffb91b0e64efd2d1caa9e686ae2422df  ba621e6d,  0cbc4d4941c509608c0892bf337abe6b004a2fa7c1e83e7ff23d54e3  23064faf,  6549dd663b597a951781f1ab6b820079f4ffeec85f396f349d5ce2f9  7b3f9bf6,  165b55f40e9b488a20a7346d7b110729f0b7025ca767b0e174c6b4  5c9e09b42b,  364bf510c9c1d54eedbcfab6260e1ea72d9bce0c9c8dd4ea8e84e25  4f5c1c91c,  320da8cc3e46df550363d8a2452c2c459bf30142da065ccb29a7f2b  9629ee112,  c29e53de6684d771cff912a4ad57d203d1a63ff8334aa30727e76c8  74492ab54,  15ada077c7bd86103f729810ea33a4856bb2b39ba1c017293c492a  347036c331,</p>

Attack Name	TYPE	VALUE
<b><u>BadIIS</u></b>	SHA256	c9a69b28d4505b608da384e104a9046d1200aa84157adc2dd1628c823f2c6323, 3150c48438d4781d4c3ada83b7be45d76d8ac7a78f5d8d602152ac1abc3528bf, 2ea3202ca7ebd5c407409d35e71520f4782a136454487ca857afb5032660f93f, cdb7c3638fffffd42111e0a72dc959f1b49e15be7e8bb9a7bad2c5d89cc00f8b, 17de3f731a78bc740c5b57fb6d667cb68d93b5fe94076c852ddb30d7089988cc, a9c92b29ee05c1522715c7a2f9c543740b60e36373cb47b5620b1f3d8ad96bfa, 3d482e87a0e97e70c8b2e7541ba0bdee388029a5a7f26bbd62d981565cc3a91b, 59249bede0deaea326c5bb6584daf5e25c9f65ede0af7e7cd5f63761dd91b3af, 9869782b98afef7b1619cebbbe3a45ec4bc50c7138a4e8291a31f2e039d08b46
<b><u>Atlantida</u></b>	SHA256	6f1f3415c3e52dcdabb012f412aef7b9744786b2d4a1b850f1f4561048716c750, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0
<b><u>GomorraH Stealer</u></b>	MD5	E02089570b24b11d6350337069b7e823, 201fb3d8b93205488e1a6a408ce18539, B479fa60615c730d0417b67c1a26274f, 3afd64484a2a34fc34d1155747dd3847
	SHA256	2f8a79b12a7a989ac7e5f6ec65050036588a92e65aeb6841e08dc228ff0e21b4, 62c6aebb6bcc4d2faf985a4af59b111ae1e162419acfae7e7f126189073bddf1, dc33943da400ea506484952ba242737460c73dd2b3e88c16f0f18a0fd6dc459c, bf78263914c6d3f84f825504536338fadd15868d788bf30d30613ca27abeb7a9
	Domain	rougecommunications[.]org
	IPv4	172[.]93[.]223[.]99
<b><u>PhantomDL</u></b>	MD5	15333d5315202ea428de43655b598eda, a2bd0b9b64fbd13537a4a4a1f3051c0
	SHA1	b6212da07dc3a4f39a33bc0f0242c86a0f4433e6, 69383141c5270ca8876674026c0a228011bb5d7d
	SHA256	201f8dd57bce6fd70a0e1242b07a17f489c5f873278475af2eaf82a751c24fa8, 582c4674ba4880f0e5dec38917e970f906ac18205499de67b076d8fb17c0dd22, 08dc76d561ba2f707da534c455495a13b52f65427636c771d445de9b10293470,

Attack Name	TYPE	VALUE
<u>PhantomDL</u>	SHA256	9f5b780c3bd739920716397547a8c0e152f51976229836e7442cf7f83acfd69
<u>PhantomCore</u>	MD5	16f97ec7e116fe3272709927ab07844e, 855b1cba23fb51da5a8f34f11c149538, 55239cc43ba49947bb1e1178fb0e9748, 0e14852853f54023807c999b4ff55f64, 99b0f80e9ae2f1fb15bfe5f068440ab8
	SHA1	9ab4d91d3db34431f451106ede4f0ed5b163ce94, 0695028a13d35aa60732b6f5069b9907d6987576, 17f6119755f80fb0308bb9aaa77b6706e5649edc, 508b88a1cdc936be6da3d58a7ea6c82b491956ee, a27c67cec10295f27c660e25ee00648d77300a01
	SHA256	5d924a9ab2774120c4d45a386272287997fd7e6708be47fb93a4cad271f32a03, 0060c80acddb1801830b50ec87c1f66e3d00fbc9e83ea732b83ffb871217406f, 5a3c5c165d0070304fe2d2a5371f5f6fdd1b5c964ea4f9d41a672382991499c9, 5192a92730e5eee19dea67ba65ec4ed8eaab4314b389faa44ea051290a4b4a66, 22eb1e647e4c5f7f0d0dcc45af02d5ac44e270ed067ca1eed504692f80014bc6, 9b005340e716c6812a12396bcd4624b8cfb06835f88479fa6cfde6861015c9e0, dc3e4a549e3b95614dee580f73a63d75272d0fba8ca1ad6e93d99e44b9f95caa, b8447ef3f429dae0ac69c38c18e8bdbbfd82170e396200579b6b0eff4c8b9a984
<u>LockBit</u>	MD5	76b23dd72a883d8b1302bb4a514b7967, 6ddc56e77f57a069539dcc7f97064983, 7acc6093d1bc18866cdd3feccb6da26a, 59242b7291a77ce3e59d715906046148, 6568ab1c62e61237baf4a4b09c16bb86, f7abdae63bf59ca468124c48257f752, 79d871ff25d9d8a1f50b998b28ff752d, 78cc508882aba99425e4d5a470371cb1, 1d2d6e2d30933743b941f63e767957fb
	SHA1	338e19e8a3615c29d8a825ebba66cf55fa0caa2c, 8fee139dc37447f2f221b0858734a88ff8eafc05, 41e19260552d038009f0835e7a19ddecaca8ae34, 3af0cb27b6a509c34bb4485fd64a0e777e9aace2, 3a8120cfd574e6eccc15aec2fa3fa1e50e98e1a7, b9ca6711d007d1b6f0ef8bd262987fad96595968, 7bcb6cb60fc08c8cf446e7b631e524a00f924fc3,

Attack Name	TYPE	VALUE
<u>LockBit</u>	SHA1	1da019570a4af615eba5d6ca85fa5ed392503450, f3e489cf30036bce1e07a6c5bca23df6c7f469d6
	SHA256	311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb 99b86, da2191203b39fda0823520a85a9ca0bb8c42c4ef5b341a929d69dfd99e 971d7d, d10996d627adec7ae4cf25a23b034387db98de569da9f7795520c0c49 944698, 9c62569f840151c89e776f57669f74ccbca29fa7f644653084117aee76 b1d53, 2d3db0ff10edd28ee75b7cf39fc42e9dd51a6867eb5962e8dc1a51d6a5 bac50, 072be899f5a9892c39250aae8a6fd89c480c02135ed0a85e0d7a181577 e67454, 0edd5b8945061d801ecb60a852dcecd507e839c23f7c93036c244c75 4b93459, 5fb9263c435c494b7e5b25da3d772ce62945e0efbd4d2bb64529c75b9 dd1e47c, 1fe97e87d00f0141449bfb3e50e2749d5c2519923bd50b9c586d7e9508 9698f6, 4c218953296131d0a8e67d70aeea8fa5ae04fd52f43f8f917145f2ee19f 30271
<u>Babuk</u>	SHA256	102bf13dede7455f750e20aba4655a37d20637488bb7c928d5b2463bc 1a9f744, 1c37c8168e39204387de4ffe7097b32e1793b16df0f33597761e1a4e4d d3702c, 9b243cca7d84f0685c5f73ebf6bc4924b2350b3be3936aa5e5ecccbb4c 648b9, 91608d0a98e5df17de04c006aa7842e2f16faaf09a0c2f518b9058a2757 7ba0b, 5363cedd35284855a632d38f4c198c9c74df70f5ed1b7312036335620e 931752
<u>SambaSpy</u>	MD5	0f3b46d496bbf47e8a2485f794132b48
	SHA1	28911b5edd5235db1119acd2e09349320d665b88
	SHA256	9948b75391069f635189c5c5e24c7fafd88490901b204bcd4075f72ece5 ec265, d3effd483815a7de1e1288ab6f4fb673b44a129386ef461466472e2214 0d47f8, 43f86b6d3300050f8cc0fa83948fbc92fc69af546f1f215313bad2e2a040 c0fa

Attack Name	TYPE	VALUE
<u>Gootloader</u>	SHA256	b939ec9447140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988, c853d91501111a873a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687b
<u>Supper backdoor</u>	MD5	0b175136f48d88e094318cc78792b876, 032bf67c14d00b5468ce0aeab927c86c, 7ca12616c3e964dcf3dcc30f8ee6a18, f176d8ee8c58223c3a1ca5b1dff274b8, c1cd52785f2ca5ef177e259c7ae3596f
	SHA267	4cd01348769bffa6623e9871ff2169de2f5e15f4c5128b232b666e0c62398cff
<u>INC Ransomware</u>	SHA256	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5dedced
<u>Diamorphine</u>	SHA256	3be13d69a4c9b94179a6cf45a310acfaa7c5455cba908982fb36277486b5ea86, 3cd21bf96050d89d3bcf8f4d7612c8d60dcc2a9fc2b8764fc6f9c08aabf81c5a, 4a411cf9f0e30eb8c8fd23d38413d2455b0f6e81b0082e749b8ca64cb9ab1e4c, bf46bd921cb615fb7490b50b0ead98ff4ebdbd599eeb3736f568c64f19eab980, d99d7b090da1f1c14a0a554492ba99a506472eab66b057435261a246c2405be5, d947b70347ce1f0088b107a3344c033cdd666782e7b382cd4bccb64724a28575, 4fdadd8b65ce5975745596f9afcd3532d89a80f01e29993ed3842318b56c58b0, 49117f048c668c3d4959796aa447d89899b0ede84dbfb486adb34c92d8cedd2f, 351d0bdab940e0195dd3c5e5da61ea4d46a0cce34a8ea9f78e27b1d233a2486f, 69e144206b607522da3b571823f93125d121065ba55c0ead651696a48e92bdcf, d9fdb25d6a30a6d63c705e25e818553fb21ee89f3b988aae7b65c10eec805a1b, b0c4456420e0d650912a99acc9fe4d4e9999f75921facafc718c2c82ea0365b5, 9ba2a5fcc9ab9b229c7d7a139dd1768858738ed3f4ff0e07e23bc59a90418ea1, f79eb2930012ac45e4c4434f8559e0bc40fa269b51fcc297ca4b78c2b61bfc7, 0d0de2151d7fcd14b1bdb64dab802e2290a5a130ba7ed7db6a6e4d5b5b095463,



Attack Name	TYPE	VALUE
<u>Diamorphine</u>	SHA256	4114d57edae1d877d62d8b5642bd93cfb457b12cf657d53a185e37d09ae51891, 91d9421125adceb27e5e40f27a8da6cb5de8971b2e8d081a18020a6c0b44e453, 1936270dc97c4e2e7bbdfd0c337ed1acdf72df6dc9598b396f6fdf4c0ad8f904, a158fc3982b8ccbec4655b9a3017eba167e0f0bb61f78f870898a51f7f6076bb, 29913a342bca81ec1084c9abc1c6be8d431d0da40fadba465a3ca3481193904b, a931bc92999eeefdcb79bf6dc294608cb825b2d8f2627b1b3ab0b71e74d8d835, 5bc5883c31f7e1432663d2f277d6cb2c849cfc1e095bca27bd5d17ff11229fed, 8b7eaea5fc2f184ad9ef6abf069bdb78d42662c891b09c3c6a9d4899526b17c8, 825b5ab1e44f6744e2fb686c07c145d3b9cbe30e25ba8f6a4b5bf8603c7ecf3a, 678d3846429bff6c54e386f65331791e932dd5f2bafc5d0c4877a493cd0ee355, c8e29d0d02610b5d9aa92a13013ea292fd3472cf62ba09f5c1b72ab73619ddc4, afe0498385984eca996d17b37851fdf9213910426f4841da29c6d9c33e98e013, 08ffdaafb82fefde776f7e0f9d5824f15cea7ff8043fb7a200e8f4e60a05e82a, e029e90d6767f2b84e9e2d618db105573404d4f09eece52734b9faae5fc25c2c, be40eee5b8b3b3dfa0c453b191ed0fccac9532a41f062c6fce56db11d366250, 5d3373476bcded34f0e2436587254fcc8edab9a771b9a040cbf59c57ab30b4da, b061611f11c620be049ee85651e2950f51e299e91f7488045c5e3b985c769898, 44233d8b9de16b9fa0fc1f048300927671a60f03394ad41b0fb7e91a803e4a5c, 5d637915abc98b21f94b0648c552899af67321ab06fb34e33339ae38401734cf, 370fff5098eda6b9ec9ae942c1ce32098e07d7e91d4a5c6e978d8bb22747e6df, 12d6326bd7e7bc8e81e0e161b5537096847253076334bca8c16a3c3f4c2c0e5b, 76c01ef5aaef29e2894beddd8f23726b75f6a8d335499333b60a0e3815de5b2e, 1a9382e491598fea6f418427f36a0e127135ed4886adc846b3339e0505284971, be8e8ef049dedc7c56e7d61f4f50a0ed324a42e1b1febe66aea77156bc6f02a0, 400f3a425ed047442d87ab96e7469f63c6dbc78424771eb2e4b9c305ea44d0b6,

Attack Name	TYPE	VALUE
<b><u>Diamorphine</u></b>	SHA256	d00771a4fd8f314417441d76812466c0a84ab053a8e5960037526d0ff4cba37d, b627725d7f4ee5b969c200c65d61123027df30a8f2b5930c7df5bfbe8a613f6b, 6d388ee0ee34d5ec409c55cee65b8d65aacbf7f3bf207db47e3fef0d7860877, 954a5905607d1bd1160b6471a36679af9aa57a5fbf777751f68492ecc54d45e1, c2b0588ff7a6d5790cbd5587fc307e6b36a618ccc90c47264b4e1bcc0a549931, 6436303b20b2836d08595a90cfd82806c6dce16f33964aa4749a86b343d0abbb, 8bf0ddff6d2921257fbd3a3791c72fc1ebc7347a84ab4bf0298085d91e5ef0d5, 12360ddc28cfa104377d7c7a92a190933c424c3dd407b65f7b69b1b5c67dca1b, 1fdda23de5a1dbfb70698f2b548c80c1d2967cb0f8d9bba41d64131aa a7532a3
<b><u>RIPCOY</u></b>	SHA256	916f3f4b895c8948b504cbf1becb601ff7cc6e982d2ed375447bce6ecb41534, 4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54, 6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbcd3094612a6696a40c664ce, 1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448, 4ad078a52abeced860ceb28ae99dda47424d362a90e1101d45c43e8e35dfd325, 04b336c3bcfe027436f36dfc73a173c37c66288c7160651b11561b39ce2cd25e
<b><u>EAGLEDOOR</u></b>	SHA256	b3b8efcaf6b9491c00049292cdff8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4befa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7
	Domain	msa.hinet[.]ink
	IPv4	167[.]172[.]89[.]142, 167[.]172[.]84[.]142
<b><u>PondRAT</u></b>	SHA256	973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c, 0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7, 3c8dbfcb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e, bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80, bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b, cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86,

Attack Name	TYPE	VALUE
<u>PondRAT</u>	Domains	jdkgradle[.]com, rebelthumb[.]net
<u>POOLRAT</u>	SHA256	f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a 71d3703, 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d417 4bace456,
	Domains	www[.]talesseries[.]com/write[.]php, rgedist[.]com/sfxl[.]php,
<u>BURNBOOK</u>	MD5	57e8a7ef21e7586d008d4116d70062a6, f3baee9c48a2f744a16af30220de5066
	File Name	libmupdf.dll
<u>TEARPAGE</u>	MD5	006cbff5d248ab4a1d756bce989830b9
	File Path	%APPDATA%\Roaming\Microsoft\BDE UI Launcher\wtsapi32.dll
<u>MISTPEN</u>	MD5	0b77dcee18660bdccaf67550d2e00b00, b707f8e3be12694b4470255e2ee58c81, cd6dbf51da042c34c6e7ff7b1641837d, eca8eb8871c7d8f0c6b9c3ce581416ed
	File Name	binhex.dll
	File Path	%APPDATA%\Roaming\Thumbs.ini
<u>SnipBot</u>	SHA256	0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e 01677501, 1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed 35c154, 2c327087b063e89c376fd84d48af7b855e686936765876da2433485d 496cb3a4, 5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aae b688129, 57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781 fd42312
<u>RomCom</u>	SHA256	1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f 354930f, 419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667 871a5c16, 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980e fa312e0, 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6 b963811, b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a5 79dee048, b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c 21cf5c39
<u>KLogExe</u>	SHA256	990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a6 7228e27 a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb2216289564 1dda0dc2 faf666019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4 f6801

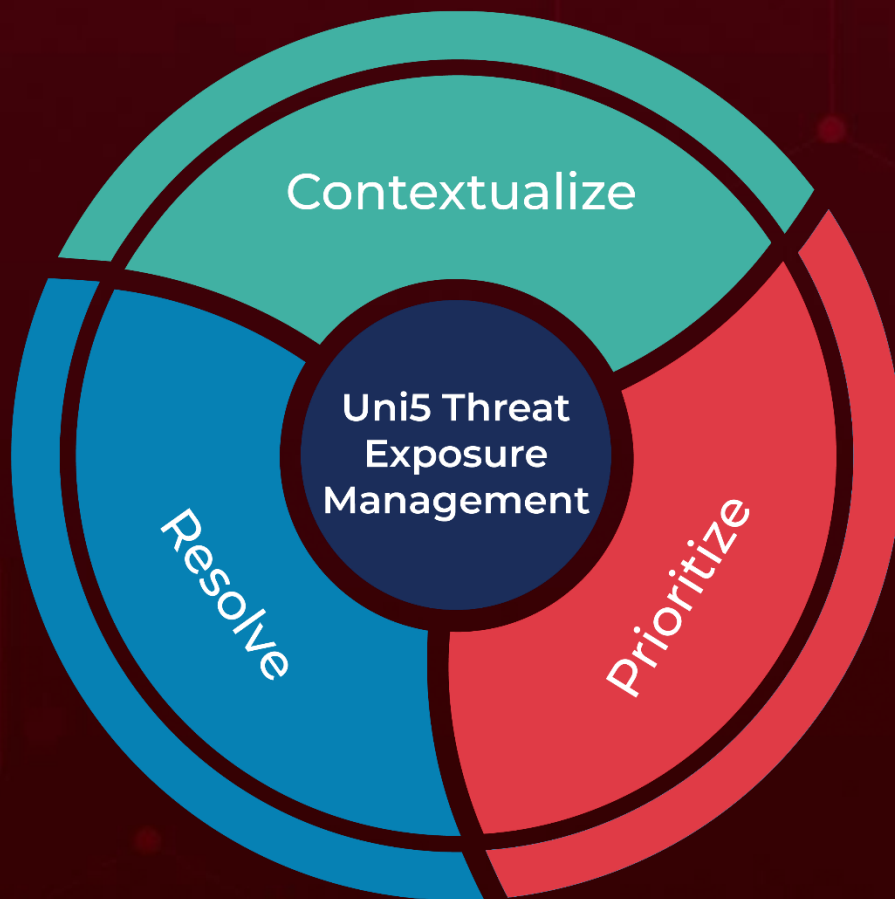
Attack Name	TYPE	VALUE
<u>FPSpy</u>	SHA256	c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343 2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

**October 1, 2024 • 7:30 AM**

© 2024 All Rights are Reserved by Hive Pro



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