

Date of Publication
September 9, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

2 to 8 September 2024

Table Of Contents

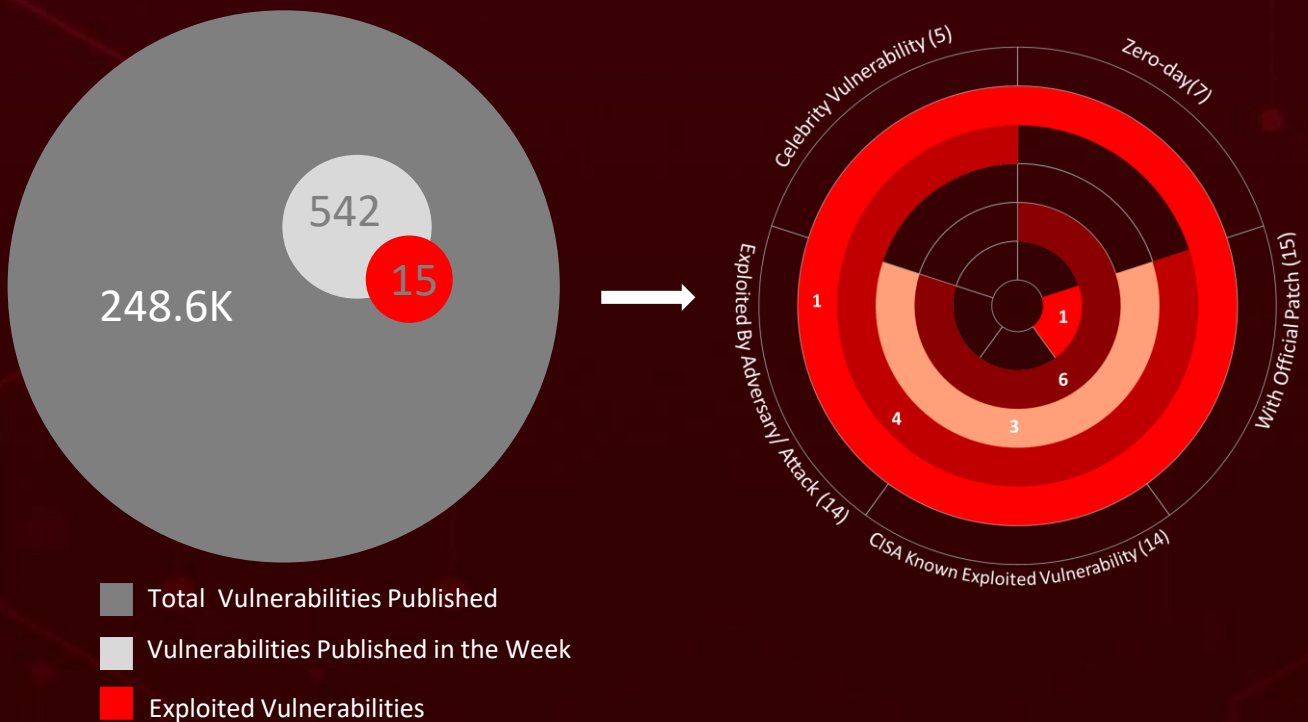
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	13
<u>Adversaries in Action</u>	21
<u>Recommendations</u>	23
<u>Threat Advisories</u>	24
<u>Appendix</u>	25
<u>What Next?</u>	27

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week alone, HiveForce Labs has detected **six** attacks, reported **fifteen** vulnerabilities, and identified **two** active adversaries. These findings highlight the relentless and escalating danger of cyber intrusions.

Additionally, a command injection vulnerability ([CVE-2024-20469](#)) in Cisco ISE allows admin users to execute arbitrary commands and escalate to root. **RansomHub**, a RaaS platform active since February 2024, has targeted over 200 victims using double extortion to encrypt and steal data for ransom.

Furthermore, **Citrine Sleet**, North Korean hackers exploited a patched Google Chrome zero-day ([CVE-2024-7971](#)) to deploy the FudModule rootkit, using a Windows Kernel exploit to gain SYSTEM privileges and maintain persistent access. These rising threats pose significant and immediate danger to users worldwide.



High Level Statistics

6

Attacks
Executed

15

Vulnerabilities
Exploited

2

Adversaries in
Action

- [FudModule](#)
- [Meow Ransomware](#)
- [Emansrepo Stealer](#)
- [RansomHub Ransomware](#)
- [China Chopper](#)
- [Crowdoor](#)

- [CVE-2024-7971](#)
- [CVE-2024-20469](#)
- [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](#)
- [CVE-2021-34473](#)
- [CVE-2021-34523](#)
- [CVE-2021-31207](#)
- [CVE-2023-26360](#)

- [Citrine Sleet](#)
- [Tropic Trooper](#)



Insights

CVE-2024-7261

Zyxel's Critical Router Vulnerability
Exploited via Malicious Cookies.

Citrine Sleet

North Korean threat actor have exploited a recently patched Google Chrome zero-day vulnerability (**CVE-2024-7971**) to deploy the FudModule rootkit on compromised systems.

Tropic Trooper

has targeted Middle Eastern governments in 2024 using China Chopper and Crowdoor malware for geopolitical espionage.

The Meow ransomware

originating from Conti's leak in 2022, paused after a decryptor's release in 2023 but resurfaced in 2024, now suspected of operating as an extortion group.

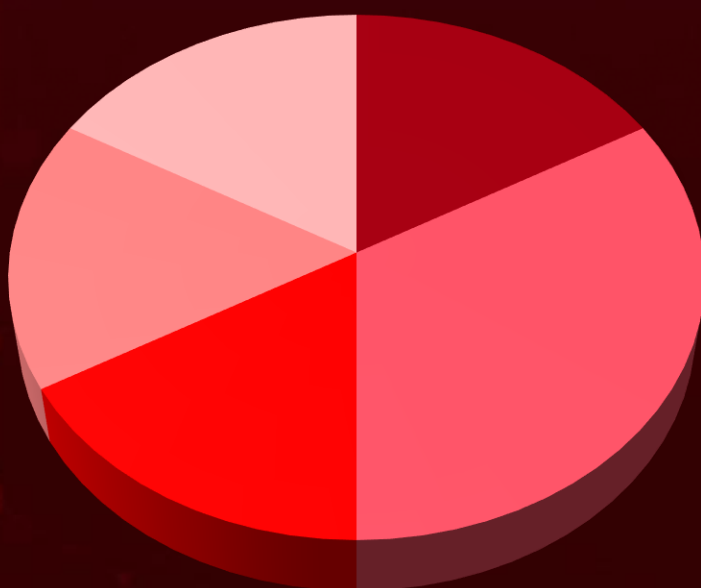
RansomHub

a RaaS platform emerging in February 2024, has targeted over 200 victims using double extortion by encrypting and exfiltrating sensitive data.

Emansrepo

a Python-based infostealer, spreads via phishing emails, stealing sensitive data from browser directories and sending it to attackers.

Threat Distribution



■ Rootkit ■ Ransomware ■ Stealer ■ Web shell ■ Loader

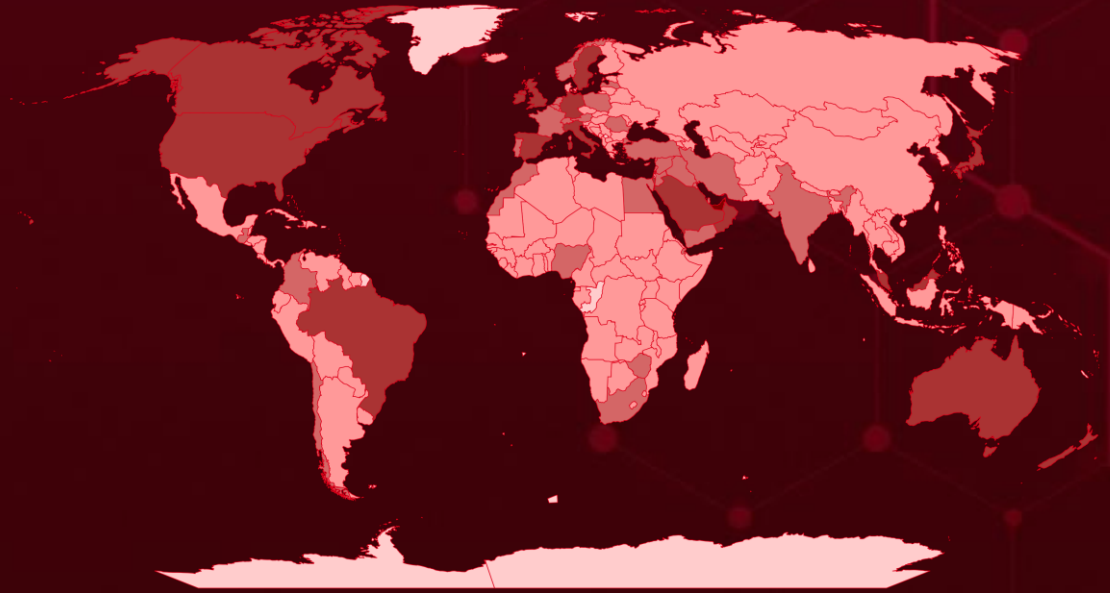


Targeted Countries

Most



Least

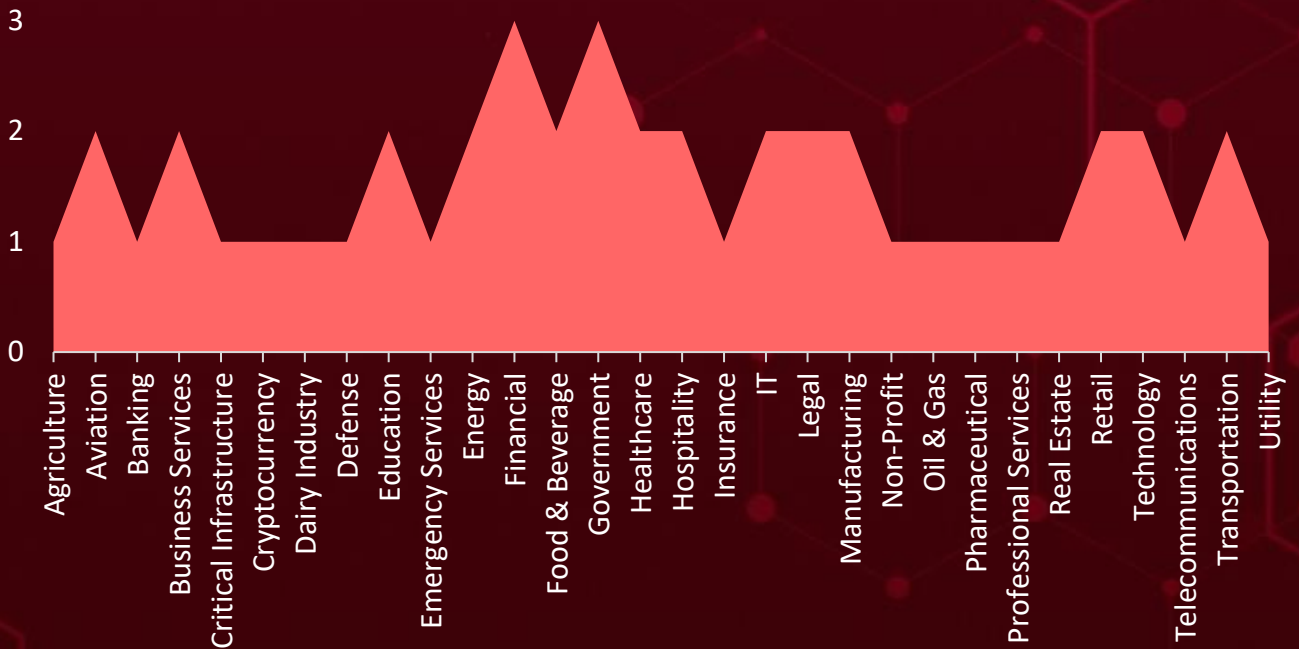


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Countries	Countries	Countries	Countries
United Arab Emirates	Austria	Ecuador	Gabon
Japan	Cyprus	Solomon Islands	South Korea
Oman	India	Bahamas	Gambia
Malaysia	Jordan	DR Congo	Cuba
Bahrain	Turkey	El Salvador	Georgia
Australia	Djibouti	Papua New Guinea	Togo
Spain	France	Equatorial Guinea	Barbados
Brazil	Latvia	Congo	Ukraine
United Kingdom	Portugal	Eritrea	Ghana
Canada	Yemen	St. Vincent & Grenadines	Cambodia
New Zealand	Romania	Estonia	Greece
Germany	Zimbabwe	Azerbaijan	Argentina
Saudi Arabia	Singapore	Eswatini	Grenada
Ireland	Egypt	Nicaragua	Central African Republic
Sweden	Guatemala	Ethiopia	Barbuda
Israel	Morocco	Pakistan	Palestine
Italy	Switzerland	Andorra	Guinea
United States	Netherlands	Armenia	Peru
Iraq	Timor-Leste	Finland	Guinea-Bissau
South Africa	Fiji	Saint Lucia	Albania
Qatar	Iran	Bangladesh	Guyana
Belgium	Nigeria	Sierra Leone	Rwanda
Syria	Norway	Slovakia	Haiti
Chile	Kuwait	Hungary	San Marino
Poland	Lebanon	Côte d'Ivoire	Holy See
Colombia	Tajikistan	Iceland	Serbia
	Comoros	Croatia	Honduras
		Belarus	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1566

Phishing

T1059

Command and Scripting Interpreter

T1078

Valid Accounts

T1190

Exploit Public-Facing Application

T1068

Exploitation for Privilege Escalation

T1588.006

Vulnerabilities

T1189

Drive-by Compromise

T1588.005

Exploits

T1588

Obtain Capabilities

T1027

Obfuscated Files or Information

T1565

Data Manipulation

T1204

User Execution

T1204.002

Malicious File

T1041

Exfiltration Over C2 Channel

T1083

File and Directory Discovery

T1587.001

Malware

T1486

Data Encrypted for Impact

T1082

System Information Discovery

T1036

Masquerading

T1055

Process Injection

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>FudModule</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
TYPE		IMPACT	AFFECTED PRODUCTS
Rootkit			
ASSOCIATED ACTOR		System compromise	PATCH LINK
Citrine Sleet			
		https://www.google.com/intl/en/chrome/?standalone=1	
IOC TYPE	VALUE		
Domains	voyagorclub[.]space, weinsteinfrog[.]com		

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>Meow Ransomware</u> TYPE Ransomware ASSOCIATED ACTOR -	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.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt files, System compromise	-
			PATCH LINK
-	-		
IOC TYPE	VALUE		
SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9, 7f6421cdf6355edfdbcddadd26bcdfbf984def301df3c6c03d71af8e30bb781f, 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099, 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f, 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Emansrepo Stealer</u> TYPE Stealer ASSOCIATED ACTOR -	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	-
		IMPACT	AFFECTED PRODUCTS
		Data theft	Microsoft Windows
			PATCH LINK
-	-		
IOC TYPE	VALUE		
SHA256	e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb04ff28e5, 8e43c97e5bc62211b3673dee13e376a1f5026502ebe9fd9f7f455dc17c253b7f		

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>RansomHub Ransomware</u>	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.	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
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-	-	-	https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467 ; https://www.fortiguard.com/psirt/FG-IR-23-097 ; https://activemq.apache.org/security-advisories.data/CVE-2023-46604 ; https://www.atlassian.com/software/confluence/download-archives ; https://my.f5.com/manage/s/article/K000137353 ; https://www.fortiguard.com/psirt/FG-IR-24-007 ; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144 ; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472 ; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0787
IOC TYPE	VALUE		
SHA256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fab14801a, 342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b, 56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763		

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	-	PATCH LINK
ASSOCIATED ACTOR			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 ; https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	
Tropic Trooper				
IOC TYPE	VALUE			
MD5	3F15C4431AD4573344AD56E8384EBD62 78B47DDA664545542ED3ABE17400C354 3B7721715B2842CDFF0AB72BD605A0CE 868B8A5012E0EB9A48D2DAF7CB7A5D87			




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	-	PATCH LINK
ASSOCIATED ACTOR			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 ; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 ; https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	
Tropic Trooper				
IOC TYPE	VALUE			
MD5	Fd8382efb0a16225896d584da56c182c, 1dd03936baf0fe95b7e5b54a9dd4a577, c10643b3fb304972c650e593b69faa1			
SHA256	9dff4c8f403338875d009508c64a0e4d4a5eeac191d7654a7793c823fb8e3018, 98af7888655b8bcac49b76c074fc08877807ac074fb4e81a6cacfd1566d52f12			




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




Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-7971</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	https://www.google.com/intl/en/chrome/?standalone=1




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-20469</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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-6kn9tSxm




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519		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	https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467?language=en_US




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27997		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	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	https://www.fortiguard.com/psirt/FG-IR-23-097




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46604</u>		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	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apache:activemq:*:*:*:*:*:* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*	RansomHub Ransomware
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories.data/CVE-2023-46604
	CWE ID	CWE-502	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-22515</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	https://www.atlassian.com/software/confluence/download-archives




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46747</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	https://my.f5.com/manage/s/article/K000137353




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




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




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
<u>CVE-2020-1472</u>		Microsoft Netlogon	-	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	RansomHub Ransomware	
Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)			ASSOCIATED TTPs	PATCH LINK
	CWE ID		T1068 : Exploitation for Privilege Escalation, T1210 : Exploitation of Remote Services	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472
	CWE-330			

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

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

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

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

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p>Citrine Sleets (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 Sleets, Jade Sleets, TraderTraitor)</p>	North Korea	Cryptocurrency, Financial	Worldwide
	MOTIVE Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-7971	FudModule	Google Chrome, Microsoft Edge
TTPs			
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
 <p><u>Tropic Trooper (aka Pirate Panda, APT 23, KeyBoy, Iron, Bronze Hobart, Earth Centaur)</u></p>	China	Government	The Middle East, and Malaysia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2023-26360	China Chopper, Crowdoor	-	

TTPs

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

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **fifteen exploited vulnerabilities** and block the indicators related to the threat actors **Citrine Sleet, Tropic Trooper** and malware **FudModule, Meow Ransomware, RansomHub Ransomware, Emansrepo Stealer, China Chopper, Crowdoor**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **fifteen exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Citrine Sleet, Tropic Trooper** and malware **Meow Ransomware, RansomHub Ransomware, Emansrepo Stealer, Crowdoor** in Breach and Attack Simulation(BAS).

Threat Advisories

[North Korean Hackers Exploit Chrome Zero-Day in Cryptocurrency Heists](#)

[Zyxel's Critical Router Vulnerability Exploited via Malicious Cookies](#)

[Meow Ransomware Resurfaces with an Extortion-Centric Model](#)

[Emansrepo: Python Infostealer with Tailored Email Exfiltration](#)

[Unpatched Cisco ISE Devices at Risk of Root Compromise](#)

[Apache Addresses Persistent RCE Flaw in OFBiz](#)

[RansomHub: The RaaS Powerhouse Exploiting 200+ Victims](#)

[Tropic Trooper Targets Middle East with New Web Shell](#)

Appendix

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

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>FudModule</u>	Domains	voyagorclub[.]space, weinsteinfrog[.]com
<u>Meow Ransomware</u>	SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9, 7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f, 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbbe8e310a645099, 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f, 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec
	SHA1	59e756e0da6a82a0f9046a3538d507c75eb95252, 987ad5aa6aee86f474fb9313334e6c9718d68daf, 94a9da09da3151f306ab8a5b00f60a38b077d594, 5949c404aee552fc8ce29e3bf77bd08e54d37c59, 578b1b0f46491b9d39d21f2103cb437bc2d71cac, 4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b
	MD5	8f154ca4a8ee50dc448181afbc95cfd7, 4dd2b61e0ccf633e008359ad989de2ed, 3eff7826b6eea73b0206f11d08073a68, 1d70020ddf6f29638b22887947dd5b9c, 033acf3b0f699a39becdc71d3e2dddcc, 0bbb9b0d573a9c6027ca7e0b1f5478bf
	TOR Address	meow6xanhzfc12gbkn3lmbqq7xjjufskkdfocqdn3ltvzggqpsg5mid[.]onion, totos7fqprkecvcs12jwy72v32glgkp2ejeqlnx5ynnxbbebgnletqd[.]onion

Attack Name	TYPE	VALUE
<u>Emansrepo</u>	SHA256	e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb04ff28e58e43c97e5bc62211b3673dee13e376a1f5026502ebe9fd9f7f455dc17c253b7f
<u>RansomHub Ransomware</u>	SHA256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fab c14801a, 342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b, 56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763
	TOR Address	ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
<u>China Chopper</u>	MD5	3F15C4431AD4573344AD56E8384EBD62, 78B47DDA664545542ED3ABE17400C354, 3B7721715B2842CDFF0AB72BD605A0CE, 868B8A5012E0EB9A48D2DAF7CB7A5D87
<u>Crowdoor</u>	SHA256	9dff4c8f403338875d009508c64a0e4d4a5eeac191d7654a7793c823fb8e3018, 98af7888655b8bcac49b76c074fc08877807ac074fb4e81a6cacfd1566d52f12
	MD5	Fd8382efb0a16225896d584da56c182c, 1dd03936baf0fe95b7e5b54a9dd4a577, c10643b3fb304972c650e593b69faaa1

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

September 9, 2024 • 11:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com