Date of Publication
September 2, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

26 AUGUST to 01 SEPTEMBER 2024

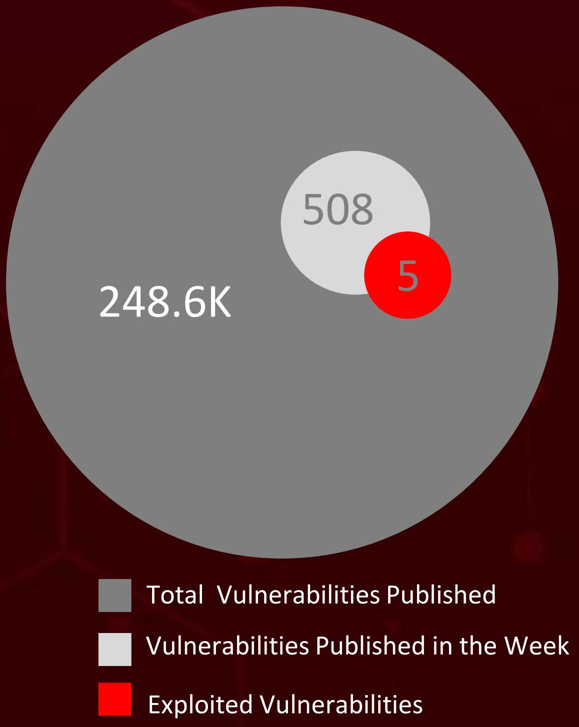
Table Of Contents

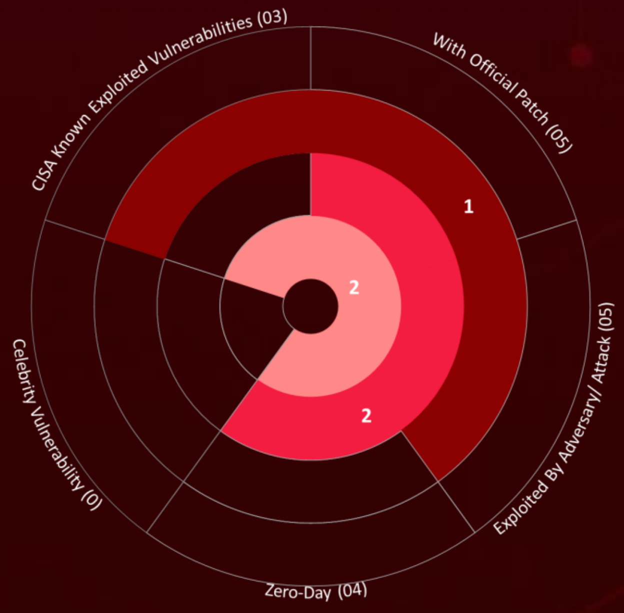
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **eleven** attacks were executed, **five** vulnerabilities were uncovered, and **three** active adversaries were identified, underscoring the persistent danger of cyberattacks.

HiveForce Labs has identified an Iranian state-sponsored threat actor **APT33** is targeting organizations in the United States and the United Arab Emirates with a new malware strain known as the **Tickler backdoor**. In these attacks, APT33 has leveraged Microsoft Azure infrastructure for command-and-control (C2) purposes, allowing them to manage and maintain access to compromised systems.

Additionally, the South Korea-linked cyberespionage group **APT-C-60** has been actively targeting organizations in East Asia by exploiting a zero-day vulnerability, **CVE-2024-7262**, in the Windows version of WPS Office. This flaw has been used to deliver the **SpyGlace** backdoor through phishing emails. Moreover, the Chinese APT group **Volt Typhoon** has been exploiting a Versa Director zero-day vulnerability **CVE-2024-39717** to deploy the VersaMem web shell, further escalating the threat landscape. These escalating threats pose a significant and immediate risk to users worldwide.





High Level Statistics

11
Attacks Executed

5
Vulnerabilities Exploited

3
Adversaries in Action

- Cthulhu Stealer
- Atomic Stealer
- PEAKLIGHT Downloader
- Lumma Stealer
- SHADOWLADDER
- CryptBot
- VersaMem
- HZ Rat backdoor
- SpyGlace Backdoor
- Tickler
- BlackByte Ransomware

- CVE-2024-7965
- CVE-2024-39717
- CVE-2024-7262
- CVE-2024-7263
- CVE-2024-37085

- Volt Typhoon
- APT-C-60
- APT33

Insights

APT33
targeting organizations in US and UAE to deploy the novel Tickler backdoor

CVE-2024-7965
critical zero-day vulnerability in the Chrome browser, enabling attackers to exploit memory corruption using a specially crafted HTML page

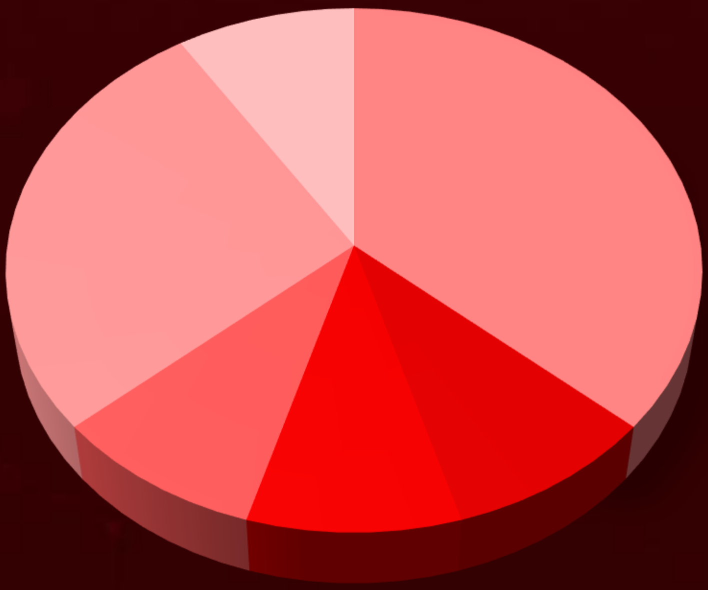
BlackByte Ransomware
exploiting security vulnerability CVE-2024-37085, affecting VMware ESXi hypervisors

CVE-2024-39717
zero-day falw in Versa Director leveraged by Chinese APT group Volt Typhoon, leading to the deployment of VersaMem web shell

Cthulhu Stealer a macOS-targeted malware written in GoLang that targets users to steal sensitive data by disguising itself as legitimate software

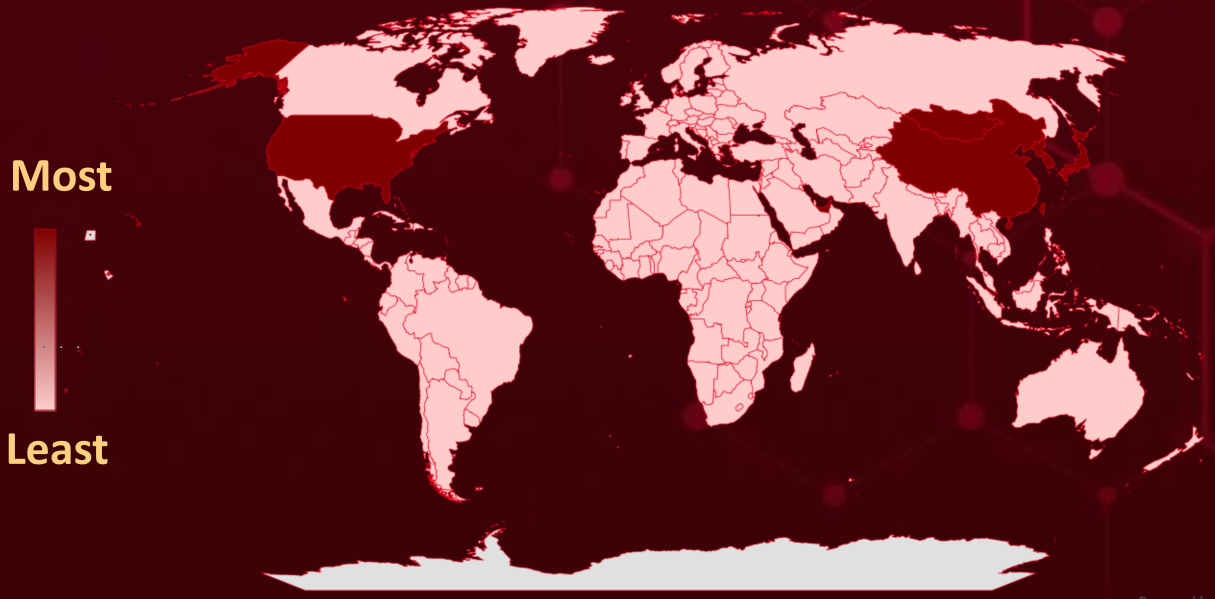
APT-C-60
exploiting zero-day flaws in WPS Office to deliver the SpyGlace backdoor

Threat Distribution



🟥 Stealer 🟥 Ransomware 🟥 Loader 🟥 Downloader 🟥 Backdoor 🟥 Web shell

Targeted Countries



Powered by Bing

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

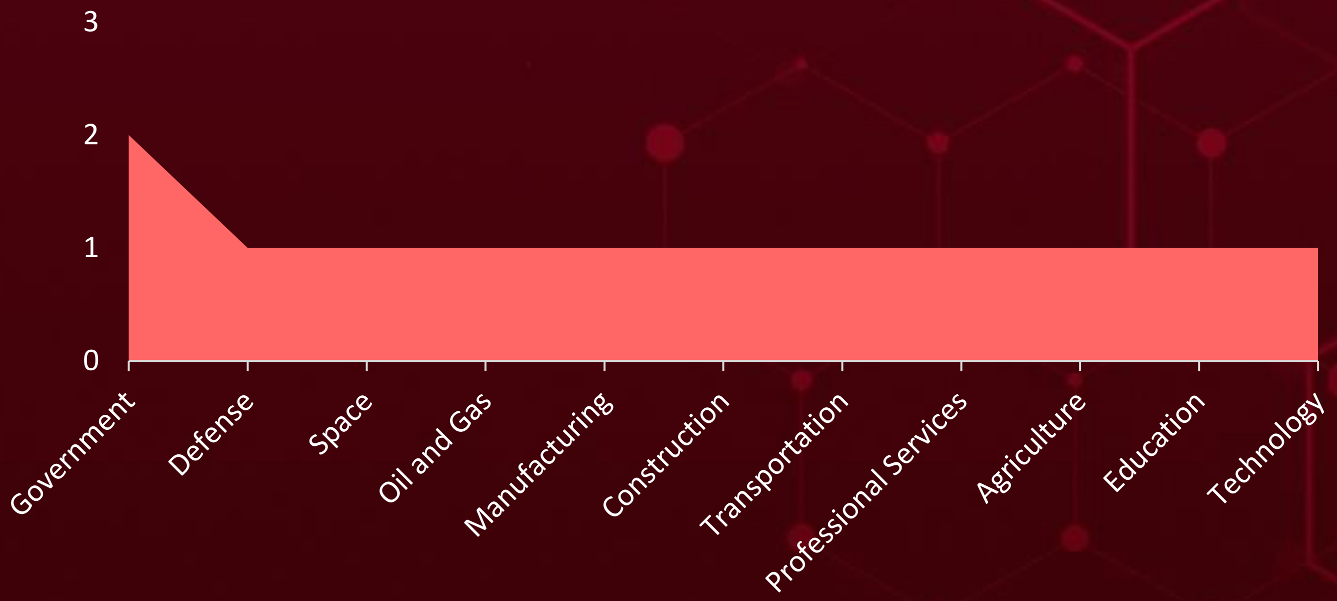
	Countries
■	Mongolia
■	South Korea
■	North Korea
■	China
■	United Arab Emirates
■	Japan
■	United States
■	Macau
■	Taiwan
■	Hong Kong
□	Pakistan
□	Lithuania
□	Sri Lanka
□	Australia
□	Montenegro
□	Austria
□	San Marino
□	Azerbaijan
□	Tunisia
□	Bahamas
□	Marshall Islands

	Countries
□	Bahrain
□	New Zealand
□	Bangladesh
□	Portugal
□	Barbados
□	Slovakia
□	Belarus
□	Syria
□	Belgium
□	Zambia
□	Belize
□	Malaysia
□	Benin
□	Micronesia
□	Bhutan
□	Namibia
□	Bolivia
□	Angola
□	Bosnia and Herzegovina
□	Paraguay
□	Botswana
□	Rwanda

	Countries
□	India
□	Singapore
□	Indonesia
□	Slovenia
□	Iran
□	Somalia
□	Iraq
□	Antigua and Barbuda
□	Ireland
□	Spain
□	Israel
□	St. Vincent & Grenadines
□	Italy
□	Sudan
□	Jamaica
□	Svalbard
□	Algeria
□	Switzerland
□	Jordan
□	Tajikistan
□	Kazakhstan
□	Thailand

	Countries
□	Kenya
□	Togo
□	Kiribati
□	Trinidad and Tobago
□	Kuwait
□	Turkey
□	United Kingdom
□	Tuvalu
□	Uruguay
□	Ukraine
□	Vanuatu
□	Armenia
□	Vietnam
□	Kyrgyzstan
□	Uzbekistan
□	Laos
□	Venezuela
□	Latvia
□	Yemen
□	Lebanon
□	Zimbabwe
□	Lesotho

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1041
Exfiltration Over C2 Channel

T1588
Obtain Capabilities

T1588.006
Vulnerabilities

T1203
Exploitation for Client Execution

T1027
Obfuscated Files or Information

T1068
Exploitation for Privilege Escalation

T1608
Stage Capabilities

T1082
System Information Discovery

T1204
User Execution

T1036
Masquerading

T1136
Create Account

T1566
Phishing

T1078
Valid Accounts

T1083
File and Directory Discovery

T1565
Data Manipulation

T1189
Drive-by Compromise

T1071.001
Web Protocols

T1190
Exploit Public-Facing Application

T1543
Create or Modify System Process

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cthulhu Stealer	Cthulhu Stealer specifically targets macOS users by exploiting their trust in well-known applications. This macOS-focused malware, written in GoLang, masquerades as legitimate software to steal passwords and cryptocurrency wallet data. Cthulhu Stealer employs `osascript` to prompt users for their credentials, stores the stolen information in text files, and then transmits it to its operators.	Malicious App Distribution	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	6483094f7784c424891644a85d5535688c8969666e16a194d397dc66779b0b12, e3f1e91de8af95cd56ec95737669c3512f90cecbc6696579ae2be349e30327a7

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atomic Stealer	Atomic Stealer, also known as AMOS, is a widely used stealer targeting macOS. This type of malware extracts and exfiltrates sensitive information from infected devices, focusing on stealing account passwords, browser data, and cryptocurrency wallet details from macOS users.	Malvertising	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	32ecc36701973fa9cebedefa6dbffe56d9cd3b98ea9006b44ca4310578d95fce, c6aa90e62b25e881388cb16c9fcbd665d5746a33d6bd8b632ef6e1a9fce47caf

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
PEAKLIGHT Downloader	PEAKLIGHT is a PowerShell-based downloader that performs various tasks, such as writing data to a file, extracting ZIP archives, downloading data from obfuscated URLs, and deobfuscating strings. This downloader is specifically designed to deliver and execute additional payloads on a compromised system, facilitating further malicious activities.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Deliver another payload	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	07061f3fd8c15bdd484b55baa44191aa9d045c9889234550939f46c063e6211c

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma Stealer	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two-factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444, e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41

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
SHADOWLADDER (aka Hijack Loader, DOILoader, IDAT Loader)	SHADOWLADDER is a loader first identified in July 2023. It employs a range of evasion strategies, including Process Doppelgänging, DLL Search Order Hijacking, and Heaven's Gate. Additionally, it has been documented concealing its malicious payload within the IDAT chunk of PNG files.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Loads another malware	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	bf1a0c67b433f52ebd304553f022baa34bfbca258c932d2b4b8b956b1467bfa5, 8235bd354b95a117a50922b994732cba101815a26a502ab9dc039a533329e2a5

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CryptBot	CryptBot is an advanced infostealer targeting Windows systems, capable of extracting credentials from browsers, cryptocurrency wallets, browser cookies, and credit card information, as well as taking screenshots of the infected system. All stolen data is compiled into a zip file and uploaded to a command-and-control (C2) server, enabling attackers to access and exploit the compromised information.	Pirated sites or cracked software	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Steal Data	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	34dcc780d2a2357c52019d87a0720802a92f358d15320247c80cc21060fb6f57, d6b2e83093cdaa1c59777b91a68ebd801161cf0e8f6499ca41fd2f99dfb2d839

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
VersaMem	VersaMem is a sophisticated web shell specifically designed to target and exploit Versa Director servers. It's a malicious tool used by threat actors to gain unauthorized access to compromised systems and execute various malicious activities. VersaMem was developed to leverage the vulnerabilities found in Versa Director, a software used to manage network configurations for SD-WAN applications.	Exploiting Vulnerabilities	CVE-2024-39717
TYPE		IMPACT	AFFECTED PRODUCTS
Web shell		Steal credentials	Versa Director
ASSOCIATED ACTOR			PATCH LINK
Volt Typhoon			https://support.versa-networks.com/support/solutions/articles/23000024323-release-21-2-3 , https://support.versa-networks.com/support/solutions/articles/23000025680-release-22-1-2 , https://support.versa-networks.com/support/solutions/articles/23000026033-release-22-1-3

IOC TYPE	VALUE
SHA256	4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37

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
HZ Rat backdoor	A new macOS variant of the HZ RAT backdoor has been identified, featuring capabilities to collect various types of information from infected machines. This malware gathers data about the system, user information from applications like WeChat and DingTalk, and user data stored in Google Password Manager, among others. The collected information is sent back to command-and-control (C2) servers controlled by the attackers.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Exfiltration	Windows, macOS
ASSOCIATE D ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	d9b0fcd3b20a82b97b4c74deebc7a2abb8fd771eaa12aaf66bdd5cdeaa30f706, f39aafb9489b9b60b34e3d4e78cd9720446b6247531b81cbd4877804b065a25f

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SpyGlace Backdoor	SpyGlace is a 64-bit DLL component created using C++ for remote-control backdoor operations. It features capabilities for file theft, plug-in loading, and shell command execution. SpyGlace has been identified in the wild as early as June 2022.	Exploiting Vulnerabilities	CVE-2024-7262 CVE-2024-7263
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	WPS Office for Windows
ASSOCIATED ACTOR			PATCH LINK
APT-C-60			https://www.wps.com/download/

IOC TYPE	VALUE
SHA256	861911e953e6fd0a015b3a91a7528a388a535c83f4b9a5cf7366b8209d2f00c3

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Tickler</td><td rowspan="5">Tickler is a custom multi-stage backdoor malware that allows attackers to deploy additional malicious payloads to compromised systems. Tickler can gather system information, executing commands, deleting files, and downloading or uploading files to and from a C&C server.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Compromise</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>APT33</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">7eb2e9e8cd450fc353323fd2e8b84fbbdfe061a8441fd71750250752c577d198, ccb617cc7418a3b22179e00d21db26754666979b4c4f34c7fda8c0082d08cec4</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>BlackByte Ransomware</td><td rowspan="5">BlackByte is a Ransomware-as-a-Service (RaaS) group that targets compromised Windows host systems, including both physical and virtual servers, by encrypting files. The group exploits vulnerable drivers to bypass security defenses and deploys a self-propagating ransomware encryptor with worm-like capabilities, enabling it to spread across networks and inflict widespread damage.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-37085</td></tr>
<tr><td><b>TYPE</b></td><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>Ransomware</td><td rowspan="3">Encrypt Data</td><td>VMware ESXi hypervisors</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">ae2bc7d6f78bba3e257be8ad29e879ee1683dd457a62bba6b7550adf09e9227c, 5051b6167f96e66d3c8ab5e726dc5731e0d907d8a983d5604976582bf78b14f2</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7965	✗	Google Chrome, Microsoft Edge	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chrome's V8 JavaScript Engine Inappropriate Implementation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-358	T1204.001: Malicious Link T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-39717	✗	Versa Director	Volt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:versa-networks:versa_director:*:*:*:*:*:*:*	VersaMem
Versa Director Dangerous File Type Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application T1505.003: Web Shell	https://support.versa-networks.com/support/solutions/articles/23000024323-release-21-2-3 , https://support.versa-networks.com/support/solutions/articles/23000025680-release-22-1-2 , https://support.versa-networks.com/support/solutions/articles/23000026033-release-22-1-3

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7262	✗	Kingsoft WPS Office for Windows	APT-C-60
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kingsoft:wps_office:*:*:*:*:*:*:*:*	SpyGlace Backdoor
WPS Office Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1203: Exploitation for Client Execution T1204.002: Malicious File	https://www.wps.com/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7263	✗	Kingsoft WPS Office for Windows	APT-C-60
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kingsoft:wps_office:*:*:*:*:*:*:*:*	SpyGlace Backdoor
WPS Office Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1203: Exploitation for Client Execution T1204.002: Malicious File	https://www.wps.com/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37085	✗	VMware ESXi	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	BlackByte Ransomware
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068 : Exploitation for Privilege Escalation T1136.002 : Domain Account	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Volt Typhoon (also known as Vanguard Panda, Bronze Silhouette, Dev-0391, UNC3236, Voltzite, and Insidious Taurus)	China	Construction, Education, Government, Industrial, IT, Maritime and Shipbuilding, Manufacturing, Telecommunications, Transportation, Utilities	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-39717	VersaMem	Versa Director
TTPs			
TA0002: Execution; TA0042: Resource Development; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0001: Initial Access; TA0003: Persistence; TA0043: Reconnaissance; TA0011: Command and Control; T1190: Exploit Public-Facing Application; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1036.008: Masquerade File Type; T1036: Masquerading; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1106: Native API; T1059: Command and Scripting Interpreter; T1136: Create Account; T1027: Obfuscated Files or Information; T1055: Process Injection; T1505.003: Web Shell; T1505: Server Software Component; T1589.001: Credentials; T1589: Gather Victim Identity Information; T1071: Application Layer Protocol; T1571: Non-Standard Port			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT-C-60 (aka False Hunter, Pseudo Hunter)	South Korea	Trade Industry, Human Resources	China, Hong Kong, Macau, Japan, Mongolia, North Korea, South Korea, Taiwan
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2024-7262 CVE-2024-7263	SpyGlace Backdoor	WPS Office for Windows

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0040: Impact; T1203: Exploitation for Client Execution; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1608: Stage Capabilities; T1608.001: Upload Malware; T1587: Develop Capabilities; T1587.004: Exploits; T1204.001: Malicious Link; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1010: Application Window Discovery; T1574: Hijack Execution Flow; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT33 (aka Refined Kitten, Elfin, Magnallium, Holmium, ATK 35, TA451, Cobalt Trinity, Peach Sandstorm, Yellow Orc, Curious Serpens)	Iran	Aviation, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Media, Petrochemical, Satellite, Oil and Gas Sectors	Iran, Iraq, Israel, Saudi Arabia, South Korea, UK, USA, UAE
	MOTIVE		
	Information theft and espionage, Sabotage and destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Tickler	-
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1110: Brute Force; T1110.003: Password Spraying; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1070: Indicator Removal; T1070.004: File Deletion; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1589: Gather Victim Identity Information; T1598: Phishing for Information; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1608: Stage Capabilities; T1566: Phishing; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1016: System Network Configuration Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1083: File and Directory Discovery			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **Volt Typhoon, APT-C-60, APT33** and malware **Cthulhu Stealer, Atomic Stealer, PEAKLIGHT Downloader, Lumma Stealer, SHADOWLADDER, CryptBot, VersaMem, HZ Rat backdoor, SpyGlace Backdoor, Tickler, BlackByte Ransomware.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Volt Typhoon, APT-C-60, APT33** and malware **Cthulhu Stealer, CryptBot, Lumma Stealer, SHADOWLADDER, PEAKLIGHT Downloader, HZ Rat backdoor, SpyGlace Backdoor, Tickler, BlackByte Ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

Cthulhu Stealer: The New Malware Targeting Mac Users

PEAKLIGHT Downloader the Stealthy Malware Living in Memory

Google Alerts Users to Actively Exploited Chrome Zero-Day Flaws

Versa Networks Patches Severe Zero-Day Flaw in Director Software

GitHub Addresses Admin Privilege Exploits in Enterprise Server

SonicWall SonicOS Flaw Allows Unauthorized Access & Firewall Crashes

HZ RAT Backdoor Slips into macOS Targeting Enterprise Messaging Apps

Critical FileCatalyst Workflow Flaw Enabling Attackers to Gain Admin Access

APT-C-60’s 1-Click WPS Office Exploit

APT33 Unleashes Custom Tickler Malware Targeting the US and UAE

BlackByte Ransomware Exploits VMware Flaw and Beyond

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
Cthulhu Stealer	SHA256	6483094f7784c424891644a85d5535688c8969666e16a194d397dc66779b0b12, e3f1e91de8af95cd56ec95737669c3512f90cecbc6696579ae2be349e30327a7, f79b7cbc653696af0dbd867c0a5d47698bcfc05f63b665ad48018d2610b7e97b, de33b7fb6f3d77101f81822c58540c87bd7323896913130268b9ce24f8c61e24, 96f80fef3323e5bc0ce067cd7a93b9739174e29f786b09357125550a033b0288
Atomic Stealer	SHA256	32ecc36701973fa9cebedefa6dbffe56d9cd3b98ea9006b44ca4310578d95fce, c6aa90e62b25e881388cb16c9fcbd665d5746a33d6bd8b632ef6e1a9fce47caf, 19023cd72c8de1423e8082232099c6e38db3e78ceca179af104a3b1ad579d8a5, cccdbb22401a37bc822e7d38ae7e2a229193b45eacca49e8e0aa93c1d068628e, 72ccc21294875bdce1fd698c5a8ad84b4a72af5d50c348c56eb66bd2d3fdc99a, eba753443171c3bc6695d880af2ab6d2265587414a0cd96102e315be94140252, 5d27b45077470ddd3c3e3852ebd8f63828cf65ed7ee18d7600b2026b30a38b93

Attack Name	TYPE	VALUE
PEAKLIGHT	SHA256	07061f3fd8c15bdd484b55baa44191aa9d045c9889234550939f46c063e6211c, e3bf61f6f96d1a121a1f7f47188cd36fc51f4565ca8cd8fc07207e56a038e7ca
	MD5	95361f5f264e58d6ca4538e7b436ab67, b716a1d24c05c6adee11ca7388b728d3
	URL	hxxps[:]//fatodex.b-cdn[.]net/fatodex, hxxps[:]//matodown.b-cdn[.]net/matodown, hxxps[:]//potexo.b-cdn[.]net/potexo
Lumma Stealer	SHA256	3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444, e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41
	MD5	43939986a671821203bf9b6ba52a51b4, 58c4ba9385139785e9700898cb097538
	Domain	relaxtionflouwerwi[.]shop, deprivedrinkyfaiir[.]shop, detailbaconroollyws[.]shop, messtimetabledkolvk[.]shop, considerrycurrentyws[.]shop, understanndtytonyguw[.]shop, patternapplauderw[.]shop, horsedwollfedrwos[.]shop, tropicalironexpressiw[.]shop
	File Name	oqnhustu, WebView2Loader.dll
SHADOWLADDER (aka Hijack Loader, DOILoader, IDAT Loader)	MD5	b15bac961f62448c872e1dc6d3931016, e7c43dc3ec4360374043b872f934ec9e, f98e0d9599d40ed032ff16de242987ca, b6b8164feca728db02e6b636162a2960, bb9641e3035ae8c0ab6117ecc82b65a1, 236c709bbcb92aa30b7e67705ef7f55a, d7aff07e7cd20a5419f2411f6330f530, a6c4d2072961e9a8c98712c46be588f8, 059d94e8944eca4056e92d60f7044f14, dfdc331e575dae6660d6ed3c03d214bd, 47eee41b822d953c47434377006e01fe
	File Name	Aaaa.exe, bentonite.cfg, cymophane.doc, K1.zip, K2.zip, L1.zip, LiteSkinUtils.dll, toughie.txt, WCLDll.dll

Attack Name	TYPE	VALUE
SHADOWLADDER (aka Hijack Loader, DOILoader, IDAT Loader)	URL	hxxp[:]//62[.]133[.]61[[.]]56/Downloads/Full%20Video%20HD%20(1080p)[.]lnk, hxxps[:]//fatodex[.]b-cdn[[.]]net/K1[.]zip, hxxps[:]//fatodex[.]b-cdn[[.]]net/K2[.]zip, hxxps[:]//forikabrof[[.]]click/flkhfaiouwrqkhfasdrhfsa[.]png, hxxps[:]//matodown[.]b-cdn[[.]]net/K1[.]zip, hxxps[:]//matodown[.]b-cdn[[.]]net/K2[.]zip, hxxps[:]//nextomax[.]b-cdn[[.]]net/L1[.]zip, hxxps[:]//nextomax[.]b-cdn[[.]]net/L2[.]zip, hxxps[:]//potexo[.]b-cdn[[.]]net/K1[.]zip, hxxps[:]//potexo[.]b-cdn[[.]]net/K2[.]zip
	SHA256	bf1a0c67b433f52ebd304553f022baa34bfbca258c932d2b4b8b956b1467bfa5, 8235bd354b95a117a50922b994732cba101815a26a502ab9dc039a533329e2a5
CryptBot	SHA256	34dcc780d2a2357c52019d87a0720802a92f358d15320247c80cc21060fb6f57, d6b2e83093cdaa1c59777b91a68ebd801161cf0e8f6499ca41fd2f99dfb2d839, 31fa6a32b73ceef86560bdad24f0b69c50bf035cb1b18ccbf7a97857a39deb64
	MD5	d6ea5dcdb2f88a65399f87809f43f83c, 307f40ebc6d8a207455c96d34759f1f3, d8e21ac76b228ec144217d1e85df2693
	URL	hxxp://gceight8vt[.]top/upload.php, hxxps://brewdogebar[.]com/code.vue
	File Name	erefgojgbu, L2.zip, Setup.exe
VersaMem	SHA256	4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37
	File Path	/tmp/[.]temp[.]data
HZ Rat	MD5	0c3201d0743c63075b18023bb8071e73, 6cc838049ece4fcb36386b7a3032171f, 6d478c7f94d95981eb4b6508844050a6, 7a66cd84e2d007664a66679e86832202, 7ed3fc831922733d70fb08da7a244224, 9cdb61a758afd9a893add4cef5608914, 287ccbf005667b263e0e8a1ccfb8daec, 7005c9c6e2502992017f1ffc8ef8a9b9, 7355e0790c111a59af377babedee9018, a5af0471e31e5b11fd4d3671501dfc32, da07b0608195a2d5481ad6de3cc6f195, dd71b279a0bf618bbe9bb5d934ce9caa

Attack Name	TYPE	VALUE
HZ Rat	SHA256	d9b0fcd3b20a82b97b4c74deebc7a2abb8fd771eaa12aaf66bdd5cdeaa30f706, f39aafb9489b9b60b34e3d4e78cd9720446b6247531b81cbd4877804b065a25f, f39aafb9489b9b60b34e3d4e78cd9720446b6247531b81cbd4877804b065a25f, 1e07585f52be4605be0459bc10c67598eebe8c5d003d6e2d42f4dbbd037e74c1, f3c101cd1e7be4ce6afe5d0236bfdd5b43870ff03556908f75692585cfd55c55, c689113a9a2fca2148caa90f71115c2c2bafeac36edebde4ffc63f87619033a9, ffeed91c223a718c1afd6d8f059a76ec97eb0eae6c4b2072b343be1b4eba09b8, 0cca3449ff12cb75c9fd9cf4628b5d72f5ac67d1954dc97d9830436207c4c917, 7af7422edf7c558b6215489c020673e195e5eedd99ae330bb90066924f5cf661, 6210ec0e905717359e01358118781a148b6d63834a54a25a95e32e228598c391, d006d5864108094a82315ee60ce057afc8be09546ffaa1f9cc63a51a96764114, 1400210f2eedab36caff8ce89d6d19859ba3116775981b2be8b5069ef109c2c3, 5d78fc86a389247d768a6bdf46f3e4fd697ed87c133b99ee6865809e453b2908, 87393d937407a6fe9e69dad3836e83866107809980e20a40ae010d7d72f90854
SpyGlace Backdoor	SHA256	861911e953e6fd0a015b3a91a7528a388a535c83f4b9a5cf7366b8209d2f00c3
Tickler	SHA256	7eb2e9e8cd450fc353323fd2e8b84fbbdfe061a8441fd71750250752c577d198, ccb617cc7418a3b22179e00d21db26754666979b4c4f34c7fda8c0082d08cec4, 5df4269998ed79fbc997766303759768ce89ff1412550b35ff32e85db3c1f57b, fb70ff49411ce04951895977acfc06fa468e4aa504676dedeb40ba5cea76f37f, 711d3deccc22f5acfd3a41b8c8defb111db0f2b474febdc7f20a468f67db0350
BlackByte	SHA256	ae2bc7d6f78bba3e257be8ad29e879ee1683dd457a62bba6b7550adf09e9227c, 5051b6167f96e66d3c8ab5e726dc5731e0d907d8a983d5604976582bf78b14f2,

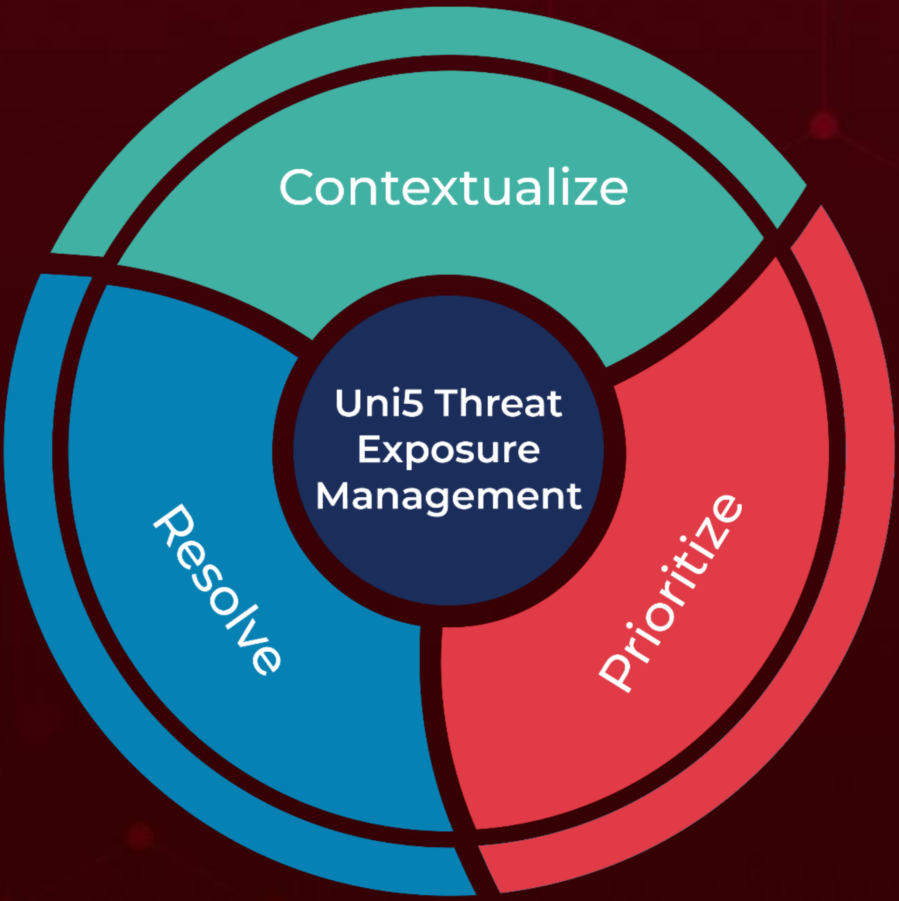
Attack Name	TYPE	VALUE
BlackByte	SHA256	98f2a569c6f67e1ed6253bb7e69f6cffcb7b29f10eadd7435b862ec3645c58f1, 0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5, 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91, 31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427

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 2, 2024 • 7:00 AM

More at www.hivepro.com