

Date of Publication  
July 08, 2024



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

01 to 07 JULY 2024

# Table Of Contents

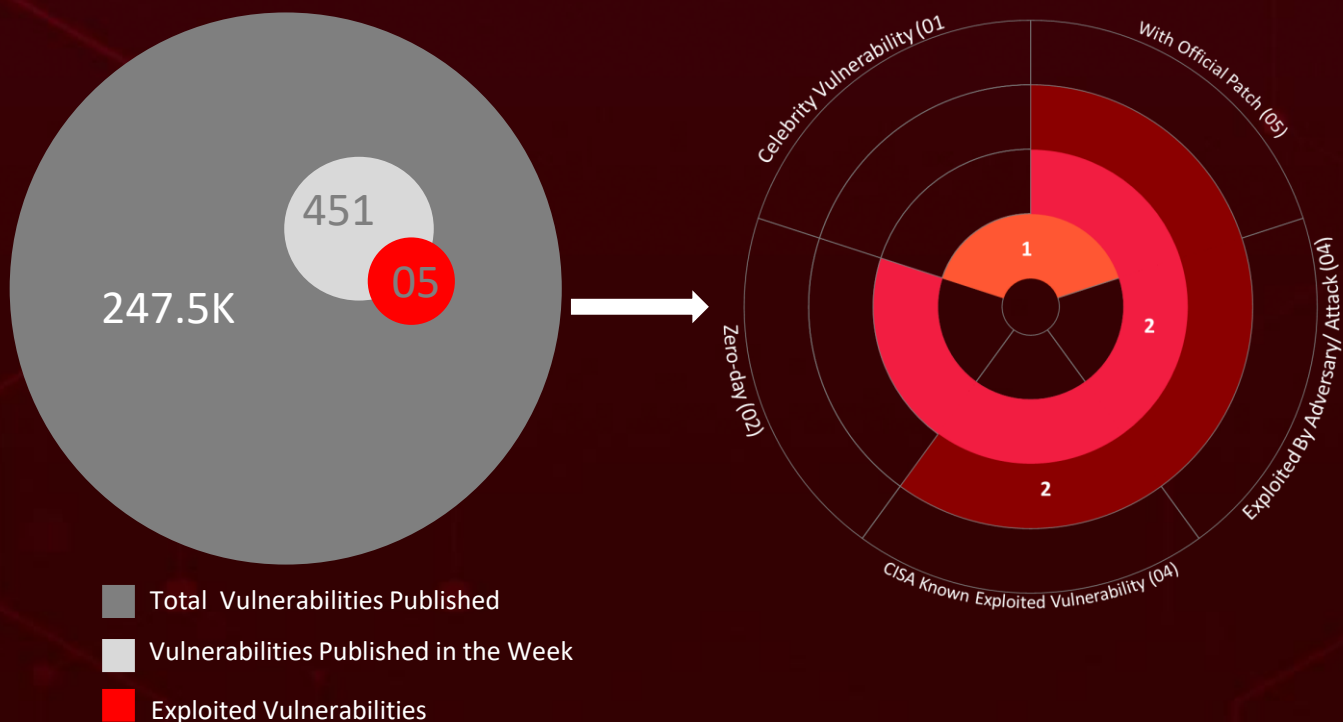
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	26

# Summary

HiveForce Labs has recently made substantial advancements in identifying cybersecurity threats. In just the past week, HiveForce Labs detected **eleven** executed attacks, reported **five** vulnerabilities, and identified **three** active adversaries. These findings underscore the persistent and escalating danger of cyber intrusions.

Moreover, the **8220 Gang**, also known as Water Sigbin, has been aggressively targeting Oracle WebLogic servers to install cryptocurrency miners. In another development, unidentified threat actors are exploiting the previously patched **CVE-2021-40444** security vulnerability in Microsoft MSHTML to disseminate **MerkSpy**.

Additionally, the "**regreSSHion**" vulnerability, **CVE-2024-6387**, in OpenSSH allows unauthenticated remote code execution with root privileges on glibc-based Linux systems. A cyber espionage group known as **Velvet Ant**, linked to China, has been exploiting the **CVE-2024-20399** zero-day vulnerability since April to spread malware. These increasing threats present a significant and immediate danger to users worldwide.



# High Level Statistics

11

Attacks  
Executed

5

Vulnerabilities  
Exploited

3

Adversaries in  
Action

- [dllFake](#)
  - [MerkSpy](#)
  - [WINELOADER](#)
  - [RootSaw](#)
  - [VaporRage](#)
  - [XMRig](#)
  - [PureCrypter](#)
  - [Nim Downloader](#)
  - [Donut](#)
  - [Silver](#)
  - [Mekotio](#)
- [CVE-2024-20399](#)
  - [CVE-2024-6387](#)
  - [CVE-2021-40444](#)
  - [CVE-2017-3506](#)
  - [CVE-2023-21839](#)
- [Velvet Ant](#)
  - [APT 29](#)
  - [8220 Gang](#)



# Insights

**India-Based**  
Company's Free  
Trials **Trojanized** to  
Spread Information-  
Stealing Malware

**Root-Level Intrusions:** Cisco  
NX-OS Zero-Day Vulnerability Exploited  
by Velvet Ant

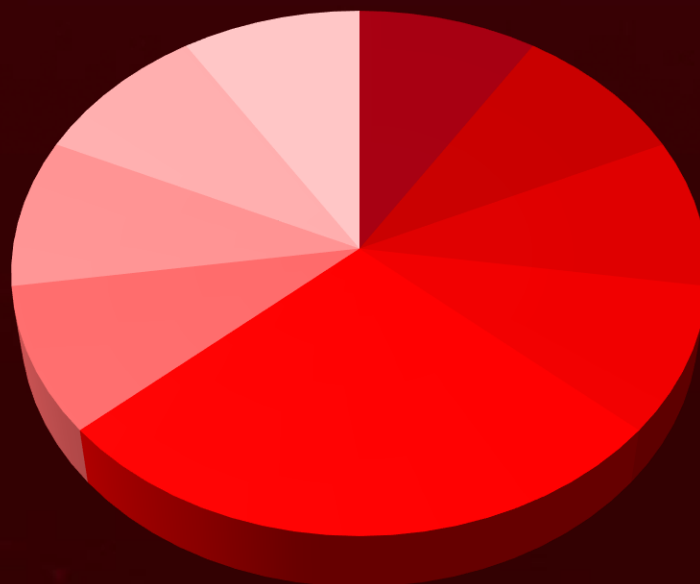
**TeamViewer Breach  
and Beyond:**  
APT29's Latest  
Cyber Espionage  
Operations

**Polyfill.io Supply Chain Attack:**  
Malicious Redirects Plague 100,000  
Websites

**Silent Surveillance: MerkSpy**  
Spyware Harvests Data Using **CVE-  
2021-40444** Exploit

**Severe OpenSSH**  
**Flaw:** 'regreSSHion'  
Vulnerability  
Threatens Linux  
Systems

## Threat Distribution



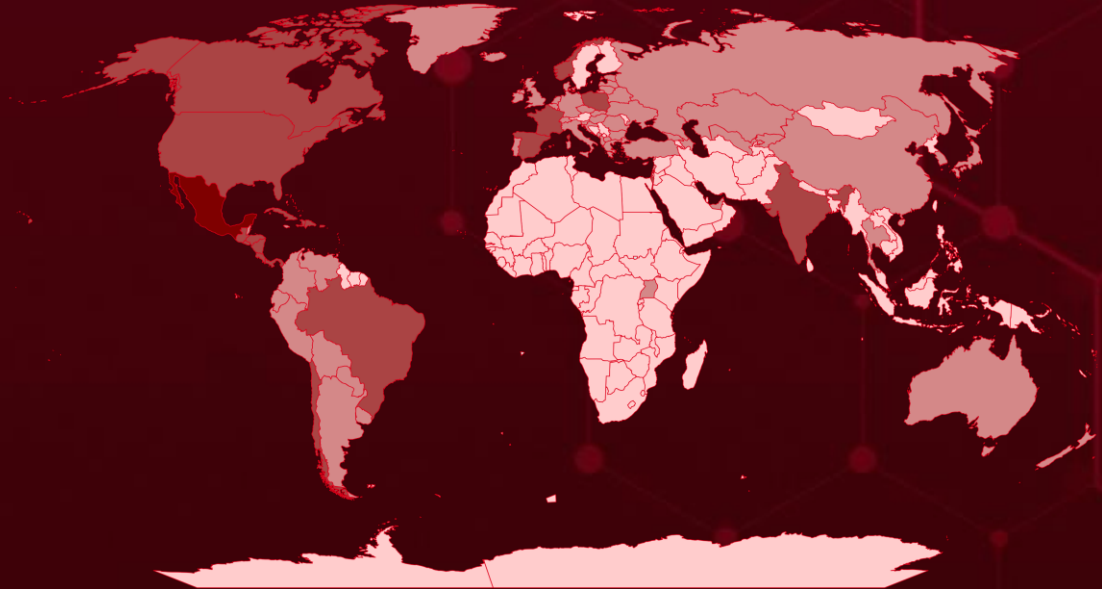
- Information Stealer
- Dropper
- Framework
- Spyware
- Downloader
- Trojan
- Backdoor
- Cryptominer
- Banking Trojan



# Targeted Countries

Most

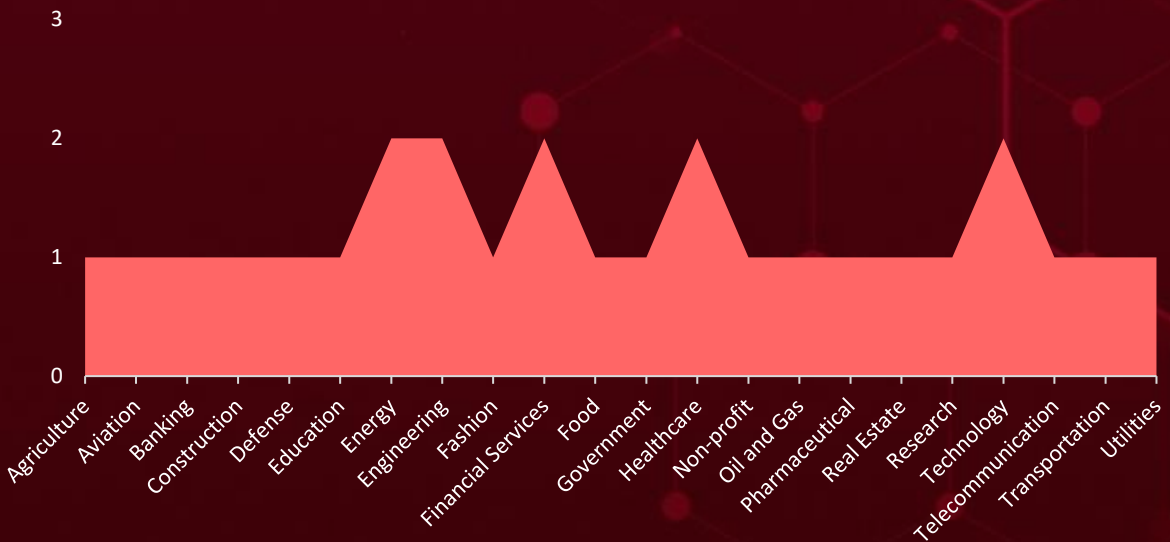
Least



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

Countries	Countries	Countries	Countries
Mexico	Aruba	Greenland	Kazakhstan
Saint Barthélemy	United Kingdom	Argentina	Thailand
Norway	Curaçao	Grenada	Latvia
Brazil	Albania	Montserrat	Turkey
Honduras	Cyprus	Guadeloupe	Lebanon
Canada	Russia	New Zealand	Uganda
Poland	Czech Republic	Barbados	Lithuania
Chile	Slovakia	North Macedonia	United Arab Emirates
Spain	Denmark	Belarus	Luxembourg
Costa Rica	Turks and Caicos Islands	British Virgin Islands	Colombia
Israel	Dominica	Belgium	Martinique
Cuba	Montenegro	Peru	Bermuda
Nicaragua	Australia	Hungary	Venezuela
Dominican Republic	Bolivia	Portugal	Ireland
Panama	Ecuador	Iceland	Kyrgyzstan
El Salvador	Paraguay	Romania	Sri Lanka
Puerto Rico	Azerbaijan	Uruguay	Easter Island
France	Anguilla	Cayman Islands	Vatican City
Saint Martin	Anguilla	Uzbekistan	Burundi
Guatemala	Estonia	Saint Lucia	Sierra Leone
United States	Saint Kitts and Nevis	Belize	Guam
Haiti	Bahamas	Saint Pierre and Miquelon	Tunisia
India	Singapore	Miquelon	Cambodia
Switzerland	Georgia	Italy	Bir Tawil
Bulgaria	South Korea	Sint Maarten	Guernsey
Netherlands	Germany	Jamaica	Saint Vincent and the Grenadines
Croatia	Trinidad and Tobago	Slovenia	Guinea
Antigua and Barbuda	Greece	Japan	
	Ukraine	China	

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1588.006

Vulnerabilities

### T1588

Obtain Capabilities

### T1204

User Execution

### T1204.002

Malicious File

### T1068

Exploitation for Privilege Escalation

### T1036

Masquerading

### T1203

Exploitation for Client Execution

### T1082

System Information Discovery

### T1190

Exploit Public-Facing Application

### T1056.001

Keylogging

### T1053.005

Scheduled Task

### T1566

Phishing

### T1071

Application Layer Protocol

### T1056

Input Capture

### T1027

Obfuscated Files or Information

### T1555.003

Credentials from Web Browsers

### T1547.001

Registry Run Keys / Startup Folder

### T1588.005

Exploits

### T1562.001

Disable or Modify Tools



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">dllFake</a>	The dllFake information-stealing malware, which has been circulating since at least January 2024, can steal browser credentials and cryptocurrency wallet information, log clipboard contents and keystrokes, and download and execute additional payloads on infected Windows hosts.	Trojanized software products	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information Stealer		Information Theft, Resource Hijacking	Notezilla, Copywhiz, and RecentX
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-	-	-	-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	1fa84b696b055f614ccd4640b724d90ccad4afc035358822224a02a9e2c12846, cdc1f2430681e9278b3f738ed74954c4366b8eff52c937f185d760c1bbba2f1d, fdc84cb0845f87a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91eb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#">MerkSpy</a>	MerkSpy is a surveillance spyware designed to covertly monitor and collect information from a victim's computer without their knowledge or consent. It can record activities such as keystrokes, browsing behavior, and personal information, often transmitting this data to a third party for espionage or theft.	Exploiting Vulnerability	CVE-2021-40444
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Spyware		Information Theft, Compromise Infrastructure	Microsoft Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-	-	-	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08, 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a		

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>WINELOADER</u></b>	The new modular backdoor WINELOADER features a modular design, where encrypted modules are downloaded from the C2 server. This backdoor employs techniques such as re-encryption and zeroing out memory buffers to protect sensitive data in memory and evade memory forensics solutions.	Spear Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
APT 29			-
<b>IOC TYPE</b>		<b>VALUE</b>	
SHA256	d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b7417501c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc,3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>RootSaw</u></b>	ROOTSAW, also known as EnvyScout, is a malicious dropper program used in the initial stage of attacks by the APT29 hacking group. Its main purpose is to install the actual malicious payload, such as WINELOADER, which allows attackers remote access.	Spear Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Dropper			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
APT 29			-
<b>IOC TYPE</b>		<b>VALUE</b>	
SHA256	a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c		

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>VaporRage</u></b>	VaporRage, a downloader malware by the APT29 group. VaporRage is designed to download, decode, and execute an arbitrary payload fully in memory. Its deployment patterns, including staging payloads on compromised websites, make it challenging for traditional forensic investigations.	Spear Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Information Theft, Espionage	-
			<b>PATCH LINK</b>
<b>TYPE</b>			
Downloader			
<b>ASSOCIATED ACTOR</b>			
APT 29			-
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4, 7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>XMRig</u></b>	XMRig is a widely-used form of malware designed to mine cryptocurrencies like Monero. It covertly harnesses the computing power of infected systems for unauthorized mining activities.	Exploiting vulnerabilities	CVE-2017-3506 CVE-2023-21839
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
		Information Theft, Espionage, Resource Hijacking, Financial Loss	Oracle WebLogic Server
			<b>PATCH LINKS</b>
<b>TYPE</b>			
Cryptominer			
<b>ASSOCIATED ACTOR</b>			
8220 Gang			<a href="https://www.oracle.com/security-alerts/cpuapr2017.html">https://www.oracle.com/security-alerts/cpuapr2017.html</a> <a href="https://www.oracle.com/security-alerts/cpujan2023.html">https://www.oracle.com/security-alerts/cpujan2023.html</a>
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	f4d1b970bc9e5d319c5432be9e3863b5a20bf26e557c8cea6f3949df0012cf01, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b,		

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>PureCrypter</u>	PureCrypter is an advanced loader that has been marketed since at least March 2021. This malware is known for distributing various remote access trojans and information stealers. The loader, implemented as a .NET executable, uses SmartAssembly for obfuscation and other obfuscation techniques to evade antivirus detection.	Exploiting vulnerabilities	CVE-2017-3506 CVE-2023-21839
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b> Downloader		Information Theft, Espionage, Resource Hijacking,	Oracle WebLogic Server
			<b>PATCH LINKS</b>
			<a href="https://www.oracle.com/security-alerts/cpuapr2017.html">https://www.oracle.com/security-alerts/cpuapr2017.html</a> <a href="https://www.oracle.com/security-alerts/cpujan2023.html">https://www.oracle.com/security-alerts/cpujan2023.html</a>
<b>ASSOCIATED ACTOR</b> 8220 Gang			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3, 5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2cd80e99, 5d649c5aa230376f1a08074aee91129b8031606856e9b4b6c6d0387f35f6629d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nim Downloader</u>	The Nim downloader is a basic utility coded in Nim, designed to retrieve second-stage malware from a staging server under the attacker's control.	Social Engineering	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b> Downloader		Information Theft, Espionage	-
			<b>PATCH LINK</b>
			-
<b>ASSOCIATED ACTOR</b> -			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	d891f4339354d3f4c4b834e781fa4eaca2b59c6a8ee9340cc489ab0023e034c8, d7a66f8529f1c32342c4ed06c4a4750a93bd44161f578e5b94d6d30f7cc41581, c21ad804c22a67ddb62adf5f6153a99268f0b26e359b842ebeabcada824c277f		

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>Donut</u>	Donut, a position-independent shellcode generation framework, is engineered to bypass security measures by manipulating functions, facilitating the deployment and execution of embedded payloads.	Social Engineering	-	
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
<b>TYPE</b> Framework		Information Theft, Espionage	-	
			<b>ASSOCIATED ACTOR</b>	<b>PATCH LINK</b>
			-	
-				
<b>IOC TYPE</b>	<b>VALUE</b>			
SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223df090bb26b3cd7			




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Silver</u>	Sliver, a freely available Golang trojan designed as a substitute for CobaltStrike, provides attackers with complete control over the victim's machine, allowing them to leverage all of Sliver's functionalities to carry out any desired actions.	Social Engineering	-	
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
<b>TYPE</b> Trojan		Information Theft, Espionage	-	
			<b>ASSOCIATED ACTOR</b>	<b>PATCH LINK</b>
			-	
-				
<b>IOC TYPE</b>	<b>VALUE</b>			
SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223df090bb26b3cd7			
Hostname	www.economy-gov-il[.]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
<b><u>Mekotio</u></b>	The Mekotio banking trojan, a sophisticated malware in operation since at least 2015, predominantly targets Latin American countries to illicitly obtain sensitive information, especially banking credentials. Mekotio is linked to other notable Latin American banking malware, including Grandoreiro.	Social Engineering	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Information Theft, Financial Gain, and Compromise infrastructure	-
Banking Trojan			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			
-			
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA1	5e92f0fcddc1478d46914835f012137d7ee3c217, f68d3a25433888aa606e18f0717d693443fe9f5a, 3fe5d098952796c0593881800975bcb09f1fe9ed		




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><a href="#">CVE-2024-20399</a></u>		MDS 9000 Series Multilayer Switches, Nexus 3000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode	Velvet Ant
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:h:cisco:nx-os:*:*:*:*:*:*	-
Cisco NX-OS Software CLI Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1059.008: Network Device CLI	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2017-3506</u></a>		Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	8220 Gang (aka Water Sigbin)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:weblogic_server:-:*:*:*:*:*	XMRig Cryptominer, PureCrypter loader
Oracle WebLogic Server 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://www.oracle.com/security-alerts/cpuapr2017.html">https://www.oracle.com/security-alerts/cpuapr2017.html</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-21839</u></a>		Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	8220 Gang (aka Water Sigbin)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:weblogic_server:-:*:*:*:*:*	XMRig Cryptominer, PureCrypter loader
Oracle WebLogic Server Unauthenticated RCE Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190 Exploit Public-Facing Application	<a href="https://www.oracle.com/security-alerts/cpujan2023.html">https://www.oracle.com/security-alerts/cpujan2023.html</a>



# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>Velvet Ant</b>	China	All	Worldwide
	<b>MOTIVE</b> Information Theft, Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-20399	-	Cisco NX-OS Software
	<b>TTPs</b>		
TA0042: Resource Development; TA0011: Command and Control; TA0010: Exfiltration; TA0009: Collection; TA0008: Lateral Movement; TA0007: Discovery; TA0006: Credential Access; TA0005: Defense Evasion; TA0004: Privilege Escalation; TA0003: Persistence; TA0002: Execution; TA0001: Initial Access; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1572: Protocol Tunneling; T1570: Lateral Tool Transfer; T1569: System Services; T1569.002: Service Execution; T1562.004: Disable or Modify System Firewall; T1135: Network Share Discovery; T1133: External Remote Services; T1090.001: Internal Proxy; T1087.002: Domain Account; T1083: File and Directory Discovery; T1082: System Information Discovery; T1078.003: Local Accounts; T1078.002: Domain Accounts; T1070.006: Timestamp; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1059.008: Network Device CLI; T1055: Process Injection; T1048: Exfiltration Over Alternative Protocol; T1047: Windows Management Instrumentation; T1039: Data from Network Shared Drive; T1037.004: RC Scripts; T1021.004: SSH; T1021.001: Remote Desktop Protocol; T1018: Remote System Discovery; T1016: System Network Configuration Discovery; T1003.001: LSASS Memory			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES		
 <p><b><u>APT 29 (aka Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, ATK7, Blue Kitsune, G0016, Midnight Blizzard, SeaDuke, TA421, UAC-0029)</u></b></p>	Russia	Aerospace, Defense, Education, Embassies, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Technology	Australia, Azerbaijan, Belarus, Belgium, Brazil, Canada, Chechnya, Chile, China, Cyprus, Czech, Denmark, France, Georgia, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Luxembourg, Mexico, Netherlands, New Zealand, Portugal, Russia, Singapore, Spain, South Korea, Switzerland, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO		
	<b>MOTIVE</b>			<b>TARGETED CVEs</b>	<b>AFFECTED PRODUCTS</b>
	Espionage and Information theft	<b>ASSOCIATED ATTACKS/RANSOM WARE</b>			
		WINELOADER, RootSaw, VaporRage	-		
<b>TTPs</b>					
TA0007: Discovery; TA0011: Command and Control; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1082: System Information Discovery; T1134: Access Token Manipulation; T1057: Process Discovery; T1007: System Service Discovery; T1027: Obfuscated Files or Information; T1070.004: File Deletion; T1070: Indicator Removal; T1055.003: Thread Execution Hijacking; T1055: Process Injection; T1083: File and Directory Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1566: Phishing; T1110: Brute Force; T1110.003: Password Spraying; T1078.004: Cloud Accounts; T1528: Steal Application Access Token; T1078: Valid Accounts; T1621: Multi-Factor Authentication Request Generation; T1543.003: Windows Service; T1543: Create or Modify System Process; T1012: Query Registry; T1098.005: Device Registration; T1098: Account Manipulation; T1651: Cloud Administration Command; T1059.009: Cloud API; T1059: Command and Scripting Interpreter					

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>8220 Gang (aka 8220 Mining Group, Water Sigbin)</b>	China	All	Worldwide
	<b>MOTIVE</b>		
	Financial Gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2017-3506 CVE-2023-21839	XMRig Cryptominer, PureCrypter loader	Oracle WebLogic Server
<b>TTPs</b>			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1047: Windows Management Instrumentation; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information; T1112: Modify Registry; T1562.001: Disable or Modify Tools; T1620: Reflective Code Loading; T1055: Process Injection; T1055.012: Process Hollowing; T1053.005: Scheduled Task; T1057: Process Discovery; T1012: Query Registry; T1518.001: Security Software Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1001: Data Obfuscation; T1571: Non-Standard Port; T1095: Non-Application Layer Protocol; T1496: Resource Hijacking			

# 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 **Velvet Ant, APT 29, 8220 Gang**, and malware **dllFake, MerkSpy, WINELOADER, RootSaw, VaporRage, XMRig, PureCrypter, Nim Downloader, Donut, Silver, Mekotio**.

## 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 **Velvet Ant, APT 29, 8220 Gang**, and malware **dllFake, MerkSpy, Nim Downloader, Mekotio** in Breach and Attack Simulation(BAS).

# Threat Advisories

[China-linked Hackers Exploit Cisco NX-OS as Zero-Day](#)

[regreSSHion: Exploiting Signal Handler Race Condition in OpenSSH](#)

[Free Trials of Sticky Notes Installer Trojanized](#)

[Microsoft MSHTML Flaw the Silent Doorway for MerkSpy Malware](#)

[Juniper Routers Auth Bypass Flaw Leads to Complete Device Takeover](#)

[APT29: A Deep Dive into Russia's Cyber Espionage](#)

[MSI Installer Flaw Enables Privilege Escalation on Windows Systems](#)

[8220 Gang's Heist: Exploiting Oracle WebLogic for Cryptomining](#)

[Polyfill.io Supply Chain Attack: Widespread Compromise Affects Over 100,000 Websites](#)

[Attackers Impersonating Israeli Ministry with Blended Tools](#)

[Mekotio Trojan Targets the Latin American Financial Sector](#)

[Critical OpenStack Vulnerability Exposes Cloud Data](#)

# 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><a href="#">dllFake</a></u>	SHA256	1fa84b696b055f614ccd4640b724d90ccad4afc035358822224a02a9e2c12846, cdc1f2430681e9278b3f738ed74954c4366b8eff52c937f185d760c1bbba2f1d, fdc84cb0845f87a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91eb, a89953915eabe5c4897e414e73f28c300472298a6a8c055fcc956c61c875fd96, 70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093, 33e4d5eed3527c269467eec2ac57ae94ae34fd1d0a145505a29c51cf8e83f1b9, 03761d9fd24a2530b386c07bf886350ae497e693440a9319903072b93a30c82d, de4e03288071cdebe5c26913888b135fb2424132856cc892baea9792d6c66249
<u><a href="#">MerkSpy</a></u>	SHA256	92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08, 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a, 0ffadb53f9624950dea0e07fcffcc31404299230735746ca43d4db05e4d708c6, dd369262074466ce937b52c0acd75abad112e395f353072ae11e3e888ac132a8, 569f6cd88806d9db9e92a579dea7a9241352d900f53ff7fe241b0006ba3f0e22, 6cdc2355cf07a240e78459dd4dd32e26210e22bf5e4a15ea08a984a5d9241067

Attack Name	TYPE	VALUE
<u>WINELOADER</u>	SHA256	d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b741750, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45
<u>RootSaw</u>	SHA256	a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c
<u>VaporRage</u>	SHA256	c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4, 7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e, 773f0102720af2957859d6930cd09693824d87db705b3303cef9ee794375ce13
<u>XMRig</u>	SHA256	f4d1b970bc9e5d319c5432be9e3863b5a20bf26e557c8cea6f3949df0012cf01, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, f34fc824a6c655bd6320b7818acdad9a5a570b88dd46507fdf73cd254af9b19f, 621a9f892436647a492e3877502454d1783dc0cf4e4ba9f3f459a8c2ac7e6d97, f63921129822475dd132a116b11312ebbb0cdc8b54f188aabeb7cf7a8c9065fd, 05e1988f56fe199f7e401c8f4d6ee50bb26ab34fb3f96c22de959c7e5f92de77, d0cf7388253342f43f9b04da27f3da9ee18614539efdc2d9c4a0239af51ddbe4, 09ec3bf64600d1fedbd11bb3ebb705a0f541d1310f5f8690de70d37648fcd4b4

Attack Name	TYPE	VALUE
<p><b>PureCrypter</b></p>	SHA256	<p>397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3,  5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2cd80e99,  5d649c5aa230376f1a08074aee91129b8031606856e9b4b6c6d0387f35f6629d,  7a5b8b448e7d4fa5edc94dcb66b1493adad87b62291be4ddcbd61fb4f25346a8,  a7c006a79a6ded6b1cb39a71183123dcaaaa21ea2684a8f199f27e16fcb30e8e,  be18d4fc15b51daedc3165112dad779e17389793fe0515d62bbcf00def2c3c2d,  c846e7bbbc1f65452bdca87523edf0fd1a58cbd9a45e622e29d480d8d80ac331,  efc0b3bfcec19ef704697bf0c4fd4f1cfb091dbfee9c7bf456fac02bcffcdef,  f950d207d33507345beeb3605c4e0adfa6b274e67f59db10bd08b91c96e8f5ad</p>
	MD5	<p>0d8b1ad53fddacf2221409c1c1f3fd70,  0ede257a56a6b1fbd2b1405568b44015,  14e4bfe2b41a8cf4b3ab724400629214,  17f512e1a9f5e35ce5761dba6ccb09cb,  18e9cd6b282d626e47c2074783a2fa78,  1d3c8ca9c0d2d70c656f41f0ac0fe818,  2499343e00b0855882284e37bf0fa327,  2964ce62d3c776ba7cb68a48d6afb06e,  2fa290d07b56bde282073b955eae573e,  3f92847d032f4986026992893acf271e,  5420dcbae4f1fba8afe85cb03dcd9bfc,  61259b55b8912888e90f516ca08dc514,  71b4db69df677a2acd60896e11237146,  754920678bc60dabeb7c96bfb88273de,  765f09987f0ea9a3797c82a1c3fced46,  785bfaa6322450f1c7fe7f0bf260772d,  8503b56d9585b8c9e6333bb22c610b54,  8ef7d7ec24fb7f6b994006e9f339d9af,  a478540cda34b75688c4c6da4babf973,  ae158d61bed131bcfd7d6cecdccde79b,  b4fd2d06ac3ea18077848c9e96a25142,  b5c60625612fe650be3dcbe558db1bbc,  b6c849fcdca6c6d8367f159047d26c4,  bbd003bc5c9d50211645b028833bbeb2c3b90a10922eef6d635c6c786f29a5d0,  c9ca95c2a07339edb13784c72f876a60,  d70bb6e2f03e5f456103b9d6e2dc2ee7,  dbcaa05d5ca47ff8c893f47ad9131b29,  de94d596cac180d348a4acdeaaaa9439,  eaaf20fdc4a07418b0c8e85a2e3c9b27,  f1c29ba01377c35e6f920f0aa626eaf5,</p>



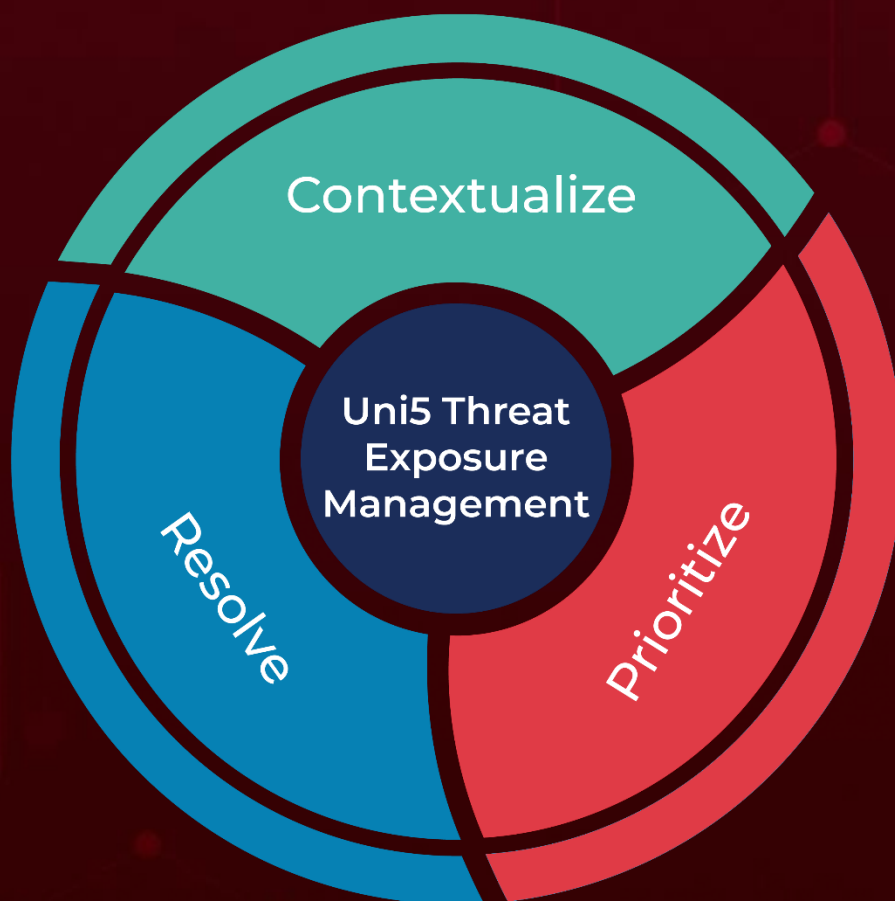
Attack Name	TYPE	VALUE
<u>PureCrypter</u>	MD5	f34d5f2d4577ed6d9ceec516c1f5a744, f4eebe921b734d563e539752be05931d, fa4ffa1f263f5fc67309569975611640, fdd4cd11d278dab26c2c8551e006c4ed
<u>Nim Downloader</u>	SHA256	d891f4339354d3f4c4b834e781fa4eaca2b59c6a8ee9340cc48 9ab0023e034c8, d7a66f8529f1c32342c4ed06c4a4750a93bd44161f578e5b94d 6d30f7cc41581, c21ad804c22a67ddb62adf5f6153a99268f0b26e359b842ebeb bcada824c277f
	URL	hxxps://auth.economy-gov- il[.]com/SUPPOSED_GRASSHOPPER.bin?token=ghhdjsdgsd
<u>Donut</u>	SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223 df090bb26b3cd7
<u>Silver</u>	SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223 df090bb26b3cd7
	Hostname	www.economy-gov-il[.]com
<u>Mekotio</u>	SHA1	5e92f0fcddc1478d46914835f012137d7ee3c217, f68d3a25433888aa606e18f0717d693443fe9f5a, 3fe5d098952796c0593881800975bcb09f1fe9ed, 1087b318449d7184131f0f21a2810013b166bf37, ef22c6b4323a4557ad235f5bd80d995a6a15024a

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

**July 8, 2024 • 11:00 PM**

© 2024 All Rights are Reserved by Hive Pro



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