Date of Publication
January 22, 2024

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

15 to 21 JANUARY 2024

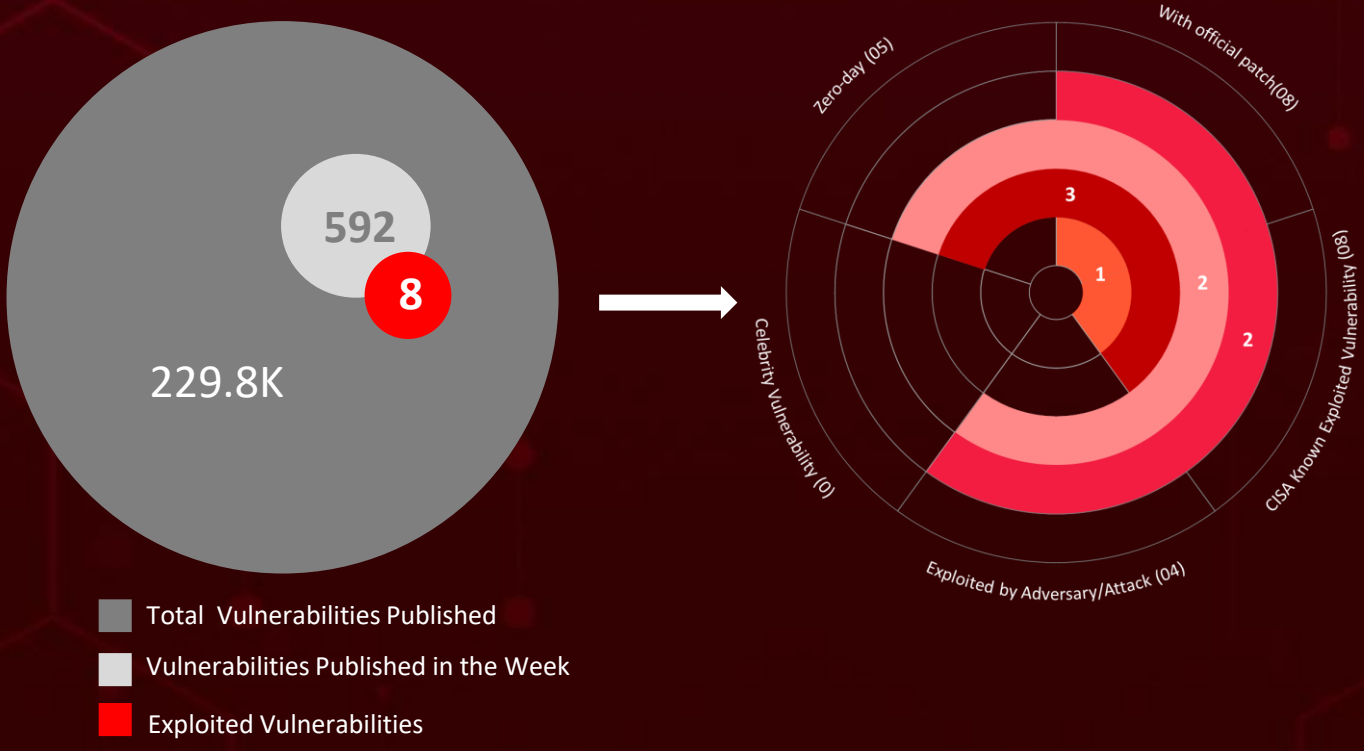
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **six** executed attacks, **two** instances of adversary activity, and **eight** exploited vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered Iranian espionage group **Mint Sandstorm**, targeted high-profile Individuals of research organizations and universities in a recent phishing by deploying new backdoor malware MediaPl backdoor and MischiefTut.

Meanwhile, a critical zero-day vulnerability (**CVE-2024-0519**), in Google Chrome that can lead to program crashes or enable arbitrary code execution. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

6
Attacks Executed

8
Vulnerabilities Exploited

2
Adversaries in Action

- Monero Cryptominer
- Phemedrone Stealer
- MediaPl Backdoor
- MischiefTut
- Androxgh0st
- SPICA Backdoor

- CVE-2023-29357
- CVE-2023-36025
- CVE-2024-0519
- CVE-2023-6548
- CVE-2023-6549
- CVE-2017-9841
- CVE-2018-15133
- CVE-2021-41773

- Mint Sandstorm
- COLDRIVER

Insights

Zero-Day

Google Chrome fixes CVE-2024-0519, that can lead to program crashes or enable arbitrary code execution

CVE-2023-36025

Phemedrone stealer malware campaign exploits a vulnerability in Microsoft Defender SmartScreen

Mint Sandstorm

threat actor targeting high-profile individuals in Middle Eastern affairs at universities and research organizations

Androxgh0st malware

is building a botnet, specifically aimed at illicitlyobtaining cloud credentials from popular applications such as Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio

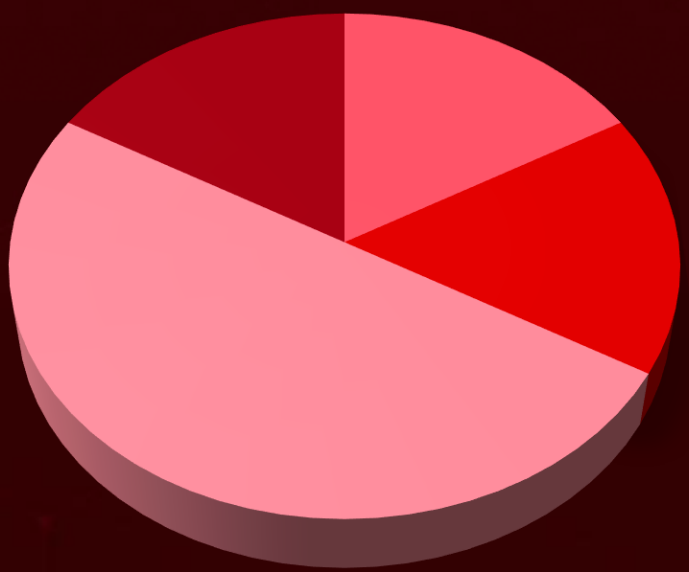
Citrix Zero-day

NetScaler ADC and NetScaler Gateway are affected by actively exploited zero-day vulnerabilities, identified as CVE-2023-6548 and CVE-2023-6549

COLDRIVER

Threat actor introduced its first custom malware, the **SPICA backdoor**, written in the Rust programming language

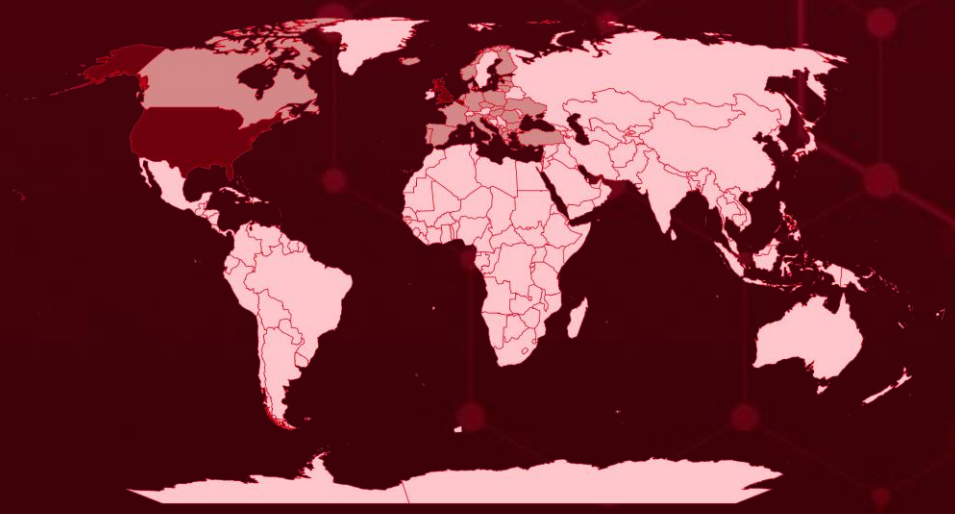
Threat Distribution



Targeted Countries

Most

Least



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

Countries
Belgium
United Kingdom
United States
Latvia
Portugal
Netherlands
Gaza
Spain
Bulgaria
Luxembourg
Canada
Norway
Croatia
Slovakia
Czech Republic
Ukraine
Denmark
Lithuania
Estonia
Montenegro
Finland

Countries
North Macedonia
France
Poland
Germany
Romania
Greece
Slovenia
Hungary
Turkey
Israel
Albania
France
Iceland
Italy
Switzerland
Uruguay
Tajikistan
Uzbekistan
The Bahamas

Countries
Ecuador
San Marino
Antigua and Barbuda
El Salvador
Sweden
Tanzania
Turkmenistan
Georgia
Barbados
Monaco
Grenada
Guatemala
Iraq
Saint Vincent and the Grenadines
Ireland
Saudi Arabia
Bahrain
Jamaica
Suriname
Jordan

Targeted Industries

TOP MITRE ATT&CK TTPS

T1082 System Information Discovery

T1083 File and Directory Discovery

T1059 Command and Scripting Interpreter

T1588 Obtain Capabilities

T1588.006 Vulnerabilities

T1588.005 Exploits

T1204 User Execution

T1027 Obfuscated Files or Information

T1566 Phishing

T1204.002 Malicious File

T1055 Process Injection

T1498 Network Denial of Service

T1041 Exfiltration Over C2 Channel

T1059.001 PowerShell

T1036 Masquerading

T1105 Ingress Tool Transfer

T1057 Process Discovery

T1659 Content Injection

T1190 Exploit Public-Facing Application

T1071.001 Web Protocols

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Monero	Monero, a privacy-focused cryptocurrency, has become a magnet for cryptominers, both legitimate and malicious. The lure lies in its unique mining algorithm, RandomX, designed to be resistant to specialized hardware (ASICs) and favor consumer-grade CPUs and GPUs.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	-
Cryptominer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	eea29961fc606fdc27bd77707bd3f7e4b8a1b17d73d7c6fcd20c014ecdb4e3fb, 61531092cd9111095aef20168c61a85f61e2bdc7341adbcdb60c39adba4d395c, 8afc300d41966777e10c321153a106125bd29ee6cf5cc0d8794697da826b5b65, 04aceaa4d58f373e64c78d19cb0d37da3453374014b2f391684958b6bb10e7f4, 7dafec3494c7b178e9cec154b89b520e789c117d735fdabb2dd9c0bd5338548b

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
Phemedrone	The Phemedrone stealer malware campaign exploits a vulnerability in Microsoft Defender SmartScreen. Phemedrone, an open-source information-stealing malware written in C#, is designed to extract data from web browsers, and cryptocurrency wallets.	Exploiting vulnerabilities	CVE-2023-36025
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025
IOC TYPE	**VALUE**		
SHA256	f32964087462ba3c96a87ee8387f89de8fa605f2f5bb84cb5f754cd736683f2d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424, 815b2125d6f0a5d99750614731aaad2c6936a1dc107a969408a88973f35064c0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MediaPl	MediaPL is a highly sophisticated malware strain crafted to undermine the security of researchers and compromise their data. Functioning as a backdoor trojan, its primary purpose is to illicitly harvest data from compromised computers.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Mint Sandstorm			-
IOC TYPE	**VALUE**		
SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f		

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 rowspan="2">Androxgh0st</td><td rowspan="6">The Androxgh0st malware is building a botnet, specifically aimed at illicitly obtaining cloud credentials from popular applications such as Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio. This stolen data is then utilized to disseminate additional harmful payloads.</td><td>Exploiting vulnerabilities</td><td>CVE-2017-9841
CVE-2018-15133
CVE-2021-41773</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Data Theft</td><td rowspan="2">Amazon Web Services (AWS), Microsoft Office 365, SendGrid, and Twilio</td></tr>
<tr><td>SMTP cracker</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://www.oracle.com/security-alerts/cpuoct2021.html; https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30; https://httpd.apache.org/security/vulnerabilities_24.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA1</td><td colspan="3">0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef,
23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066,
59e90be75e51c86b4b9b69dcede2cf815da5a79f7e05cac27c95ec35294151f4,
6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc,
bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7</td></tr>
</table>

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
MischiefTut	MischiefTut, a custom PowerShell-based backdoor, performs reconnaissance, records outputs, and can download additional tools on compromised systems.	Unknown	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Mint Sandstorm			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SPICA	SPICA, written in Rust, employs JSON over websockets for command and control. It executes shell commands, steals browser cookies, uploads/downloads files, and explores the filesystem. Upon execution, it establishes persistence and opens a decoy PDF, awaiting further commands in its C2 loop.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Exfiltration, Disruption	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
COLDRIVER			-
IOC TYPE	VALUE		
SHA256	84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507, 37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9, C97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d		

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-2023-29357	✗	Microsoft SharePoint Server: 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*	-
Microsoft SharePoint Server Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36025	✗	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:*:*:*:*:*:*:*:*	Phemedrone Stealer
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0519		Google Chrome prior to 120.0.6099.224	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Out of bounds memory access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1082: System Information Discovery	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6548		NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15, NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21, NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1055: Process Injection, T1059: Command and Scripting Interpreter	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6549	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35, NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15, NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21, NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1059: Command and Scripting Interpreter	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9841	✗	PHPUnit: 4.8.0 - 5.6.2	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:phpunit_project:phpunit:*:*:*:*:*:*:*:*	Androxgh0st
PHPUnit Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94	T1055: Process Injection, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpuoct2021.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-15133		Laravel Framework: 5.5.0 - 5.6.29	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:laravel:laravel:*:*:*:*:*:*:*:*	Androxgh0st
Laravel Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-41773		Apache HTTP Server versions 2.4.49 or 2.4.50	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*	Androxgh0st
Apache HTTP Server Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter	https://httpd.apache.org/security/vulnerabilities_24.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Mint Sandstorm (aka Charming Kitten, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Ballistic Bobcat)	Iran	High-profile Individuals of research organizations and universities	Belgium, France, Gaza, Israel, the United Kingdom, and the United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MediaPl backdoor, MischiefTut	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting: Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1036: Masquerading; T1573: Encrypted Channel; T1053: Scheduled Task/Job; T1204: User Execution; T1204.002: Malicious File; T1132: Data Encoding; T1132.001: Standard Encoding

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
COLDRIVER (aka Star Blizzard, Nahrelbared, NahrElbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto)</td><td>Russia</td><td rowspan="2">High profile individuals in NGOs, former intelligence and military officers and NATO governments</td><td rowspan="2">Ukraine, NATO countries</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>SPICA backdoor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1539: Steal Web Session Cookie; T1083: File and Directory Discovery; T1053: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1560: Archive Collected Data; T1105: Ingress Tool Transfer; T1071: Application Layer: Protocol; T1071.001: Web Protocols</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actor **Mint Sandstorm, COLDRIVER** and malware **Monero cryptominer, Phemedrone Stealer, MediaPl backdoor, Androxgh0st, SPICA backdoor.**

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 **eight exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Mint Sandstorm, COLDRIVER** and malware **Monero cryptominer, Phemedrone Stealer, MediaPl backdoor, Androxgh0st, SPICA backdoor** in Breach and Attack Simulation(BAS).

Threat Advisories

Active Exploitation of Two Critical Flaws in Microsoft SharePoint

New Attacks Target Misconfigured Apache Applications with Monero Miner

Windows SmartScreen Exploit Paves the Way for Phemedrone Stealer

Juniper's Critical RCE Vulnerability Shakes Network Security

Google Fixes First Actively Exploited Chrome Zero-day of 2024

Citrix Warns of Critical Netscaler Flaws Actively Exploited in Attacks - Urges Immediate Patching

Mint Sandstorm’s Campaign Targets Researchers with Novel Backdoor

GitLab Fixes Critical Account Takeover Vulnerability

Androxgh0st Malware Uses Stealthy Tactics in Pilfering Credentials

COLDRIVER Expands Beyond Phishing, Incorporating Custom SPICA Backdoor

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.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Monero cryptominer	SHA256	eea29961fc606fdc27bd77707bd3f7e4b8a1b17d73d7c6fcd20c014ecdb4e3fb, 61531092cd9111095aef20168c61a85f61e2bdc7341adbcdb60c39adba4d395c, 8afc300d41966777e10c321153a106125bd29ee6cf5cc0d8794697da826b5b65, 04aceaa4d58f373e64c78d19cb0d37da3453374014b2f391684958b6bb10e7f4, 7dafec3494c7b178e9cec154b89b520e789c117d735fdabb2dd9c0bd5338548b, a3af09049c4ba6ef13bf2ec645cf653777ede84c0cfc04f2aa6c0c9fa6e93dac, 6ef7e257764b1438c3a83f46699c81ad46ec35a38737f7980d65debc0fbf2007, ab8601854e04de69ec28b2996a364854a8a9ff238574569305d7455e6c52f690, 4d2c328739e69a3dcb457ca7447eba21b8d364af33539fbc2a51c24dafd28eb4, 1727ffd1ed79775dd36fc812381aea3414a2f235ff8ce7755eb0b1b7388af7cc, d073960d52393ccf2af5a7cc0661a41a913a5c440158a29794a8461bf27bd8b6, e613ef1133c27266edf01b389575336b471101f202cc92e513a40ca7b91b9dfe, 0375749ada9056ed6e9c38ece8956172605470fd1d13685a6b03a376c2566076, 14ddc4e3184c6212e656b267f8a600bb0aac606d6c48d1e0854d6a3f6ce867fd,

Attack Name	TYPE	VALUE
Monero cryptominer	SHA256	0b9cdd16c45db58d1e69804953d38b1ed6b063989d2c125054f3a94b0f79f591, a1dea403ba55e900419ef7cd355253b4e9d08005cf44918a8993df844b616e10, c0eda3d6d769d945595e6d4fa2b68e3186fa66b662d4feb42173026c438626a0, 745a736dd76e415ab9e42688f9d4d21616ce182451f0afa760156b76f07194f9, 73d68aed6e9a5789938b86c450e50dc5151dbec0bc7c272f57d58229bfd9b4a9, 90898ba98f396d9fcb621b7c1ff58e12f00c05e6caf026d9855ebc507666f203
Phemedrone Stealer	SHA256	f32964087462ba3c96a87ee8387f89de8fa605f2f5bb84cb5f754cd736683f2d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424, 815b2125d6f0a5d99750614731aaad2c6936a1dc107a969408a88973f35064c0, ccd19ef6e81e936fc944ebafaefd2ad99ccd11dd15fbc7d3460726bb38237595, ea9b0dee3b7583ce60bba277e2189acb660284abf6b3b9273b6a60c85b0a5ce3, 9a96406ae06b703d827fffd1f1ced0781f89ca2af6d5041721e9fbd2647c8430, 22236e50b5f700f5606788dcd5ab1fb69ee092e8dffdd783ac3cab47f1f445ab, 1433efd142007ce809aff5b057810f5a1919ea1e3ff740ff0fcc2fc729226be5, ad513d2cba6cc82a50ee6531b275e937480d8fee20af2b4f41da5f88e408a4e9, 7c0a1e11610805bd187ef6e395c8fa31c1ae756962e26cdbff704ce54b9e678a, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c9743e7ffb6f6978f08f86e970ddb82e24920d266b32bd242254fbf51abfe6ce,

Attack Name	TYPE	VALUE
Phemedrone Stealer	SHA256	c3bfaa1f52abdbb673d83af67090112dfdfe9ea8ff7a613f62bd48bace205f75, 6bd8449de1e1bdd62a86284ed17266949654f758e00e10d8cd59ec4d233c32e5, 4446d5b475ce8aed5244da917ae42b6cb9744ffc4efd766af8e4dee7dd5a3e19, 70c23213096457df852b66443d9a632e66816e023fdf05a93b9087ffb753d916, 69941417f26c207f7cbbbe36ce8b4d976640a3d7f407d316932428e427f1980b, e2d19a23b19a07d35d16990e78c5cfaa3dd97b9ce92201f4db18a7da95fe6ff8, b7f53c507a1aa4254b66a883285e27b42d65ea4ea4206fe674e0d03738f52141, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, f24a8b3144e89b9bececfbf76add87ddefbd19a024a85692026e97f3a9911902, e64b185c149cb523d13cb46ea3911e2c0595b6f10ae86e6a14b15e8d45c0cdcb, cb58bf466675be9e11cfb404503cb122514f47b9708d033e381f28a60535812c, 80f88566fda41ebc1b4e35d89748a804740bba0d03049c33c536cffd5e0491e2, 4a36cc607ca5c2acc536510fd1b0ddd43a9403dac168d2420d474611909ed9e6, 89caa1568fcff162086dae91e6bd34fd04facba50166ebff800d45a999d0be8b, 188c72f995ebd5e1e8d0e3b9d34eeeec2ec95d4d0fee30d2ea0f317ab1596eef, e326c1b9e61cca6823300158e55381c6951b09d2327a89a8d841539cad3b4df3, 4da33c7fe62f71962913d7b40ff76aff9f1586e57db707b3d6b88162c051f402, ff44e502bd5ea36e17b3fc39b480e65971b36002f27fb441e4acadd6bf604a20, b7980f64f892d70b1cd72a8c80f8319f50c3c410aba4e4bc63fd6494bcb4f313, 480fae3bdc2604cba846779dd7dced95b3ce036bdef629ded247771a2e4d5d58, 348aea633c99e5f6a0ac7b850961be0a145a35678e5bd074b4852f7a2419f518,

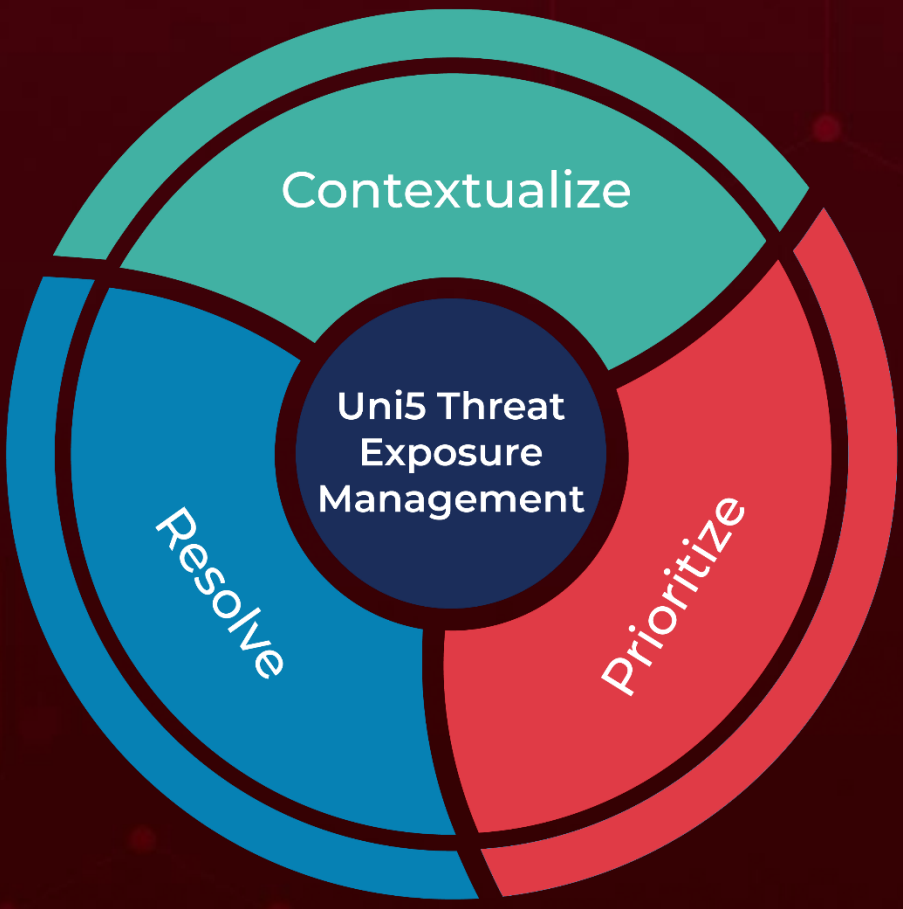
Attack Name	TYPE	VALUE
Phemedrone Stealer	SHA256	1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415, b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53, f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, 8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d, 9b9ba722b314febfc44919551a03dde1539f115333183c2cb5e74b8e644ba5b3, 568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322563, 5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211, d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e364d437a454b, 5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326, 40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc6d266, 3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871
Androxgh0st	SHA256	0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef, 23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066, 59e90be75e51c86b4b9b69dcede2cf815da5a79f7e05cac27c95ec35294151f4, 6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc, bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7, ca45a14d0e88e4aa408a6ac2ee3012bf9994b16b74e3c66b588c7eabaaec4d72, dcf8f640dd7cc27d2399cce96b1cf4b75e3b9f2dfdf19cee0a170e5a6d2ce6b6, de1114a09cbab5ae9c1011ddd11719f15087cc29c8303da2e71d861b0594a1ba

Attack Name	TYPE	VALUE
Androxgh0st	SHA1	06641b9b3b5088c48c7660ad3bf160bc87a929fd, 7d1beb03c32db43f5edd4c28f3c905954e40dbd6, 59ce7486745b08d1adba49f2413133c441194986, 79d3143a47dc02768ff5fda8dbcf464c5cdf115b, 09bd9b17a64b20ba66582dbc3ce08169697177a8
	MD5	95f745a5db131b1ca34e44848fd52edb, 3fae93618edffe4331d18d8b8e6df693, c1070aca9fcff4a32934e6c8aee4ea48, 9039ae16e5aaa63d9ffe88dfaf0f5108, fe53c38f61588efd90af97185e315612, 62a06bea8c6e276b5e532944cfc863e5, 6e793efe40e355643423f53de43952d3, 1fb78440dc44b0900b27260a16d9771e
MediaPl backdoor	SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f
SPICA backdoor	SHA256	84523ddad722e205e2d52eedfb682026928b63f919a7bf1ce6f1ad4180d0f507, 37c52481711631a5c73a6341bd8bea302ad57f02199db7624b580058547fb5a9, C97acea1a6ef59d58a498f1e1f0e0648d6979c4325de3ee726038df1fc2e831d

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

January 22, 2024 • 4:30 AM

More at www.hivepro.com