

Date of Publication
February 5, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 JANUARY to 04 FEBRUARY 2024

Table Of Contents

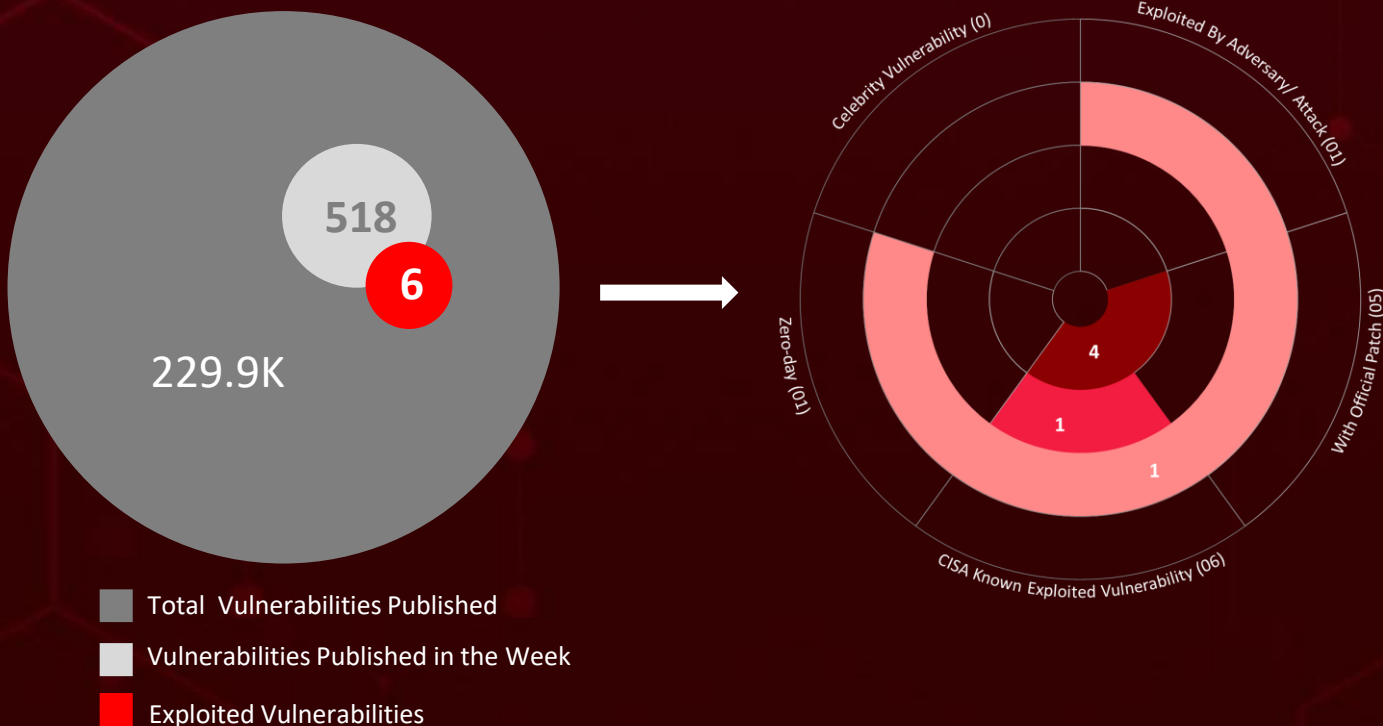
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	23

Summary

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

Furthermore, HiveForce Labs uncovered Financial gain group **UNC4990**, targeting organizations in Italy by utilizing weaponized USB drives as an initial infection vector and deploying malwares EMPTYSpace and QUIETBOARD

Meanwhile, a critical zero-day vulnerability (**CVE-2024-21893**), in Ivanti that enables remote attackers to conduct SSRF attacks by exploiting insufficient validation of user-provided information in the SAML component. Ivanti anticipates a significant surge in exploitation of the flaw in coming days.



High Level Statistics

7

Attacks
Executed

6

Vulnerabilities
Exploited

2

Adversaries in
Action

- [AllaKore RAT](#)
- [FAUST ransomware](#)
- [PlugX](#)
- [Gh0st RAT](#)
- [CherryLoader](#)
- [EMPTYSPACE](#)
- [QUIETBOARD](#)

- [CVE-2024-23897](#)
- [CVE-2024-23898](#)
- [CVE-2024-23899](#)
- [CVE-2024-23905](#)
- [CVE-2024-23904](#)
- [CVE-2024-21893](#)

- [Midnight Blizzard](#)
- [UNC4990](#)



Insights

CVE-2024-23897

a critical vulnerability in Jenkins allows attackers to read system files and potentially enable code execution

FAUST ransomware

a variant of the Phobos family, launches fileless attacks through an Office document with a VBA script

CVE-2024-21893

zero-day flaw in Ivanti enables unauthenticated attackers to access restricted resources

Midnight Blizzard

exploited a legacy test OAuth application with elevated access due to a common password and lack of MFA, to move laterally

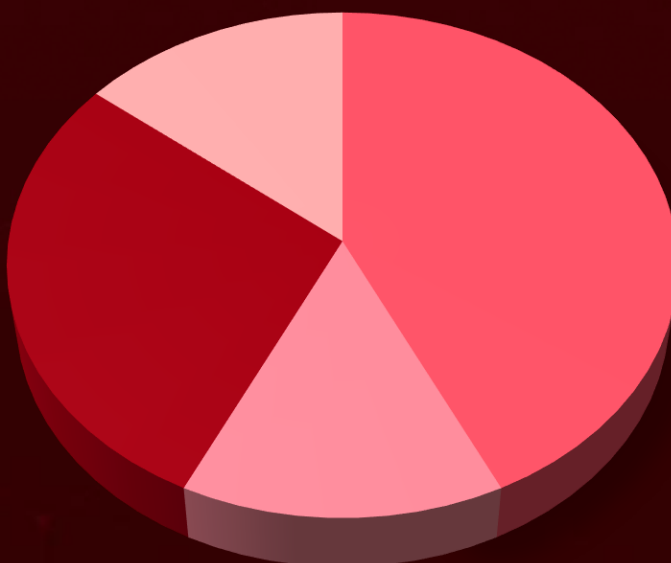
UNC4990

a financially motivated threat actor, has been observed targeting organizations in Italy by utilizing weaponized USB drives as an initial infection vector

CherryLoader

a new Go-based downloader, surfaced in cyber attacks, masquerading as the legitimate CherryTree note-taking app

Threat Distribution



■ RAT ■ Ransomware ■ Downloader ■ Backdoor

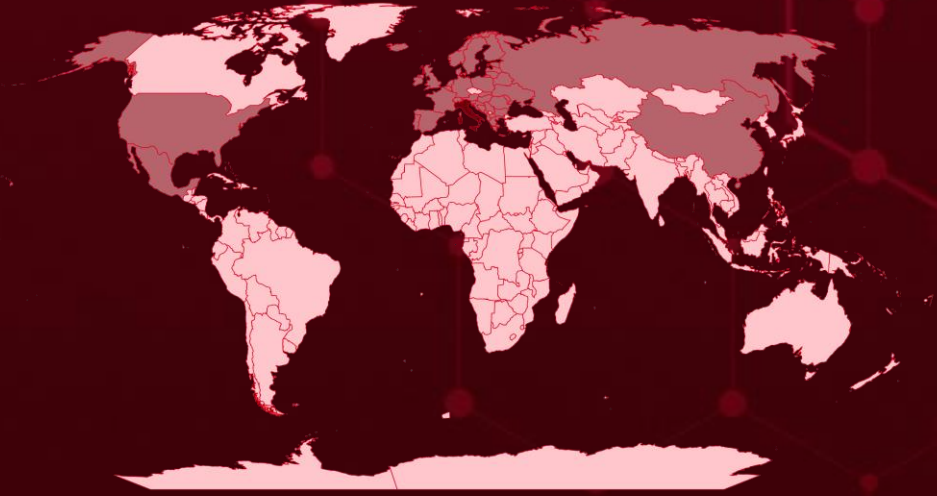


Targeted Countries

Most



Least



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

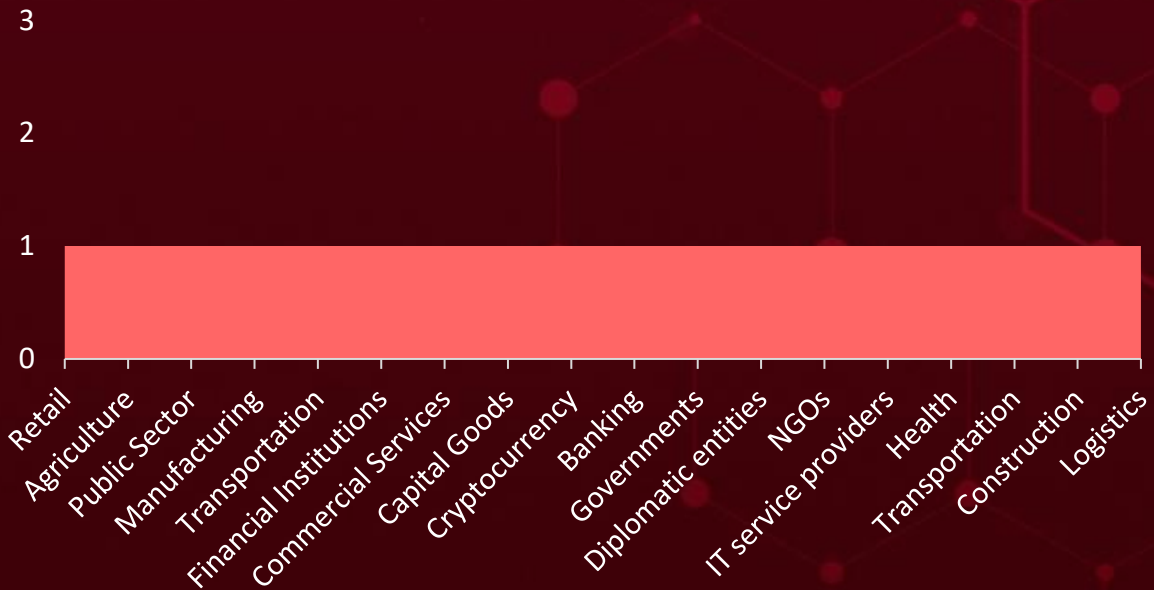
Countries
Italy
Norway
Luxembourg
Slovenia
Andorra
Monaco
Austria
Russia
Belarus
Albania
Belgium
Mexico
Bosnia and Herzegovina
Netherlands
Bulgaria
Portugal
China
Serbia
Croatia
Sweden
Czech Republic (Czechia)

Countries
Denmark
Malta
Estonia
Moldova
Finland
Montenegro
France
North Macedonia
Germany
Poland
Greece
Romania
Holy See
San Marino
Hungary
Slovakia
Iceland
Spain
Ireland
Switzerland
Ukraine
United Kingdom

Countries
Latvia
Timor-Leste
Colombia
Nigeria
Dominican Republic
Somalia
DR Congo
Myanmar
Ecuador
Papua New Guinea
Egypt
Senegal
El Salvador
Sudan
Equatorial Guinea
Uganda
Eritrea
Cameroon
Bahrain
Oman
Eswatini

Countries
India
Tonga
Indonesia
Turkmenistan
Iran
United Arab Emirates
Iraq
Dominica
Bolivia
Namibia
Israel
Nepal
Argentina
New Zealand
Jamaica
Niger
Japan
North Korea
Jordan
Central African Republic
Kazakhstan

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1059.001

PowerShell

T1588.006

Vulnerabilities

T1204

User Execution

T1588

Obtain Capabilities

T1204.002

Malicious File

T1082

System Information Discovery

T1218.007

Msiexec

T1105

Ingress Tool Transfer

T1204.001

Malicious Link

T1574

Hijack Execution Flow

T1218

System Binary Proxy Execution

T1068

Exploitation for Privilege Escalation

T1566

Phishing

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1113

Screen Capture

T1140

Deobfuscate/Decode Files or Information

T1070.004

File Deletion

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AllaKore RAT</u>	AllaKore RAT is typically distributed through phishing emails containing malicious attachments. Once opened, the attachment downloads and installs the malware on the system. The malware is used in targeted attacks against Mexican businesses.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	-
RAT			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	13d88bcf312896fae6d03d59c564bc9521e0916096098cfe41508395955aab0e, 168ac972b7f0610f978e50b426e39938f889422b1bcfaf9cddf518e3e1ed9aa9, 2ff3cdb886b1caf3eaad9a2467bfa16b9269b88695b76bb6a0da481458e30aa3, 305cde85573131949fab5a3973525a886962c4f8c02558d3a215689a49f53406, 33578228c11ad0b3d86a198a32b602aa93a91d2feeae2fb2e83f8c6595c8acd9		

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
FAUST ransomware	FAUST ransomware, a variant of the Phobos family, exhibiting intricate deployment stages, from decoding Base64 data to injecting shellcode. Notably, it employs a fileless attack through an Office document with a VBA script, emphasizing the need for user caution with document files from untrusted sources.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt Data	-
			PATCH LINK
			-
TYPE	Ransomware		
ASSOCIATED ACTOR	-		
IOC TYPE	VALUE		
SHA256	426284b7dedb929129687303f1bf7e4def607f404c93f7736d17241e43f0ab33, 50e2cb600471fc38c4245d596f92f5444e7e17cd21dd794ba7d547e0f2d9a9d5, a0a59d83fa8631d0b9de2f477350faa89499e96fd5ec07069e30992aaabe913a, ebe77c060f8155e01703cfc898685f548b6da12379e6aefb996dbcaac201587c, c10dc2f6694414b68c10139195d7db2bb655f3afdcc1ac6885ef41ef1f0078df		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX	PlugX is a well-established Remote Access Trojan (RAT) malware family with a history dating back to 2008. It's known for its modularity, allowing attackers to customize it with various functionalities for different purposes.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
			PATCH LINK
			-
TYPE	RAT		
ASSOCIATED ACTOR	-		
IOC TYPE	VALUE		
SHA256	d6a4bc7940f98b926b66fed5d3cb1a444c527d02c906beabd53856022edd4f4a, 7df1864afc8dfee93722735a7512b748e2b1ddd8f0701275fe0c9798fd14400c, 4d0f6cce0e423a96ff3b76a8e41bca9e3bb97ff0f78d57fe45494b97415c2dfe, e42ba4c493d6841f24667db5c1c6ad9a0107833e5a27d930e2ce454d6194b9d0, 0b81b33d24ad693be288a9a14a091210b90c8d8ba20b9b205c52e66b50728050		

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>Gh0st RAT</u>	Gh0st RAT allows attackers to remotely control and spy on infected devices. It has been used in various cyberattacks, including those targeting sensitive computer networks. It possesses features like keylogging, screenshot capture, webcam and microphone access, file manipulation, and remote control capabilities.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
			PATCH LINK
			-
TYPE			
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	954337ceb86b9aec6dcd3a09ec713161281c8ac78dbc8c68ee94747e89dcff3f, 4adb1fb761af827cea1bc674dd08b572ac5af7bc8d441e022d557430b167cb67, 21c3b30041dc16f6fb0fe758c4cd1767e272133ff45dd21aee22506e6d9199aa, 83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>CherryLoader</u>	CherryLoader, a new Go-based downloader, has surfaced in cyber attacks, masquerading as the legitimate CherryTree note-taking app. This sophisticated threat infiltrates compromised hosts, delivering malicious payloads such as privilege escalation tools for exploitation and persistent control.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Deploy malware	-
			PATCH LINK
			-
TYPE			
Downloader			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	8c42321dd19bf4c8d2ef11885664e79b0064194e3222d73f00f4a1d67672f7fc		




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>EMPTYSPACE (aka VETTA Loader and BrokerLoader)</u>	EMPTYSPACE is a downloader that can execute any payload served by the command and control (C2) server, and deliver backdoor.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Deploy Backdoor	-
			PATCH LINK
			-
TYPE			
Downloader			
ASSOCIATED ACTOR			
UNC4990			
IOC TYPE	VALUE		
SHA256	a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40, 8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d, 060882f97ace7cb6238e714fd48b3448939699e9f085418af351c42b401a1227, 8c25b73245ada24d2002936ea0f3bcc296fdcc9071770d81800a2e76bfca3617, b9ffba378d4165f003f41a619692a8898aed2e819347b25994f7a5e771045217		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>QUIETBOARD</u>	QUIETBOARD is a Python-based pre-compiled multi-component backdoor. It includes the ability to execute arbitrary commands, manipulate clipboard content for cryptocurrency theft, infect USB or removable drives, capture screenshots, gather system information, and communicate with a C2 server.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		System Compromise	-
			PATCH LINK
			-
TYPE			
Backdoor			
ASSOCIATED ACTOR			
UNC4990			
IOC TYPE	VALUE		
SHA256	15d977dae1726c2944b0b4965980a92d8e8616da20e4d47d74120073cbc701b3, 26d93501cb9d85b34f2e14d7d2f3c94501f0aaa518fed97ce2e8d9347990decf, 26e943db620c024b5e87462c147514c990f380a4861d3025cf8fc1d80a74059a, 71c9ce52da89c32ee018722683c3ffbc90e4a44c5fba2bd674d28b573fba1fdc, 539a79f716cf359dceaa290398bc629010b6e02e47eae2356074bffa072052f		




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-2024-23897		Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*	-
Jenkins Arbitrary File Read Vulnerability			
	CWE ID		
	CWE-284	T1588.006: Vulnerabilities T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23898		Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*	-
Jenkins Cross-site WebSocket Hijacking Vulnerability			
	CWE ID		
	CWE-1385	T1059: Command and Scripting Interpreter	https://www.jenkins.io/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23899		Git server version 99.va_0826a_b_cdafa_d	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:Gitserver :*:*:*:*:*:*	-
Jenkins Git Server File Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1588.006: Vulnerabilities	https://www.jenkins.io/download/


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23905		Red Hat Dependency Analytics version 0.7.1 and prior versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:RedHat_Dependency_Analytics:*:*:*:*:*	-
Jenkins Red Hat Dependency Analytics Plugin Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1588.006: Vulnerabilities	https://www.jenkins.io/download/


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23904		Log Command versions 1.0.2 and prior versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jenkins:Log_Command:*.:*:*:*:*:*	-
Jenkins Log Command File Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1588.006: Vulnerabilities	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21893		Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*.:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*.:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1588.006: Vulnerabilities	https://forums.ivanti.com/s/product-downloads/



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Midnight Blizzard (aka APT 29, 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)</u></p>	Russia	Governments, Diplomatic entities, Non-Governmental Organizations (NGOs) and IT service providers	US and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
-	-	-	
TTPs			
TA0001: Initial Access; TA0006: Credential Access; TA0042: Resource Development; TA0005: Defense Evasion; T1110.003: Password Spraying; T1110: Brute Force; T1027: Obfuscated Files or Information; T1586: Compromise Accounts; T1190: Exploit Public-Facing Application; T1583: Acquire Infrastructure; T1583.006: Web Services; T1586.002: Email Accounts			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>UNC4990</u>	Unknown	Health, Transportation, Construction, and logistics	Italy
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	EMPTYSPACE, QUIETBOARD	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1071: Application Layer Protocol; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1566: Phishing; T1113: Screen Capture; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1614: System Location Discovery			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actor **Midnight Blizzard, UNC4990** and malware **AllaKore RAT, FAUST ransomware, PlugX, Gh0st RAT, CherryLoader, EMPTYSPACE, QUIETBOARD**.

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 **six exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Midnight Blizzard, UNC4990** and malware **AllaKore RAT, FAUST ransomware, PlugX, Gh0st RAT, CherryLoader, EMPTYSPACE** in Breach and Attack Simulation(BAS).



Threat Advisories

[AllaKore RAT's Grip Tightens on Mexican Financial Institutions](#)

[Midnight Blizzard Exploiting Legacy OAuth for Lateral Movement](#)

[FAUST: A Phobos Ransomware Variant Launches Fileless Attack](#)

[Malicious Google Ads Target Chinese Users, Covertly Delivering RATs](#)

[CherryTree Impostor Dubbed CherryLoader Makes Its Move](#)

[Critical Remote Code Execution Flaws Uncovered in Jenkins](#)

[UNC4990 Leverage Hosting Platforms in USB Infection Chain](#)

[Ivanti Addresses Zero-Day Vulnerability Exploited in Attacks](#)

[Leaky Vessels in Cloud Environments Shake Docker 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
<u>AllaKore RAT</u>	SHA256	13d88bcf312896fae6d03d59c564bc9521e0916096098cfe41508395955aab0e, 168ac972b7f0610f978e50b426e39938f889422b1bcfaf9cddf518e3e1ed9aa9, 2ff3cdb886b1caf3eaad9a2467bfa16b9269b88695b76bb6a0da481458e30aa3, 305cde85573131949fab5a3973525a886962c4f8c02558d3a215689a49f53406, 33578228c11ad0b3d86a198a32b602aa93a91d2feeae2fb2e83f8c6595c8acd9, 422c9471c29fe17457e142df1a567c273212019eb20b0b4783891c529c1248a8, 46c14c2f0d04710f53db16473877d3315c13e1a33a3236846a87e8f91808c8eb, 49a04f31e49cee3ae65e9d776bc0f8aedf40c52fafcd002ccf7de4044abec2dd, 52134d02cd77f8a65fd5b15c7c57ff2909ac39f0b5779592c533a18bf6b23879, 5961b42f8efad58c437bdad862a0337c6bcd57f7cbf35184f2de60f4609fd477, 673d4fe6f9e46fae37649c525f1d0d89cfd3b8310210dff4ddc7349418d9e80f, 6d516a96d6aa39dd9fc2d745ea39658c52ab56d62ef7a56276e2e050d916e19f,

Attack Name	TYPE	VALUE
AllaKore RAT	SHA256	89206ca169747d4aa70d49350415f21df7f1a00a3bf8d0c253b6beda2eb919d9, 8fce1d24cf952528169f473b9462724482511615ed31165710e5e3a74cefdd02, 911e45d053bdf3a41e812203ae29db739cf3505a4e37209936c1cc83ee42e8e9, 9221470c77b46bcd457951ae3a3d31d60ad4602ea9d152d51d1e4f9a5b3bca3a, a5af60355c423fa4cc9695b86a5697f847259eae724065162d303cc4523d447, b858d451804a641fc51dd6d3c50668d6a08dc9033252aee52f582264a970cff8, bc423bd9acd7c5a1f2849091f21de5429f2fc79e2655f92866e1c8b7b1f96f7e, c778739c5214aa580cba05f01afe2d9fc8f12d3fa7ad864a279bcb4ad6d266b4, cde045a0269a5a05928128c6ca7c030947f96034c9204e2b747a0d626e3f22f3, e2d82ab6cc71a1d8d2a2ba2312b0d8a4a3d23e3902d5b180383d9e406097a9ff, ee772e1260c6adc532bed57cacdbb6e0b8db311996074ad42eaf1aefd243187a, eecc201c80809b636d945aa537b954dd2e39382c36067a040a672167a1257a09, fba031543c3ab694a09e603a7df6417f93742f0b87f9fedaf9ab84d11340ccb5, fd8c49d00effa8bc730e06ae217655a430ba03122ca974945d41642299853dfa
FAUST ransomware	SHA256	426284b7dedb929129687303f1bf7e4def607f404c93f7736d17241e43f0ab33, 50e2cb600471fc38c4245d596f92f5444e7e17cd21dd794ba7d547e0f2d9a9d5, a0a59d83fa8631d0b9de2f477350faa89499e96fd5ec07069e30992aaabe913a, ebe77c060f8155e01703cfc898685f548b6da12379e6aefb996dbcaac201587c, c10dc2f6694414b68c10139195d7db2bb655f3afdcc1ac6885ef41ef1f0078df
PlugX	SHA256	d6a4bc7940f98b926b66fed5d3cb1a444c527d02c906beabd53856022edd4f4a, 7df1864afc8dfef93722735a7512b748e2b1ddd8f0701275fe0c9798fd14400c, 4d0f6cce0e423a96ff3b76a8e41bca9e3bb97ff0f78d57fe45494b97415c2dfe,

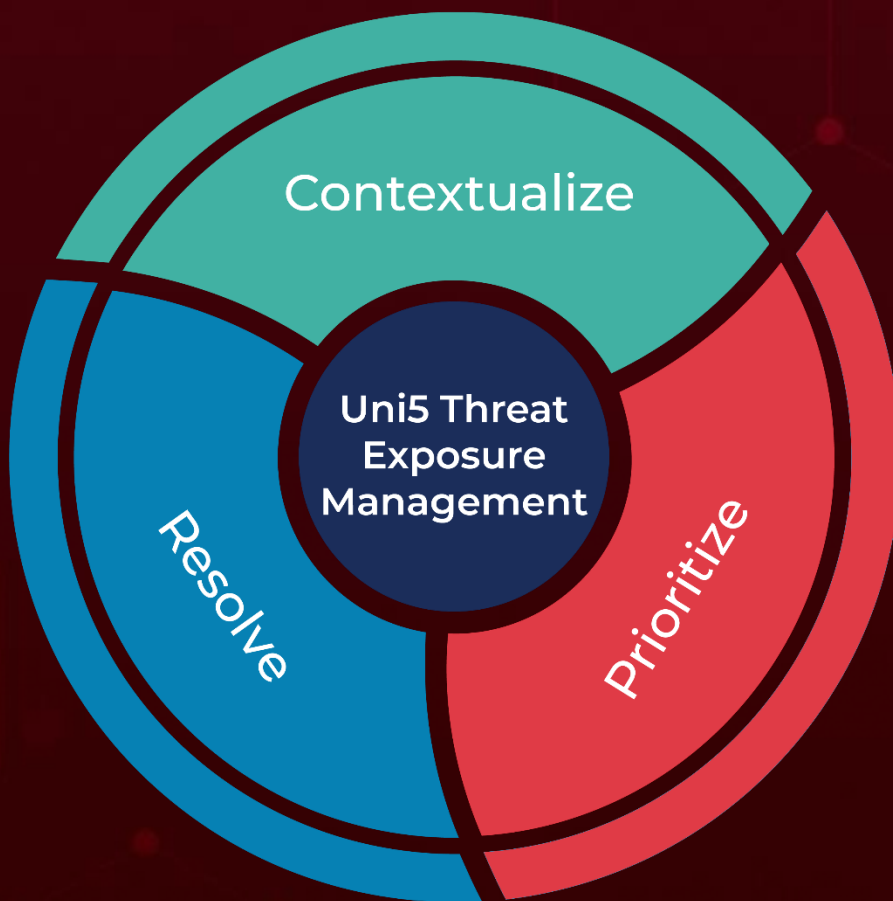
Attack Name	TYPE	VALUE
<u>PlugX</u>	SHA256	e42ba4c493d6841f24667db5c1c6ad9a0107833e5a27d930e2ce454d6194b9d0, 0b81b33d24ad693be288a9a14a091210b90c8d8ba20b9b205c52e66b50728050, c79550db4bc421bc8d5ed5db6dc9f608724f6934a41f5501333bde78f731ecb2, a54b3c1cfd65f351c9eb28cb293d338598267a8923c7f447a7e4244eb374238a, 9da62b3d6805d77c13cc58bbcbfcbce51cb1b95b956654082fdf26828756b7e00, c0545f119cea422f092a3c358a3ce4888d212ccb7531bf161c8f4fa46d97a587, ee82542d12b1620add9191bb3dbd947192ee900cb9f3d16dc36b346e76361fe5, 149b86e1877fa6f7600c4154be07b2fc90b9ee30e988d8f2f67130069d6fd80e, a281d5e93518d3a0e6e83f2874297389aec4d42ece26b358623e902cd1959189, bf0bfd017bdce9ba2359784a42c4ce7ee3e1a6ce47716e0b31c40be8c61e18a, 405bac66c665f2ffe99811b1b73716d663e91f93a9dd469eb361df63da4c1ee3, 9c4c4c770a018612b780162bd046fd713e6347a72a5176ed0ee3e51b11823534, d8d59353d0e19957cd4cce5102dff5b706ed9c412db6b8778b3ea4726b2429b3, 72120bf8bf604bc1f1aa455b22d3df431cc95836306fab186cd64da53527a274, 503e7059334032bfa50ba878f0992a3b909952d380fc9757949c43109973ede7, 2dc28b596c37dac4771a628ae5c67de9e77f528e309b0972f4360cadc3171680, 096ab2d8480196d6e16de70d9698f2cf9e1c0eff906e5e3bbd13dd2251c858f1, 0af8058a65750350c95ac26df850a9a2505d2098414f54bfa1a289cd93f746f5, dbf692a521ff5c28e2ca25afa0b37bdcec77177a7ba8f27086708b4806a670e4, 4ed7053705a49a742ed3034da2fc834d9790e63d10c4162175dcb9f6b7715451
<u>CherryLoader</u>	SHA256	8c42321dd19bf4c8d2ef11885664e79b0064194e3222d73f00f4a1d67672f7fc

Attack Name	TYPE	VALUE
<u>Gh0st RAT</u>	SHA256	954337ceb86b9aec6dcd3a09ec713161281c8ac78dbc8c68ee94747e89dcff3f, 4adb1fb761af827cea1bc674dd08b572ac5af7bc8d441e022d557430b167cb67, 21c3b30041dc16f6fb0fe758c4cd1767e272133ff45dd21aee22506e6d9199aa, 83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6
<u>EMPTYSPACE</u>	SHA256	a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40, 8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d, 060882f97ace7cb6238e714fd48b3448939699e9f085418af351c42b401a1227, 8c25b73245ada24d2002936ea0f3bcc296fdcc9071770d81800a2e76bfca3617, b9ffba378d4165f003f41a619692a8898aed2e819347b25994f7a5e771045217, 84674ae8db63036d1178bb42fa5d1b506c96b3b22ce22a261054ef4d021d2c69
<u>QUIETBOARD</u>	SHA256	15d977dae1726c2944b0b4965980a92d8e8616da20e4d47d74120073cbc701b3, 26d93501cb9d85b34f2e14d7d2f3c94501f0aaa518fed97ce2e8d9347990decf, 26e943db620c024b5e87462c147514c990f380a4861d3025cf8fc1d80a74059a, 71c9ce52da89c32ee018722683c3ffbc90e4a44c5fba2bd674d28b573fba1fdc, 539a79f716cf359dceaa290398bc629010b6e02e47eaed2356074bffa072052f

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

February 5, 2024 • 5:45 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com