Date of Publication
December 18, 2023

Hive Pro®

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

11 to 17 DECEMBER 2023

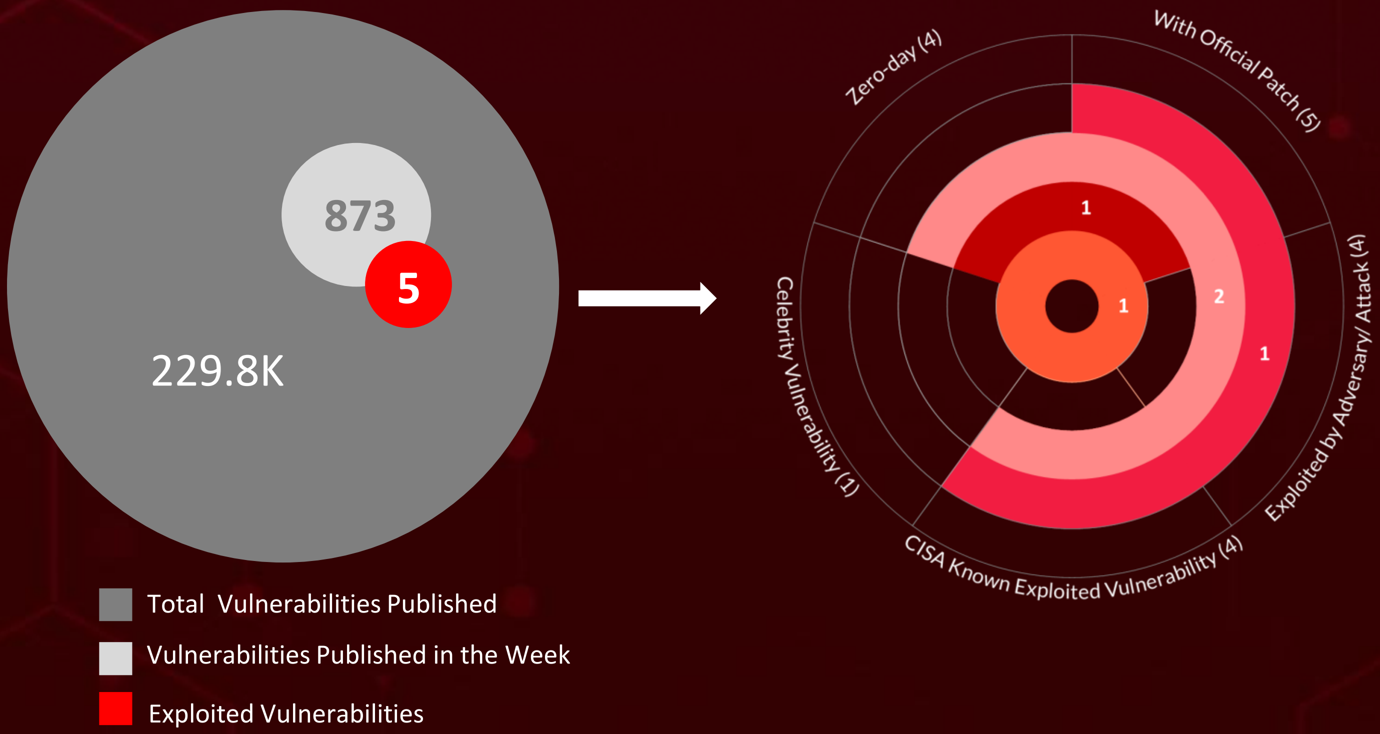
Table Of Contents

Summary

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

Furthermore, HiveForce Labs uncovered **GambleForce**, a newly identified threat actor that utilizes SQL injections in targeted attacks across the Asia-Pacific region to illicitly obtain sensitive information.

Meanwhile, a critical vulnerability (**CVE-2023-42793**) in JetBrains TeamCity Actively Exploited by **APT 29**, Allowing Full Server Compromise. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

11
Attacks Executed

- MrAnon Stealer
- NineRAT
- DLRAT
- BottomLoader
- HazyLoad
- LuaDream
- KEYPLUG
- Editbot Stealer
- More_Eggs
- GraphicalProton
- Rhadamanthys stealer

5
Vulnerabilities Exploited

- CVE-2021-44228
- CVE-2023-42916
- CVE-2023-42917
- CVE-2023-20588
- CVE-2023-42793

6
Adversaries in Action

- Lazarus Group
- GambleForce
- Sandman
- Storm-0866
- TA4557
- APT 29

Insights

Apple Zero-Day

Apple fixes actively exploited WebKit vulnerabilities (CVE-2023-42916 and CVE-2023-42917)

Lazarus Group

Exploiting **Log4j** vulnerability and introducing the NineRAT, DLRAT, and BottomLoader malware to gain control over their victims in latest campaign named “**Operation Blacksmith**"

Editbot Stealer

A new malicious campaign employs WinRAR archives for a multi-stage attack

APT 29

Exploits Critical Vulnerability (CVE-2023-45247) in JetBrains TeamCity, Posing Substantial Risk to Developer Environments

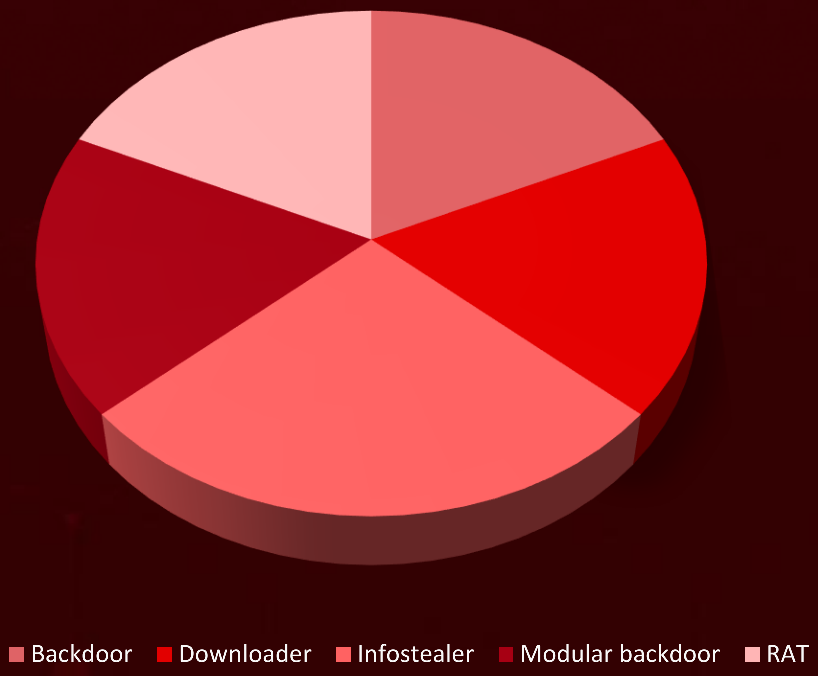
Sandman APT

linked to China's Storm-0866 (Red Dev 40), deploys LuaDream and KEYPLUG concurrently within victim environments

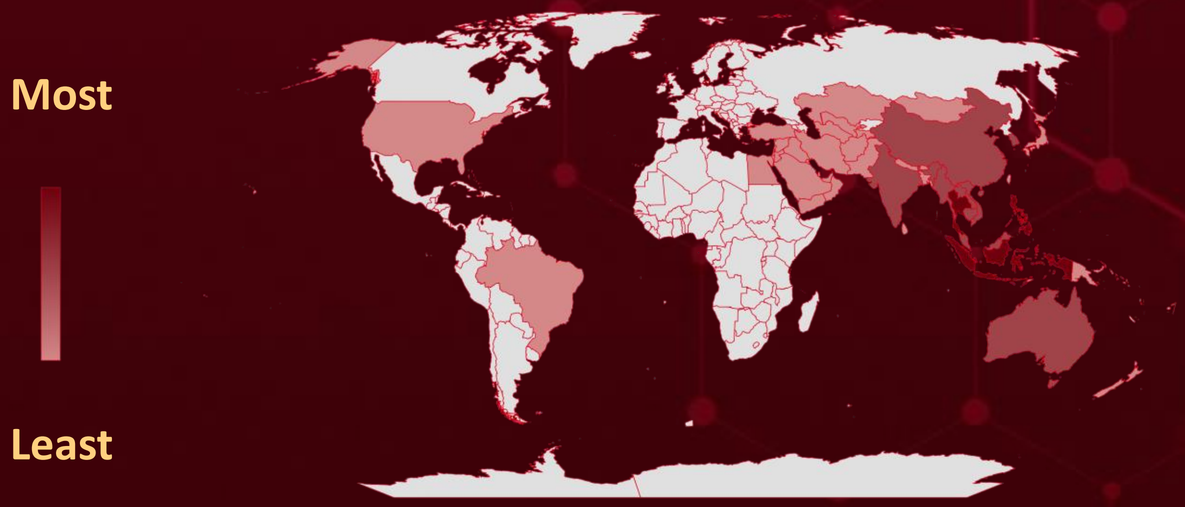
MrAnon Stealer

A phishing campaign uses fake booking details to trick victims, aiming to deploy the Python-based information stealer

Threat Distribution



Targeted Countries



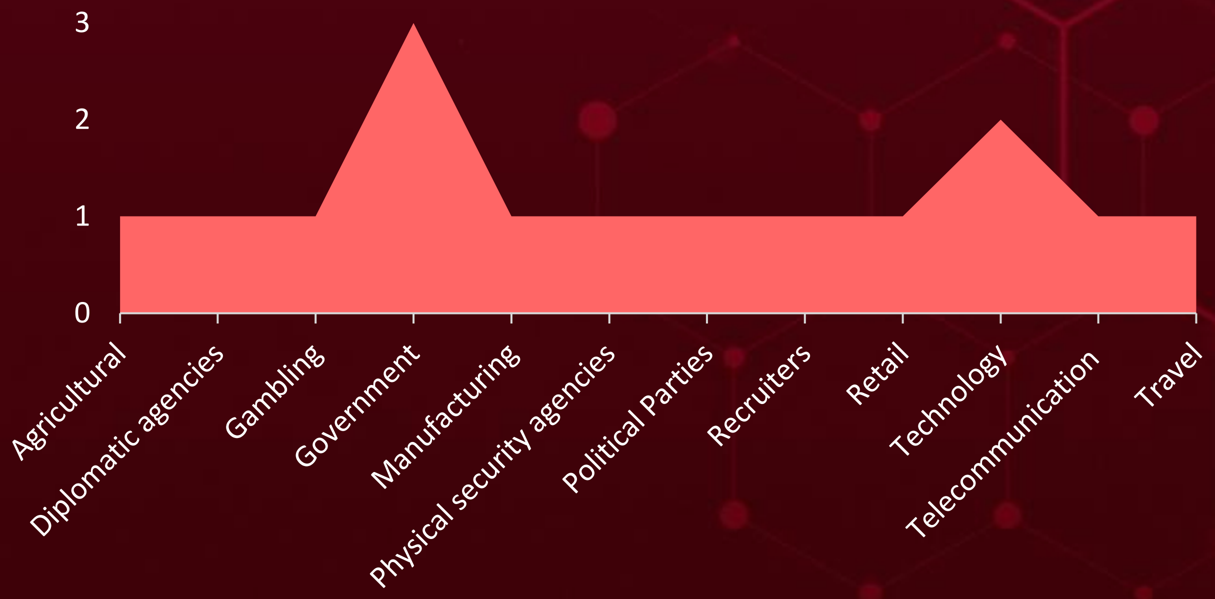
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

	Countries
█	Thailand
█	Philippines
█	Indonesia
▓	Brunei
▓	Vietnam
▓	South Korea
▓	China
▓	Myanmar
▓	India
▓	Singapore
▓	Australia
▓	Cambodia
▓	Laos
▓	Malaysia
░	Turkey
░	Egypt
░	Papua New Guinea
░	Iran
░	Taiwan
░	Iraq
░	Vanuatu
░	Israel

	Countries
░	Japan
░	Sri Lanka
░	Jordan
░	Brazil
░	Kazakhstan
░	United Arab Emirates
░	Kuwait
░	Palestine
░	Bangladesh
░	East Timor
░	Lebanon
░	Saudi Arabia
░	Bhutan
░	Fiji
░	United States
░	Syria
░	Mongolia
░	Tajikistan
░	Cyprus
░	Maldives

	Countries
░	Timor-Leste
░	Nepal
░	Turkmenistan
░	New Zealand
░	Uzbekistan
░	Oman
░	Bahrain
░	Pakistan
░	Afghanistan
░	Qatar
░	Yemen

Targeted Industries



TOP MITRE ATT&CK TTPS

T1566
Phishing

T1059
Command and Scripting Interpreter

T1036
Masquerading

T1105
Ingress Tool Transfer

T1204.002
Malicious File

T1204
User Execution

T1041
Exfiltration Over C2 Channel

T1083
File and Directory Discovery

T1543
Create or Modify System Process

T1027
Obfuscated Files or Information

T1071.001
Web Protocols

T1071
Application Layer Protocol

T1053
Scheduled Task/Job

T1574
Hijack Execution Flow

T1190
Exploit Public-Facing Application

T1059.001
PowerShell

T1056
Input Capture

T1005
Data from Local System

T1547.001
Registry Run Keys / Startup Folder

T1082
System Information Discovery

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">MrAnon Stealer</td><td rowspan="6">MrAnon Stealer is a infostealer malware currently being used in phishing malicious campaigns. This malicious software is designed to pilfer victims' credentials, system details, browser sessions, and cryptocurrency extensions.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data Theft</td><td rowspan="2">-</td></tr>
<tr><td>Infostealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</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">075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0,
48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9,
0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312,
8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7,
96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">NineRAT</td><td rowspan="6">NineRAT, part of Lazarus Group's Operation Blacksmith, is a D programming language-based remote access trojan. It steals sensitive information, including credentials, system data, and browser sessions.</td><td>Exploiting vulnerability</td><td>CVE-2021-44228</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data Theft</td><td rowspan="2">Apache Log4j2</td></tr>
<tr><td>RAT</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Lazarus Group</td><td>https://logging.apache.org/log4j/2.x/security.html</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433,
ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4,
47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30,
f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59,
5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541</td></tr>
</table>

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">DLRAT</td><td rowspan="6">DLRAT is a Remote Access Trojan (RAT), written in the D programming language. Linked to the Lazarus Group, it executes commands for extensive system reconnaissance upon activation.</td><td>Exploiting vulnerability</td><td>CVE-2021-44228</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data Theft</td><td rowspan="2">Apache Log4j2</td></tr>
<tr><td>RAT</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Lazarus Group</td><td>https://logging.apache.org/log4j/2.x/security.html</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f,
9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">BottomLoader</td><td rowspan="6">BottomLoader is a DLang-based malware downloader that acts as the initial stage of a cyber attack. Its primary function is to fetch and execute additional malicious payloads.</td><td>Exploiting vulnerability</td><td>CVE-2021-44228</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data theft</td><td rowspan="2">Apache Log4j2</td></tr>
<tr><td>Downloader</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Lazarus Group</td><td>https://logging.apache.org/log4j/2.x/security.html</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA256</td><td colspan="3">0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f</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
HazyLoad	HazyLoad is a specialized proxy tool identified in the Lazarus Group's Operation Blacksmith campaign. Its primary function is to create a lasting connection between the compromised host and infrastructure controlled by the attackers.	Exploiting vulnerability	CVE-2021-44228
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	Apache Log4j2
Downloader			**PATCH LINK**
ASSOCIATED ACTOR			https://logging.apache.org/log4j/2.x/security.html
Lazarus Group			

IOC TYPE	VALUE
SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LuaDream	LuaDream is a newly emerged backdoor malware with global reach. Functioning as an info-stealing malware, it has the capability to extract sensitive data, including credentials, system information, and user data, using various protocols.	DLL hijacking	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	-
Modular backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Sandman and Storm-0866			

IOC TYPE	VALUE
SHA1	fc8fdf58cd945619cbfede40ba06aada10de9459
Domains	mode.encagil[.]com, ssl.explorecell[.]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
KEYPLUG	KEYPLUG is a modular backdoor malware written in C++. It has the capability to steal sensitive data, assume control of a computer, and execute various other attacks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Sandman and Storm-0866			-

IOC TYPE	VALUE
IPv4	172.67.216[.]63, 185.38.142[.]129, 37.120.140[.]205, 45.129.199[.]122, 45.90.59[.]17

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Editbot Stealer	Editbot Stealer is a malware that targets compromised networks, operated through a central command and control server. It specializes in stealing sensitive information such as browsing history, internet cookies, and login credentials.	Unknown	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	-
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	3f7bd47fbbf1fb0a63ba955c8f9139d6500b6737e5baf5fdb783f0cedae94d6d
SHA1	eed59a282588778ffbc772085b03d229a5d99e35
MD5	669e7ac187fb57c4d90b07d9a6bb1d42

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>More_Eggs</td><td rowspan="5">More_Eggs is a JScript backdoor employed by the TA4557. It possesses the capability to collect data on installed anti-malware programs, assess the existence of various antivirus tools, and download as well as execute additional payloads.</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">Data Theft</td><td>-</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>TA4557</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>-</td><td colspan="3">-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">GraphicalProton</td><td rowspan="6">GraphicalProton, linked to APT29, is a backdoor (also known as BlueBravo) utilized in campaigns involving TeamCity exploitation. The malware acts as a loader, communicating through OneDrive or Dropbox.</td><td>Phishing</td><td>CVE-2023-42793</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data Theft, Lateral movement</td><td rowspan="2">TeamCity</td></tr>
<tr><td>Backdoor</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>APT29</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">01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd,
01b5f7094de0b2c6f8e28aa9a2ded678c166d615530e595621e692a9c0240732,
0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5,
18101518eae3eec6ebe453de4c4c380160774d7c3ed5c79e1813013ac1bb0b93,
19f1ef66e449cf2a2b0283dbb756850cca396114286e1485e35e6c672c9c3641</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
Rhadamanthys stealer	Rhadamanthys, the information-stealing malware, has taken a significant leap with its v0.5.0 upgrade, introducing expanded stealing features, raw syscalls, and an enhanced loader design, showcasing advanced evasion techniques. Its modular architecture allows for continuous updates, showcasing improved loader design and enhanced spying functionalities.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38

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-2021-44228	LOG4J	Apache Log4j2	Lazarus Group
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	NineRAT, DLRAT, BottomLoader, HazyLoad, LockBit Ransomware
Apache Log4j2 Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917 CWE-20 CWE-400 CWE-502	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42916	✗	iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple WebKit Out-of-Bounds Read Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**

	CWE-125	T1059: Command and Scripting Interpreter	https://support.apple.com/enus/HT214031;
			https://support.apple.com/enus/HT214032;
			https://support.apple.com/en-us/HT214033

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42917	✗	iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple WebKit Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-787	T1059: Command and Scripting Interpreter	https://support.apple.com/enus/HT214031;
			https://support.apple.com/enus/HT214032;
			https://support.apple.com/en-us/HT214033

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20588	✗	Windows Server: 2008 - 2022 23H2 Windows: 10 - 11 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
AMD Speculative Execution information disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-369	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-20588

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42793	✗	JetBrains TeamCity versions prior to 2023.05.4	APT 29
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	GraphicalProton
JetBrains TeamCity Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1082: System Information Discovery	https://www.jetbrains.com/teamcity/download/other.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)	North Korea	Manufacturing, Agricultural and Physical security companies	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-44228	NineRAT, DLRAT, BottomLoader, HazyLoad	Apache Log4j2
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1574: Hijack Execution Flow; T1134: Access Token Manipulation; T1547: Boot or Logon Autostart: Execution; T1102: Web Service; T1082: System Information Discovery; T1003: OS Credential Dumping; T1003.005: Cached Domain Credentials; T1112: Modify Registry; T1518: Software Discovery; T1136: Create Account; T1098: Account Manipulation; T1033: System Owner/User: Discovery; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Sandman	Unknown	Telecommunication providers, and Government entities	The Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LuaDream, KEYPLUG (aka ELFSHELF)	-
TTPs			
TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; T1190: Exploit Public-Facing Application; T1595.002: Vulnerability Scanning; T1584.004: Server; T1543: Create or Modify System Process; T1055: Process Injection; T1570: Lateral Tool Transfer; T1112: Modify Registry; T1588.001: Malware; T1007: System Service Discovery; T1560: Archive Collected Data; T1497: Virtualization/Sandbox Evasion; T1129: Shared Modules			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Storm-0866 (aka Red Dev 40)	China	Telecommunication providers, and Government entities	The Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LuaDream, KEYPLUG (aka ELFSHELF)	-
TTPs			
TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; T1190: Exploit Public-Facing Application; T1595.002: Vulnerability Scanning; T1584.004: Server; T1543: Create or Modify System Process; T1055: Process Injection; T1570: Lateral Tool Transfer; T1112: Modify Registry; T1588.001: Malware; T1007: System Service: Discovery; T1560: Archive Collected Data; T1497: Virtualization/Sandbox Evasion; T1129: Shared Modules			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">TA4557</td><td>Unknown</td><td rowspan="3">Recruiters</td><td rowspan="3">Philippines</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>-</td><td>More_Eggs</td><td>-</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; T1566: Phishing; T1566.001: Spearphishing: Attachment; T1566.002: Spearphishing Link; T1218: System Binary Proxy Execution; T1047: Windows Management Instrumentation; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1497: Virtualization/Sandbox Evasion; T1070: Indicator Removal; T1070.004: File Deletion; T1622: Debugger Evasion; T1220: XSL Script Processing; T1082: System Information Discovery; T1105: Ingress Tool Transfer</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">GambleForce (aka EagleStrike)</td><td>Unknown</td><td rowspan="3">Government, Gambling, Retail, and Travel</td><td rowspan="3">Australia, Brazil, China, India, Indonesia, the Philippines, South Korea, Thailand and APAC region</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>CVE-2023-23752</td><td>-</td><td>Joomla!</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0011: Command and Control; TA0010: Exfiltration; T1595: Active Scanning; T1595.002: Vulnerability: Scanning; T1595.003: Wordlist Scanning; T1592: Gather Victim Host Information; T1592.002: Software; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1190: Exploit Public-Facing Application; T1071: Application Layer Protocol; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT 29 (aka Midnight Blizzard, 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)	Russia	Government, Political, Diplomatic agencies, and Technology	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-42793	GraphicalProton	JetBrains TeamCity versions prior to 2023.05.4
TTPs			
T1003 - OS Credential Dumping; T1020 - Automated Exfiltration; T1027 - Obfuscated Files or Information; T1033 - System Owner/User Discovery; T1036 - Masquerading; T1041 - Exfiltration Over C2 Channel; T1046 - Network Service Scanning; T1047 - Windows Management Instrumentation; T1049 - System Network Connections Discovery; T1053 - Scheduled Task/Job; T1055 - Process Injection; T1057 - Process Discovery; T1059 - Command and Scripting Interpreter; T1068 - Exploitation for Privilege Escalation; T1098 - Account Manipulation; T1190 - Exploit Public-Facing Application; T1203 - Exploitation for Client Execution; T1210 - Exploitation of Remote Services; T1505 - Server Software Component; T1547 - Boot or Logon Autostart Execution; T1555 - Credentials from Password Stores; T1558 - Steal or Forge Kerberos Tickets; T1562 - Impair Defenses; T1564 - Hide Artifacts; T1567 - Exfiltration Over Web Service; T1568 - Dynamic Resolution; T1572 - Protocol Tunneling; T1574 - Hijack Execution Flow; T1590 - Gather Victim Network Information; T1592 - Gather Victim Host Information; T1531 - Account Access Removal; T1140 - Deobfuscate/Decode Files or Information; T1550 - Use Alternate Authentication Material; T1195 - Supply Chain Compromise; T1102 - Web Service			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **Lazarus Group, GambleForce, Sandman, Storm-0866, TA4557, APT 29** and malware **MrAnon Stealer, NineRAT, DLRAT, BottomLoader, HazyLoad, LuaDream, KEYPLUG, Editbot Stealer, GraphicalProton, Rhadamanthys stealer.**

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 vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Lazarus Group, GambleForce, Sandman, Storm-0866, TA4557, APT 29** and malware **MrAnon Stealer, NineRAT, DLRAT, BottomLoader, HazyLoad, LuaDream, KEYPLUG, Editbot Stealer, GraphicalProton, Rhadamanthys stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

Decoding MrAnon Stealer’s Plot through Deceptive Emails

Lazarus's Operation Blacksmith Deploys Novel Dlang RATs

The Unseen Thread Linking Sandman APT and KEYPLUG Backdoor

Adversaries Leverage Social Media to Disseminate New Python-Based Stealer

Apple's Timely Response to Actively Exploited Zero-Days

Microsoft’s December 2023 Patch Tuesday Addresses One Zero-day Vulnerability

Critical Remote Code Execution Flaw Uncovered in Apache Struts 2

TA4557 Targets Recruiters by Delivering Malware Disguised as Job Applicant

Russian SVR Exploits Critical TeamCity Vulnerability Globally

Unveiling GambleForce: A SQL Injection Gang

Rhadamanthys Stealer Version 0.5.0 Upgrade Overview

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.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
MrAnon Stealer	SHA256	29ca95ce3eca818872a7ad47e4fafa3f9582836e0b24c5a6486df76397344521, 075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0, 48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9, 0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312, 8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7, 96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628, 8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0, 45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22
NineRAT	MD5	534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433, ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4, 47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30, f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59, 5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541, 82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def

Attack Name	TYPE	VALUE
DLRAT	SHA256	e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f, 9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a
Bottom Loader	SHA256	0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f
HazyLoad	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
LuaDream	Domains	mode.encagil[.]com, ssl.explorecell[.]com
	SHA1	fc8fdf58cd945619cbfede40ba06aada10de9459
	IPv4	185.82.218[.]230
KEYPLUG	Domains	dan.det-ploshadka[.]com, ssl.e-novauto[.]com, yum.luxyries[.]com
	SHA1	a7932112b7880c95d77bc36c6fcced977f4a5889, b6d759c9ea5d2136bacb1b2289a31c33500c8de8
	IPv4	172.67.216[.]63, 185.38.142[.]129, 37.120.140[.]205, 45.129.199[.]122, 45.90.59[.]17, 5.2.67[.]176, 5.2.72[.]130, 5.255.88[.]188, 79.110.52[.]160

Attack Name	TYPE	VALUE
Editbot Stealer	SHA256	3f7bd47fbbf1fb0a63ba955c8f9139d6500b6737e5baf5fdb783f0cedae94d6d
	SHA1	eed59a282588778ffbc772085b03d229a5d99e35
	MD5	669e7ac187fb57c4d90b07d9a6bb1d42
Graphical Proton	SHA256	01B5F7094DE0B2C6F8E28AA9A2DED678C166D615530E595621E692A9C0240732, 34C8F155601A3948DDB0D60B582CFE87DE970D443CC0E05DF48B1A1AD2E42B5E, 620D2BF14FE345EEF618FDD1DAC242B3A0BB65CCB75699FE00F7C671F2C1D869, 773F0102720AF2957859D6930CD09693824D87DB705B3303CEF9EE794375CE13, 7B666B978DBBE7C032CEF19A90993E8E4922B743EE839632BFA6D99314EA6C53, 8AFB71B7CE511B0BCE642F46D6FC5DD79FAD86A58223061B684313966EFEF9C7, 971F0CED6C42DD2B6E3EA3E6C54D0081CF9B06E79A38C2EDE3A2C5228C27A6DC, CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF, CD3584D61C2724F927553770924149BB51811742A461146B15B34A26C92CAD43, EBE231C90FAD02590FC56D5840ACC63B90312B0E2FEE7DA3C7606027ED92600E, F1B40E6E5A7CBC22F7A0BD34607B13E7E3493B8AAD7431C47F1366F0256E23EB, C7B01242D2E15C3DA0F45B8ADEC4E6913E534849CDE16A2A6C480045E03FBEE4, 4BF1915785D7C6E0987EB9C15857F7AC67DC365177A1707B14822131D43A6166, 18101518EAE3EEC6EBE453DE4C4C380160774D7C3ED5C79E1813013AC1BB0B93, 19F1EF66E449CF2A2B0283DBB756850CCA396114286E1485E35E6C672C9C3641, 1E74CF0223D57FD846E171F4A58790280D4593DF1F23132044076560A5455FF8, 219FB90D2E88A2197A9E08B0E7811E2E0BD23D59233287587CCC4642C2CF3D67,

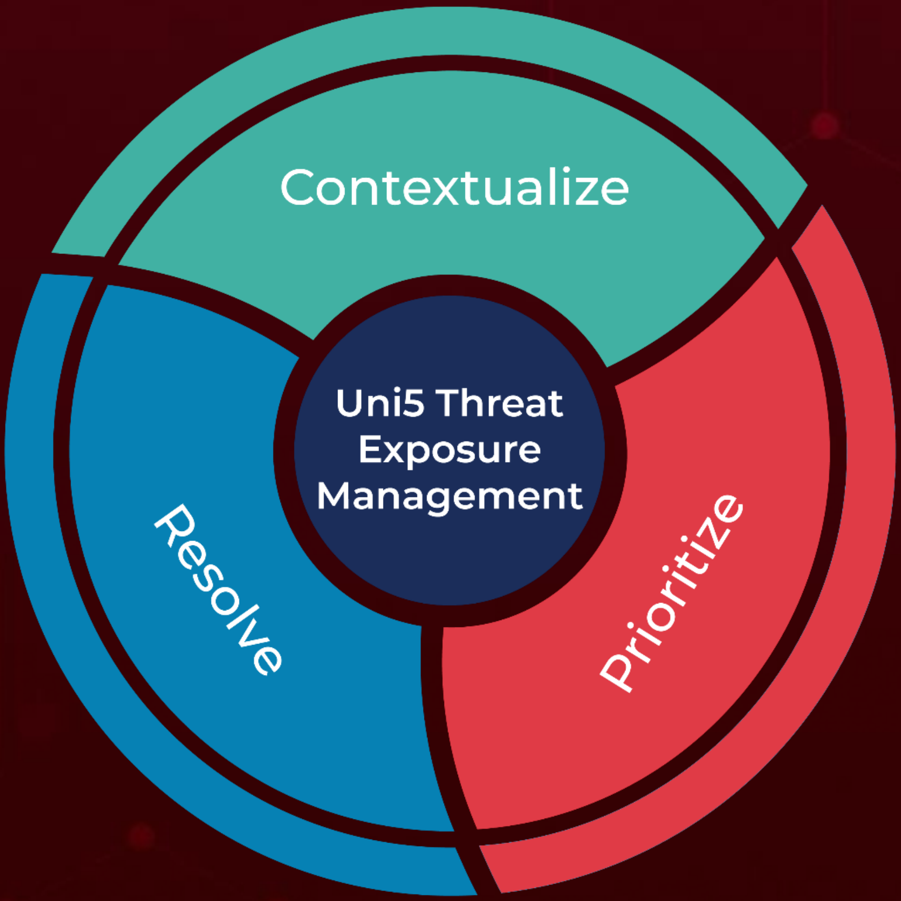
Attack Name	TYPE	VALUE
Graphical Proton	SHA256	92C7693E82A90D08249EDEAFBCA6533FED81B62E9E056DEC34C24756E0A130A6, B53E27C79EED8531B1E05827ACE2362603FB9F77F53CEE2E34940D570217CBF7, C37C109171F32456BBE57B8676CC533091E387E6BA733FBAA01175C43CFB6EBD, C40A8006A7B1F10B1B42FDD8D6D0F434BE503FB3400FB948AC9AB8DDFA5B78A0, C832462C15C8041191F190F7A88D25089D57F78E97161C3003D68D0CC2C4BAA3, F6194121E1540C3553273709127DFA1DAAB96B0ACFAB6E92548BFB4059913C69,
Rhadamanthys stealer	SHA256	bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476,

Attack Name	TYPE	VALUE
Rhadamanthys stealer	SHA256	3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

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

December 18, 2023 • 7:30 AM

More at www.hivepro.com