

Date of Publication
April 1, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

25 to 31 MARCH 2024

Table Of Contents

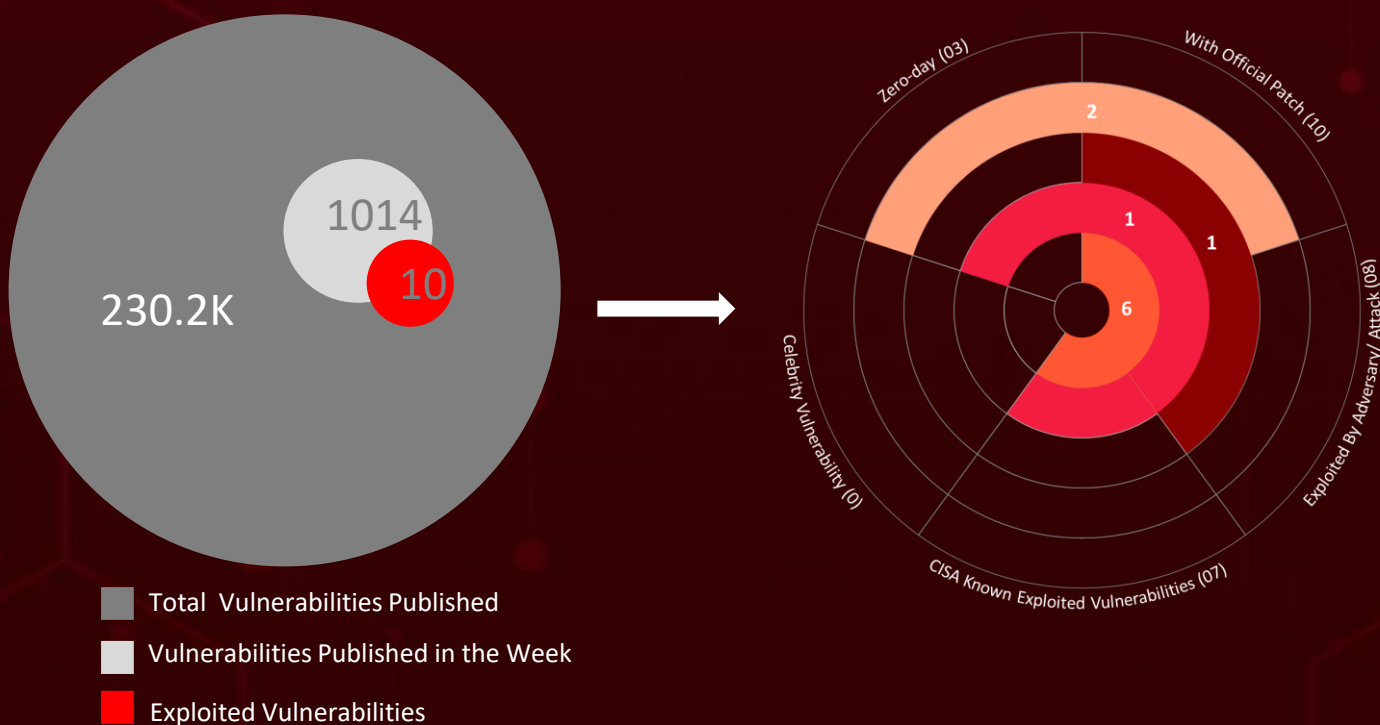
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	17
<u>Adversaries in Action</u>	22
<u>Recommendations</u>	24
<u>Threat Advisories</u>	25
<u>Appendix</u>	26
<u>What Next?</u>	29

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **twelve** attacks were executed, **ten** vulnerabilities were uncovered, and **two** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a cybercriminal group **APT29**, targeting Germany to deploy a new backdoor variant named WINELOADER, marking a broader threat to European and Western political entities.

Meanwhile Google has addressed two zero-day vulnerabilities identified in Chrome, (**CVE-2024-2886**, **CVE-2024-2887**). Uncovered in Pwn2Own Vancouver 2024 event, these vulnerabilities empower attackers to achieve arbitrary code execution.



High Level Statistics

12

Attacks
Executed

10

Vulnerabilities
Exploited

2

Adversaries in
Action

- WINELOADER
- ROOTSAW
- Evil Ant
- Ransomware
- StrelaStealer
- Agenda
- ransomware
- Sysrv Botnet
- XMRig Miner
- SNOWLIGHT
- GOHEAVY
- GOREVERSE
- SUPERSHELL
- HackBrowserData
- CVE-2017-9805
- CVE-2023-22527
- CVE-2021-26084
- CVE-2023-46747
- CVE-2024-1709
- CVE-2023-22518
- CVE-2022-0185
- CVE-2022-30525
- CVE-2024-2886
- CVE-2024-2887
- APT29
- UNC5174



Insights

Evil Ant

Ransomware,
Python-based malware, elevate user privileges to the admin level

Operation FlightNight

Campaign lead by unidentified threat actors targeting Indian government agencies and energy companies, aiming to deploy a modified variant of HackBrowserData stealer

StrelaStealer

Deployed in phishing attacks targeting over 100 organizations across the US and the E.U.

Zero-day Flaws in Chrome,

CVE-2024-2886, CVE-2024-2887 from Pwn2Own Vancouver 2024, allowing threat actor arbitrary code execution

UNC5174 - Initial Access

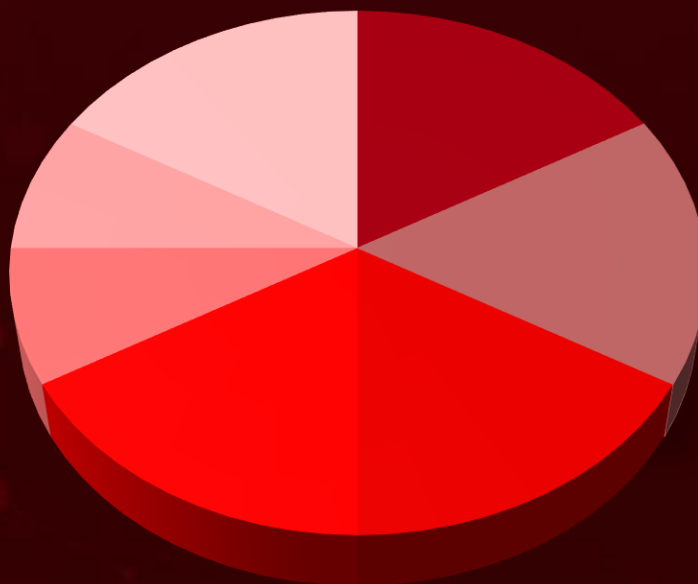
Broker exploiting various vulnerabilities to deploy custom tools such as SNOWLIGHT, GOHEAVY, and GOREVERSE for post-exploitation activities

Agenda

ransomware

Targeting Industries worldwide by crippling virtual machines and causing data loss

Threat Distribution



- Backdoor
- Dropper
- Ransomware
- Stealer
- Botnet
- Miner
- Hack Tool

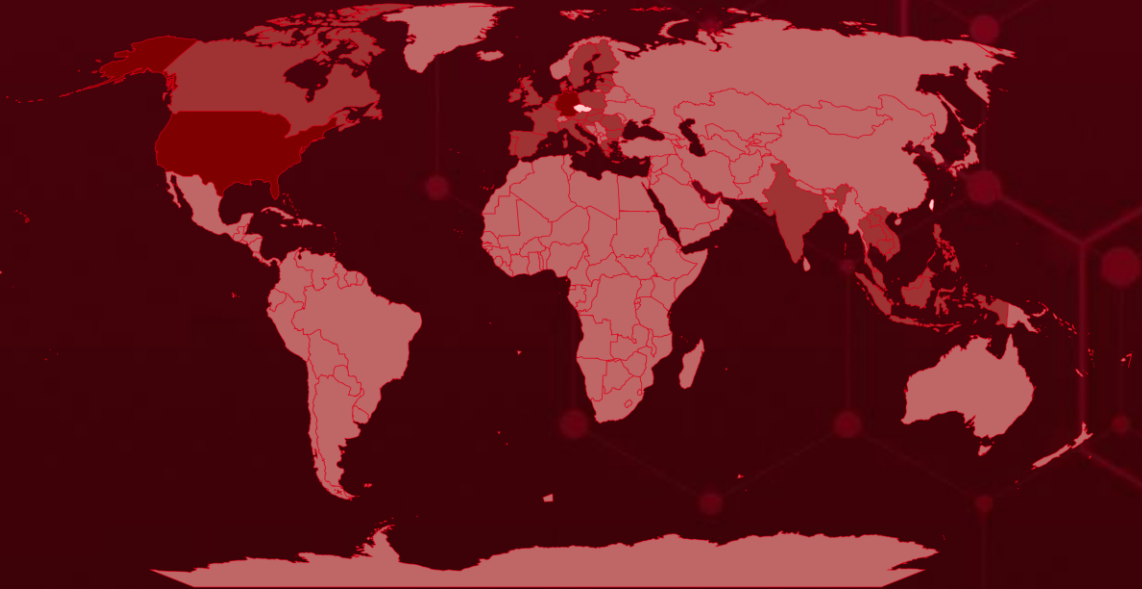


Targeted Countries

Most



Least

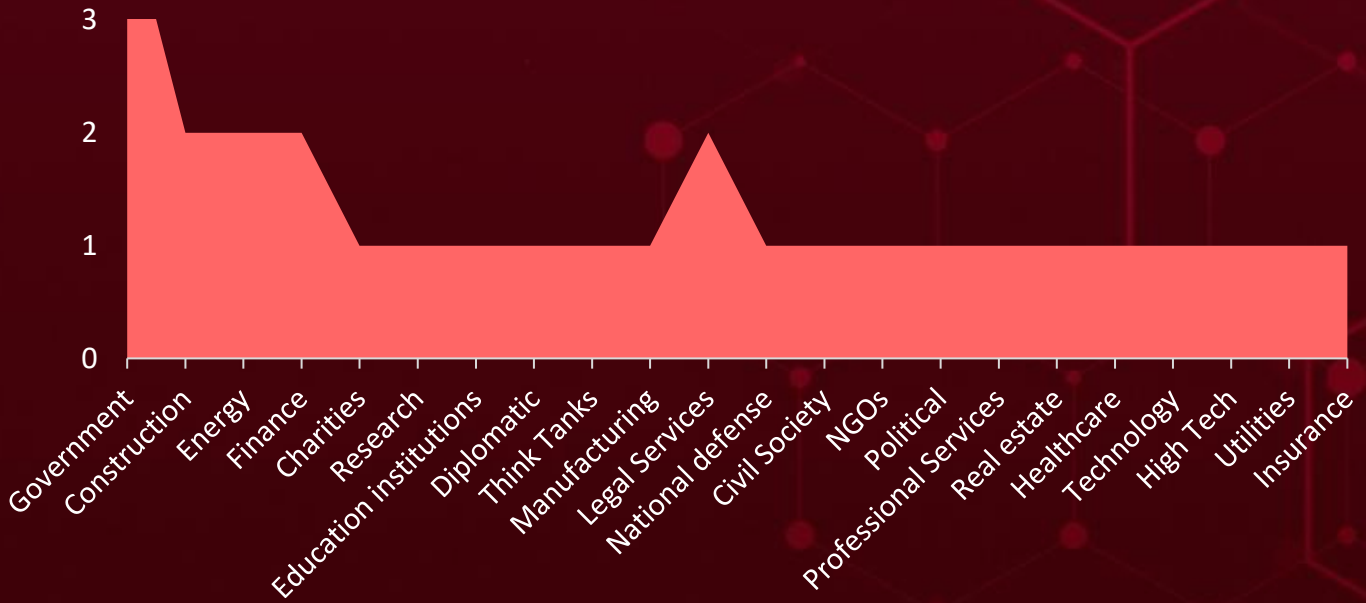


Powered by Bing

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

Countries	Countries	Countries	Countries
United States	Belgium	South Africa	Mozambique
Germany	Portugal	Djibouti	Fiji
Sweden	Romania	Togo	Nepal
Malta	Greece	Dominica	Bahamas
Vietnam	Slovakia	Montenegro	Niger
Brunei	Hungary	Dominican Republic	Bahrain
Singapore	Spain	New Zealand	Norway
Bulgaria	India	DR Congo	Gabon
Austria	Thailand	Pakistan	Panama
Cambodia	Indonesia	Ecuador	Gambia
Luxembourg	United Kingdom	Antigua and Barbuda	Burundi
Canada	Ireland	Egypt	Georgia
Philippines	Italy	San Marino	Cameroon
Croatia	Latvia	El Salvador	Bangladesh
Slovenia	Suriname	Central African Republic	Saint Lucia
Cyprus	Paraguay	Equatorial Guinea	Ghana
Timor-Leste	Namibia	Sri Lanka	Saudi Arabia
Denmark	Armenia	Eritrea	Barbados
Laos	Serbia	Tajikistan	Sierra Leone
Estonia	Cuba	Azerbaijan	Grenada
Lithuania	Ukraine	Turkey	Solomon Islands
Finland	Australia	Eswatini	Guatemala
Malaysia	North Korea	Uruguay	South Sudan
France	Czech Republic (Czechia)	Ethiopia	Guinea
Netherlands	Rwanda		State of Palestine
Poland	Albania		Guinea-Bissau
			Switzerland

Targeted Industries



TOP MITRE ATT&CK TTPs

T1083

File and Directory Discovery

T1059

Command and Scripting Interpreter

T1204.002

Malicious File

T1027

Obfuscated Files or Information

T1566

Phishing

T1082

System Information Discovery

T1204

User Execution

T1057

Process Discovery

T1574.002

DLL Side-Loading

T1070

Indicator Removal

T1140

Deobfuscate/Decode Files or Information

T1003

OS Credential Dumping

T1543.003

Windows Service

T1497

Virtualization/Sandbox Evasion

T1036

Masquerading

T1574

Hijack Execution Flow

T1041

Exfiltration Over C2 Channel

T1486

Data Encrypted for Impact

T1055

Process Injection

T1543

Create or Modify System Process

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>WINELOADER</u>	WINELOADER is a backdoor malware linked to APT29, a hacking group believed to be affiliated with Russia's Foreign Intelligence Service (SVR). It grants remote access to compromised devices and networks for the attackers.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			Windows
ASSOCIATED ACTOR		Date Loss, System Compromise	PATCH LINK
APT29			-
IOC TYPE	VALUE		
MD5	e017bfc36e387e8c3e7a338782805dde, 8bd528d2b828c9289d9063eba2dc6aa0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ROOTSAW</u>	ROOTSAW, also known as EnvyScout, is a malicious dropper program used in the first stage of an attack by the APT29 hacking group. Its primary function is to "drop" or install the real malicious payload, which is typically something like WINELOADER that provides remote access to attackers.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Dropper			Windows
ASSOCIATED ACTOR		Date Loss, System Compromise	PATCH LINK
APT29			-
IOC TYPE	VALUE		
MD5	efafcd00b9157b4146506bd381326f39		

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>Evil Ant Ransomware</u>	Evil Ant Ransomware, a sophisticated Python-based malware compiled with PyInstaller, operates covertly by hiding its console window and executing tasks discreetly. It aims to gain access to critical system functions and encrypt secured files.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			PATCH LINK
-		Date Loss, Financial Loss	-
IOC TYPE	VALUE		
SHA256	355784fa1c77e09c0de0fcd277bfc9edb3920933f2003d2d1d1b84822f25697b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>StrelaStealer</u>	StrelaStealer, a dynamic information-stealing malware. It is notorious for its capability to steal email login credentials from well-known email clients and send them to an attacker-controlled server. The latest iteration features an improved DLL payload obfuscation technique and is disseminated through a compressed JScript file.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Date Loss	-
IOC TYPE	VALUE		
SHA256	0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a, e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1, f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e, aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054, b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680		

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>Agenda ransomware (aka Qilin, Water Galura)</u>	<p>Agenda ransomware, also known as Qilin, active since 2022, targets global victims across industries. Their latest tactic leverages a custom script to infect VMWare environments, potentially crippling virtual machines and causing data loss.</p>	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			
ASSOCIATED ACTOR		Date Loss, Financial Loss	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Sysrv Botnet</u>	<p>Sysrv is a potent threat, generating conspicuous bot traffic that targets numerous sites across various countries. It endeavors to exploit well-known web vulnerabilities in Apache Struts and Atlassian Confluence.</p>	Exploiting network vulnerabilities	CVE-2017-9805 CVE-2023-22527 CVE-2021-26084
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet			
ASSOCIATED ACTOR		Date Loss, System Compromise, Financial Loss	PATCH LINK
-			https://cwiki.apache.org/confluence/display/WW/S2-052 https://jira.atlassian.com/browse/CONFSERVER-93833 https://jira.atlassian.com/browse/CONFSERVER-67940
IOC TYPE	VALUE		
SHA256	1ba8f42d8db461bb45f9d3e991c137b7b504aee5213cfe7a12cd4b366512696e		

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>XMRig</u>	<p>XMRig is open-source software designed for mining cryptocurrencies. It is also commonly abused by cybercriminals in their attacks, who infect computers with cryptojackers and use their resources to mine cryptocurrency on the attacker's behalf.</p>	Exploiting Vulnerabilities	CVE-2017-9805 CVE-2023-22527 CVE-2021-26084
TYPE		IMPACT	AFFECTED PRODUCTS
Miner		Mining cryptocurrencies	Apache Struts, Atlassian Confluence
ASSOCIATED ACTOR			PATCH LINK
-			https://cwiki.apache.org/confluence/display/WW/S2-052 https://jira.atlassian.com/browse/CONFSERVER-93833 https://jira.atlassian.com/browse/CONFSERVER-67940
IOC TYPE	VALUE		
SHA256	6fb9b4dced1cf53a9533ed497f38550915f9e448e62a6f43e9d8b696bd5375dc, f0a299b93f1a2748edd69299f694d3a12edbe46485d29c1300172d4ac4fd09d4, 495500dcd8b3fa858335f0c85ddcc265f09ed638d87226e8bce8b53ef626464e, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, 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>SNOWLIGHT</u>	<p>SNOWLIGHT is a 64-bit ELF downloader written in C, specifically designed to run on Linux systems. It utilizes raw sockets to establish connections with a hard-coded IP address over TCP port 443. Additionally, it employs a binary protocol to communicate with the command-and-control (C2 or C&C) server.</p>	Exploiting vulnerabilities	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525
TYPE		IMPACT	AFFECTED PRODUCTS
Dropper		Data Loss, System Compromise	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls
ASSOCIATED ACTOR			PATCH LINK
UNC5174 (aka Uteus)			https://my.f5.com/manage/s/article/K000137353 https://screenconnect.connectwise.com/download https://www.atlassian.com/software/confluence/download-archives https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls
IOC TYPE	VALUE		
MD5	c867881c56698f938b4e8edafe76a09b, df4603548b10211f0aa77d0e9a172438, 0951109dd1be0d84a33d52c135ba9c97, 0ba435460fb7622344eec28063274b8a, a78bf3d16349eba86719539ee8ef562d		

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>GOHEAVY</u>	<p>GOHEAVY is a Golang-based tunneler tool that utilizes the Gin framework to manage traffic routing functionalities. It continuously broadcasts the string "SpotUdp" to existing network interfaces.</p>	Exploiting vulnerabilities	<p>CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525</p>
TYPE		IMPACT	AFFECTED PRODUCTS
Hack Tool		<p>Data Loss, System Compromise</p>	<p>F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls</p>
ASSOCIATED ACTOR			PATCH LINK
UNC5174 (aka Uteus)			<p>https://my.f5.com/manage/s/article/K000137353 https://screenconnect.connectwise.com/download https://www.atlassian.com/software/confluence/download-archives https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</p>

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>GOREVERSE</u>	GOREVERSE is a publicly available reverse shell backdoor written in GoLang. It operates over Secure Shell (SSH) and calls back to the Command-and-Control (C2) infrastructure previously observed hosting the SUPERSHELL framework.	Exploiting vulnerabilities	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Loss, System Compromise	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls
ASSOCIATED ACTOR			PATCH LINK
UNC5174 (aka Uteus)			https://my.f5.com/manage/s/article/K000137353 https://screenconnect.connectwise.com/download https://www.atlassian.com/software/confluence/download-archives https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls
IOC TYPE	VALUE		
SHA256	9e1527fc21622f99b1bce657cda6ad243b0854763eaa0cec45b2c6a64cae9846, 2b54d1c064892a22f48b5742ba6da55bf62b73e5b1e0649e8b7880b286498735, 4d3570a0c63109786a10ff66eaf0c6c134715dc33e5c85e701ba0cc8cf139df2		

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>SUPERSHELL</u>	<p>SUPERSHELL is a Command-and-Control (C2) infrastructure hosted on webservers, offering a user interface for managing remote connections along with additional malicious toolkits. It is a publicly available C2 framework published on GitHub and is utilized extensively in related infrastructure by the administrators of SUPERSHELL.</p>	Exploiting vulnerabilities	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525
TYPE		IMPACT	AFFECTED PRODUCTS
Hack Tool		Data Loss, System Compromise	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls
ASSOCIATED ACTOR			PATCH LINK
UNC5174 (aka Uteus)			https://my.f5.com/manage/s/article/K000137353 https://screenconnect.connectwise.com/download https://www.atlassian.com/software/confluence/download-archives https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls
IOC TYPE	VALUE		
URL	http://172.245.68[.]110:8888		




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>HackBrowserData</u>	HackBrowserData, originally an open-source tool for stealing browser login credentials, cookies, and history, has been modified for more nefarious purposes. In Operation FlightNight, a variant of this tool was observed, the modified variant includes new functionalities such as communication via Slack channels.	Slack channels	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information stealer			-
ASSOCIATED ACTOR			PATCH LINK
-		Data Loss, System Compromise	-
IOC TYPE	VALUE		
SHA256	4dd0b10dac5966bb0126269e2bd65216980f054e77047fcfff126ae6b20484a6, b4d9a690cc7e05555e64a4610698d565f7ec0fe1758b85d141e1eb984699201b, ef1dfe421654b384c88f66a0fd2d72dcb81efac560e882881397bb852b1089f, 791accb23604998764e781c0060225c5daa8b97b876d7cade7c3fe20dd934eb2, dd7503ba0cae14a8fae67fa9e80ec3f5752b2587251417bdaafcf9f32fca5d7		




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-2017-9805		Apache Struts	-			
	ZERO-DAY					
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE			
NAME	CISA KEV	cpe:2.3:a:apache:struts:- .*:.*:.*:.*:.*:.*	Sysrv Botnet, XMRig Miner			
Apache Struts Deserialization of Untrusted Data Vulnerability				CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502			T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://cwiki.apache.org/confluence/display/WW/S2-052	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR			
CVE-2023-22527		Atlassian Confluence Data Center and Server	-			
	ZERO-DAY					
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE			
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*.:*:*.:*:*.:*: * cpe:2.3:a:atlassian:confluence_server:*.:*:*.:*:*.:*: *	Sysrv Botnet, XMRig Miner			
Atlassian Confluence Data Center and Server Template Injection Vulnerability				CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74			T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://jira.atlassian.com/browse/CONFSERVER-93833	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-26084</u>		Atlassian Confluence Server and Data Center	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*	Sysrv Botnet, XMRig Miner
Atlassian Confluence Server and Data Center		cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*	
Object-Graph Navigation Language (OGNL) Injection Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	<u>https://jira.atlassian.com/browse/CONFSERVER-67940</u>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-46747</u>		F5 BIG-IP Configuration Utility	UNC5174 (aka Uteus)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL
F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306 CWE-288	T1190: Exploit Public-Facing Application	<u>https://my.f5.com/manage/s/article/K000137353</u>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR		
<u>CVE-2024-1709</u>		ConnectWise ScreenConnect	UNC5174 (aka Uteus)		
	ZERO-DAY				
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE		
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL		
ConnectWise ScreenConnect Authentication Bypass Vulnerability				ASSOCIATED TTPs	PATCH LINK
	CWE ID			T1190: Exploit Public-Facing Application	<u>https://screenconnect.com/connectwise.com/download</u>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR		
<u>CVE-2023-22518</u>		Confluence Data Center, Confluence Server	UNC5174 (aka Uteus)		
	ZERO-DAY				
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE		
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:* * cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL		
Atlassian Confluence Improper Authorization Vulnerability				ASSOCIATED TTPs	PATCH LINK
	CWE ID			T1574: Hijack Execution Flow, T1190: Exploit Public-Facing Application	<u>https://www.atlassian.com/software/confluence/download-archives</u>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-0185</u>		FAS/AFF BMC, NetApp HCI BMC	UNC5174 (aka Uteus)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel: *.*.*.*.*.*.*.*	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL
Linux Kernel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-191 CWE-190	T1574: Hijack Execution Flow, T1211: Exploitation for Defense Evasion	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-30525</u>		USG FLEX, ATP series, VPN series	UNC5174 (aka Uteus)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:zyxel:usg_flex_100 w:-.*.*.*.*.*.*.*	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL
Zyxel Multiple Firewalls OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-2886		Google Chrome prior to 123.0.6312.86	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrom	
Google Chrome WebCodecs Use After Free Vulnerability		e:*.:.:.:.:.:.:.*.:	-
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-416	T1059: Command and Scripting Interpreter, T1189: Drive-by Compromise	Update Chrome browser to the latest version 123.0.6312.86/.87 for Windows and Mac and 123.0.6312.86 for Linux. Link: https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-2887		Google Chrome prior to 123.0.6312.86	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrom	
Google Chrome WebAssembly Type Confusion Vulnerability		e:*.:.:.:.:.:.:.*.:	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter, T1189: Drive-by Compromise	Update Chrome browser to the latest version 123.0.6312.86/.87 for Windows and Mac and 123.0.6312.86 for Linux. Link: https://www.google.com/intl/en/chrome/?standalone=1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>APT29 (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, Midnight Blizzard, UNC3524, Cranefly, TEMP.Monkeys, Cloaked Ursa, Blue Dev 5, NobleBaron, Solar Phoenix)</u></p>	Russia	Diplomatic, Political, Government, and Civil Society	Germany
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	WINELOADER, ROOTSAW	Windows	
TTPs			
<p>TA0007: Discovery; TA0011: Command and Control; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1543.003: Windows Service; T1543: Create or Modify System Process; T1012: Query Registry; 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; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution</p>			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>UNC5174 (aka Uteus)</u>	Affiliated to China	Research, Education institutions, Charities and Non-governmental organizations (NGOs), Government organizations, Think Tanks	Southeast Asia, US, Hong Kong, UK, Canada, Taiwan
	MOTIVE		
	Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525	SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1140: Deobfuscate/Decode Files or Information; T1222: File and Directory Permissions Modification; T1222.002: Linux and Mac File and Directory Permissions Modification; T1601: Modify System Image; T1601.001: Patch System Image; T1016: System Network Configuration Discovery; T1049: System Network Connections Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.001: Local Account; T1531: Account Access Removal; T1003: OS Credential Dumping; T1003.008: /etc/passwd and /etc/shadow; T1608: Stage Capabilities; T1608.003: Install Digital Certificate

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **APT29, UNC5174** and malware **WINELOADER, ROOTSAW, Evil Ant Ransomware, StrelaStealer, Agenda ransomware, Sysrv Botnet, XMRig Miner, SNOWLIGHT, GOHEAVY, GOREVERSE, SUPERSHELL, HackBrowserData**.

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 **ten exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT29, UNC5174** and malware **WINELOADER, ROOTSAW, Evil Ant Ransomware, StrelaStealer, Agenda ransomware, XMRig Miner, SNOWLIGHT, HackBrowserData** in Breach and Attack Simulation(BAS).

Threat Advisories

[APT29 Targets German Political Parties with New WINELOADER](#)

[Evil Ant: The Python-Powered Ransomware](#)

[StrelaStealer Resurfaces with Upgraded Attack Chain](#)

[Agenda Ransomware Targets VMWare vCenter & ESXi Servers Globally](#)

[Sysrv Harnessing Google Subdomains to Circulate XMRig](#)

[UNC5174 Functions as an Initial Access Broker, Exploiting Vulnerabilities](#)

[Google Patches Critical Zero-Day Exploits Found at Pwn2Own](#)

['Operation FlightNight' Targeting India with Deceptive Air Force Invitations](#)

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>WINELOADER</u>	MD5	e017bfc36e387e8c3e7a338782805dde, 8bd528d2b828c9289d9063eba2dc6aa0
<u>ROOTSAW</u>	MD5	efafcd00b9157b4146506bd381326f39
<u>Evil Ant Ransomware</u>	MD5	ac612b8f09ec1f9d87a16873f27e15f0
	SHA1	066b96a82ac998a04897dc1bd25c2e1b6d075182
	SHA256	355784fa1c77e09c0de0fcd277bfc9edb3920933f2003d2d1d1 b84822f25697b
	URL	hxxps[://]api[.]telegram[.]org/bot6893451039:AAGMOFYI9- RF8rfOKQUSizMAqvr28TKmgpY/sendMessage
	Email	evilant[.]ransomware[.]gmail[.]com
	Bitcoin Address	3CLUhZqfXmM8VUHhR3zTgQ8wKY72cSn989
<u>StrelaStealer</u>	IPv4	193[.]109[.]85[.]231

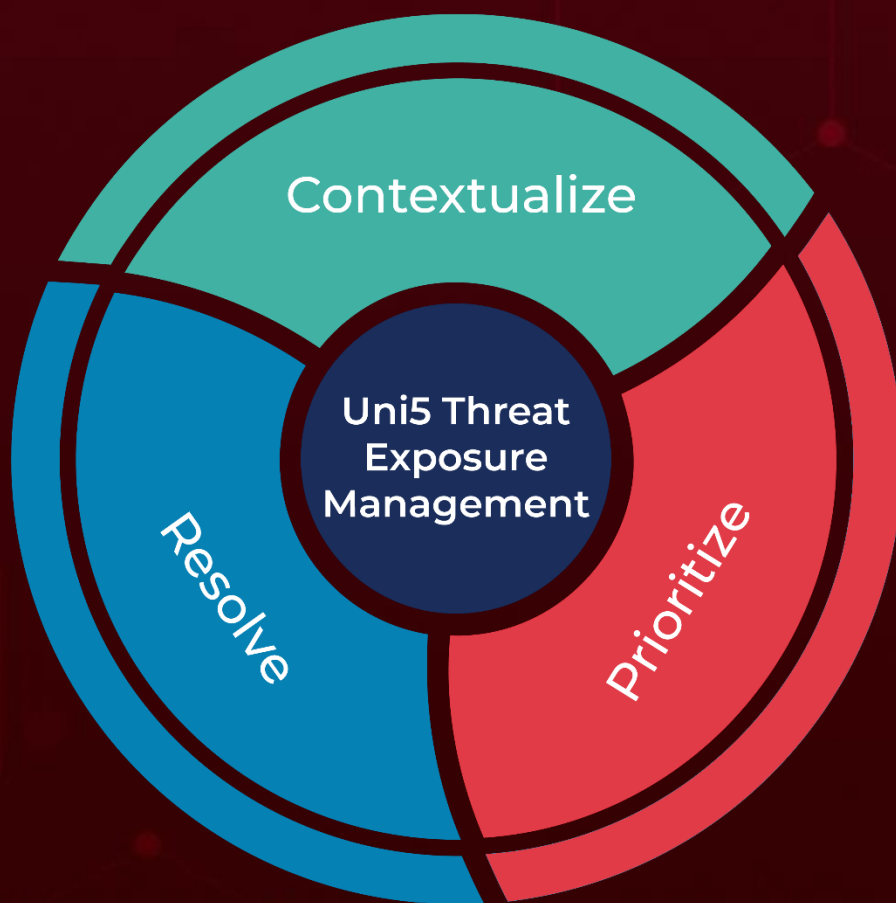
Attack Name	TYPE	VALUE
<u>StrelaStealer</u>	SHA256	0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a, e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1, f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e, aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054, b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680, 3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b, 544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45
<u>Agenda ransomware</u>	SHA256	73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38
<u>Sysrv Botnet</u>	SHA256	1ba8f42d8db461bb45f9d3e991c137b7b504aee5213cfe7a12cd4b366512696e
<u>XMRig Miner</u>	SHA256	6fb9b4dced1cf53a9533ed497f38550915f9e448e62a6f43e9d8b696bd5375dc, f0a299b93f1a2748edd69299f694d3a12edbe46485d29c1300172d4ac4fd09d4, 495500dcd8b3fa858335f0c85ddcc265f09ed638d87226e8bce8b53ef626464e, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b
<u>SNOWLIGHT</u>	MD5	c867881c56698f938b4e8edafe76a09b, df4603548b10211f0aa77d0e9a172438, 0951109dd1be0d84a33d52c135ba9c97, 0ba435460fb7622344eec28063274b8a, a78bf3d16349eba86719539ee8ef562d
<u>GOREVERSE</u>	SHA256	9e1527fc21622f99b1bce657cda6ad243b0854763eaa0ceec45b2c6a64cae9846, 2b54d1c064892a22f48b5742ba6da55bf62b73e5b1e0649e8b7880b286498735, 4d3570a0c63109786a10ff66eaf0c6c134715dc33e5c85e701ba0cc8cf139df2
<u>SUPERSHELL</u>	URL	http://172.245.68[.]110:8888

Attack Name	TYPE	VALUE
<u>HackBrowserData</u>	SHA256	4dd0b10dac5966bb0126269e2bd65216980f054e77047cfff126ae6b20484a6, b4d9a690cc7e05555e64a4610698d565f7ec0fe1758b85d141e1eb984699201b, ef1dfe421654b384c88f66a0fd2d72dcba81efac560e882881397bb852b1089f, 791accb23604998764e781c0060225c5daa8b97b876d7cade7c3fe20dd934eb2, dd7503ba0cae14a8fae67fa9e80ec3f5752b2587251417bdaafcfd9f32fca5d7, c4d8284c12dfb8f066cc790adf197c1a231d225b085695528329b619958918a0

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

April 1, 2024 • 7:15 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com