

Date of Publication
October 07, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

30 SEPTEMBER to 06 OCTOBER 2024

Table Of Contents

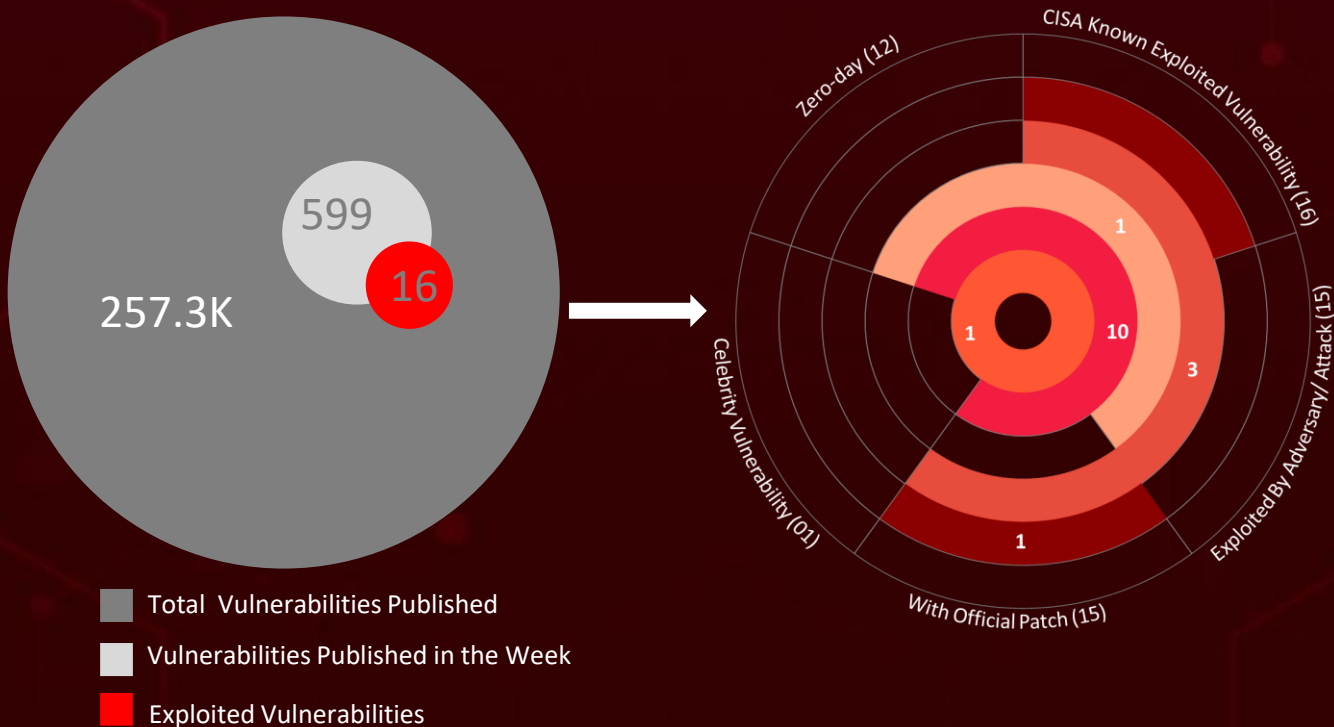
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	19
<u>Recommendations</u>	22
<u>Threat Advisories</u>	23
<u>Appendix</u>	24
<u>What Next?</u>	28

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **four** attacks were executed, **sixteen** exploited vulnerabilities were uncovered, and **three** active adversaries were identified. These findings highlight the growing and persistent risk posed by cyber intrusions.

A new **cryptojacking operation** is targeting Docker and Kubernetes environments, exploiting exposed Docker API endpoints without authentication to mine cryptocurrency. The **Raptor Train botnet framework**, operational since mid-2020, has evolved into a highly complex, multi-layered network primarily targeting SOHO networks and IoT devices. By June 2024, the botnet had expanded significantly, amassing a database of over **1.2 million compromised devices** globally.

Additionally, **SloppyLemming**, a sophisticated threat actor likely originating from India, has been orchestrating an advanced cyberespionage campaign across South and East Asia. Concurrently, a recent spear-phishing campaign is targeting recruiters, leveraging a JavaScript-based backdoor known as **More eggs**, disguised as fraudulent job applications. These escalating threats present an immediate and critical danger to global cybersecurity.



High Level Statistics

4

Attacks
Executed

- [XMRig](#)
- [More eggs](#)
- [Nosedive](#)
- [Raptor Train](#)

16

Vulnerabilities
Exploited

- [CVE-2024-5217](#)
- [CVE-2024-4577](#)
- [CVE-2024-29973](#)
- [CVE-2024-21762](#)
- [CVE-2023-38035](#)
- [CVE-2023-3519](#)
- [CVE-2023-35081](#)
- [CVE-2023-27997](#)
- [CVE-2023-22515](#)
- [CVE-2022-42475](#)
- [CVE-2022-26134](#)
- [CVE-2021-44228](#)
- [CVE-2020-8515](#)
- [CVE-2023-24229](#)
- [CVE-2023-38831](#)
- [CVE-2024-29824](#)

3

Adversaries in
Action

- [FIN6](#)
- [Flax Typhoon](#)
- [SloppyLemming](#)



Insights

Unsecured Docker APIs Are the New Goldmine for Cryptocurrency Thieves

Hiring Gone Wrong: Fake Job Applications Deliver More_eggs Malware

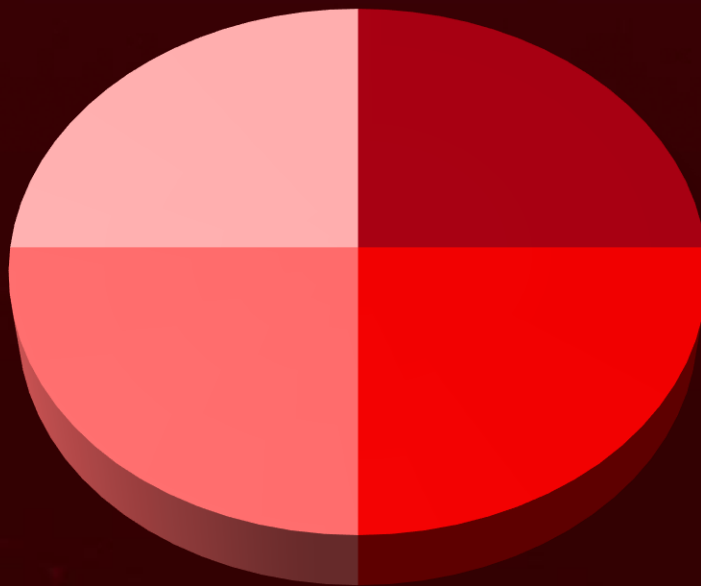
Ivanti Patches Critical EPM Flaws: Act Now to Prevent Full System Compromise

Sloppy Lemming Cyberespionage Campaign: Credential Theft and Malware Sweep Asia

Raptor Train Botnet Surges to 1.2 Million Devices: Tied to Four Major Cyber Campaigns Targeting SOHO Networks and IoT Devices

Google's Critical Fix: Chromium Users Advised to Update to Prevent Potential Exploits

Threat Distribution



■ Cryptominer ■ Backdoor ■ Botnet ■ Framework

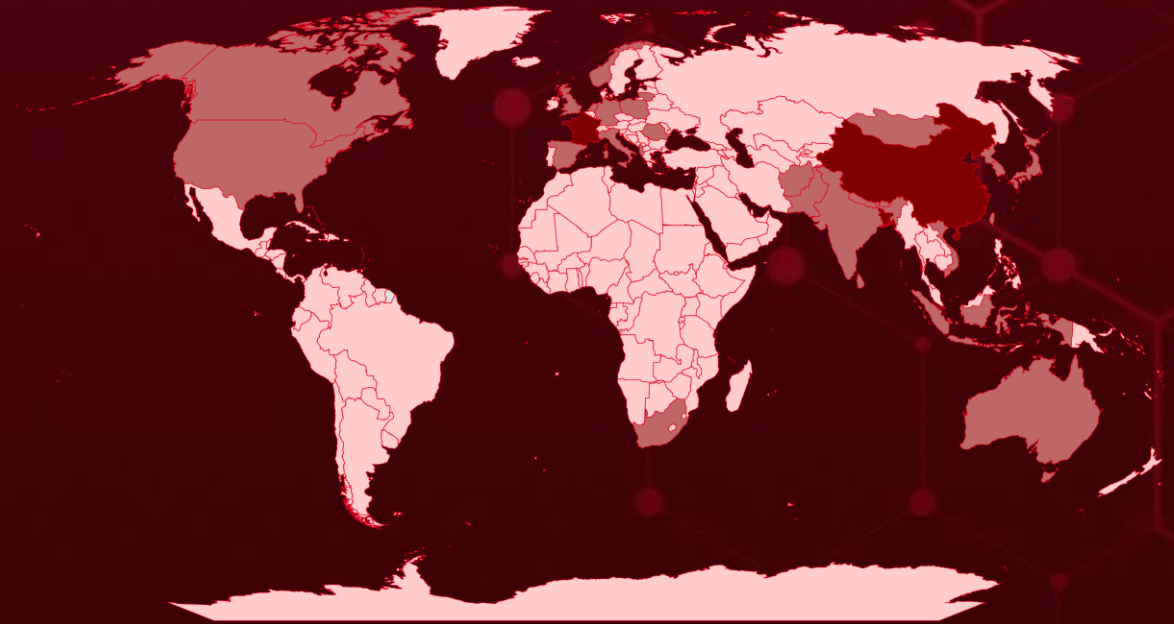


Targeted Countries

Most



Least

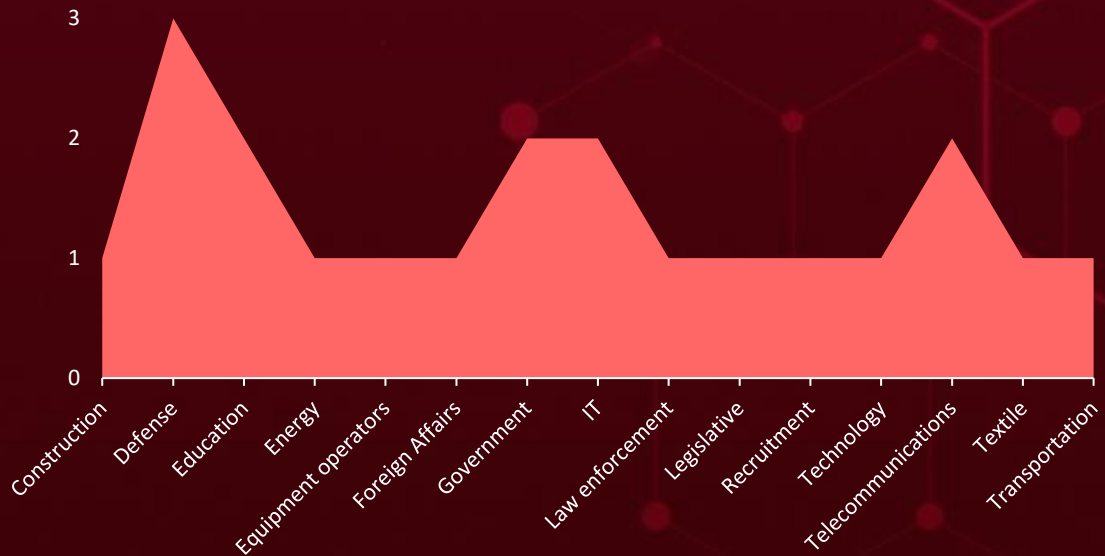


Powered by Bing

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

Countries	Countries	Countries	Countries
France	Spain	American Samoa	U.S. Virgin Islands
China	Japan	Malaysia	Costa Rica
Bangladesh	Taiwan	Cape Verde	Mali
Hong Kong	United States	Micronesia	Croatia
Maldives	United Kingdom	Cayman Islands	Mauritius
Sri Lanka	Barbados	Myanmar	Cuba
Romania	Suriname	Central African Republic	Monaco
Bhutan	Saint Barthélemy	Niger	Curaçao
Lithuania	Bouvet Island	Chad	Morocco
Canada	Marshall Islands	Belgium	Cyprus
Nepal	Brazil	Chile	Nauru
Albania	Palestine	Peru	Czech Republic
South Korea	British Indian Ocean Territory	Andorra	New Zealand
Australia	Sint Eustatius	Bermuda	Democratic Republic of the Congo
Vietnam	British Virgin Islands	Christmas Island	Niue
Germany	Turkmenistan	Saint Martin	Denmark
Macau	Brunei	Clipperton Island	Northern Cyprus
Netherlands	Montenegro	Serbia	Djibouti
Mongolia	Bulgaria	Cocos	Belize
North Korea	Belarus	Solomon Islands	Dominica
Afghanistan	Burkina Faso	Colombia	Papua New Guinea
Pakistan	Portugal	Bolivia	Dominican Republic
Norway	Burundi	Comoros	Pitcairn Islands
India	San Marino	Syria	East Timor
Poland	Cambodia	Cook Islands	Qatar
Indonesia	Cameroon	Transnistria	Easter Island
South Africa	Thailand	Coral Sea Islands	Rwanda
Italy			

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1588

Obtain Capabilities

T1068

Exploitation for Privilege Escalation

T1588.006

Vulnerabilities

T1562

Impair Defenses

T1204

User Execution

T1574

Hijack Execution Flow

T1059.003

Windows Command Shell

T1204.002

Malicious File

T1016

System Network Configuration Discovery

T1566

Phishing

T1105

Ingress Tool Transfer

T1203

Exploitation for Client Execution

T1496

Resource Hijacking

T1562.004

Disable or Modify System Firewall

T1588.001

Malware

T1574.002

DLL Side-Loading

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is an open-source cryptocurrency mining software primarily used to mine Monero (XMR), a privacy-focused cryptocurrency. It is frequently exploited in malicious campaigns, where attackers install it on compromised systems to secretly mine Monero, consuming system resources. This makes it a popular tool in cryptojacking attacks.	Exploiting container vulnerabilities	-
TYPE		IMPACT	AFFECTED PRODUCTS
Cryptominer			
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure, Financial Gains	PATCH LINK
-			
IOC TYPE	VALUE		
SHA256	505237e566b9e8f4a83edbe45986bbe0e893c1ca4c5837c97c6c4700cfa0930a, 0af1b8cd042b6e2972c8ef43d98c0a0642047ec89493d315909629bcf185dff, c5391314ce789ff28195858a126c8a10a4f9216e8bd1a8ef71d11c85c4f5175c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
More_eggs	More_eggs is a JavaScript backdoor, part of the Golden Chickens Malware-as-a-Service (MaaS) toolkit, widely adopted by financially motivated cybercriminal groups. It leverages legitimate Windows processes to bypass detection mechanisms, making it more elusive to traditional security tools.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Information Theft, Compromise Infrastructure, Deploys Payloads, Evades detection tools	PATCH LINK
FIN6			
IOC TYPE	VALUE		
SHA256	e1b4911959b6ca0db40873983e1f9d76e637818cb05d74e70b83701a5f4f4ef4		

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	TOP TARGETED CVEs
<u>Nosedive</u>	<p>Nosedive is a custom variant of the Mirai malware, and the primary implant found across most Raptor Train networks. It operates entirely in memory, allowing it to execute commands, transfer files, and conduct DDoS attacks on compromised devices. Nosedive is typically deployed using a unique URL encoding technique and a domain injection method.</p>	<p>Deployed from Tier 2 Raptor Train Framework</p>	<p>CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229</p>
TYPE		IMPACT	TOP AFFECTED PRODUCTS
Botnet		<p>Information Theft, Compromise Infrastructure, Exfiltration of data</p>	<p>RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek</p>
ASSOCIATED ACTOR			PATCH LINKS
Flax Typhoon			<p>https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313,https://www.php.net/downloads,https://www.zyxel.com/global/en/support/download,https://fortiguard.fortinet.com/psirt/FG-IR-24-015,https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035,https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467,https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081,https://www.fortiguard.com/psirt/FG-IR-23-097,https://www.atlassian.com/software/confluence/download-archives,https://www.fortiguard.com/psirt/FG-IR-22-398,https://jira.atlassian.com/browse/CONFSERVER-79016,https://logging.apache.org/security.html,https://www.draytek.com/about/security-advisory/vigor3900/-vigor2960/-vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/</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	TOP TARGETED CVEs
<u>Raptor Train</u>	<p>The Raptor Train botnet framework, active since mid-2020, has evolved into a sophisticated multi-tiered network that primarily targets SOHO networks and IoT devices. It enables scalable bot exploitation, remote control of C2 infrastructure, file transfers, command execution, and large-scale IoT-based DDoS attacks.</p>	Exploiting Vulnerabilities on SOHO networks and IoT devices	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229
TYPE		IMPACT	TOP AFFECTED PRODUCTS
Framework		<p>Sensitive Information Theft, Financial Loss, Compromised Infrastructure, Exfiltration of data</p>	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
ASSOCIATED ACTOR			PATCH LINKS
Flax Typhoon			<p>https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313,https://www.php.net/downloads.html,https://www.zyxel.com/global/en/support/download,https://fortiguard.fortinet.com/psirt/FG-IR-24-015,https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035,https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467,https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081,https://www.fortiguard.com/psirt/FG-IR-23-097,https://www.atlassian.com/software/confluence/download-archives,https://www.fortiguard.com/psirt/FG-IR-22-398,https://jira.atlassian.com/browse/CONFSERVER-79016,https://logging.apache.org/security.html,https://www.draytek.com/about/security-advisory/vigor3900-/vigor2960-/vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/</p>
IOC TYPE	VALUE		
IPv4	114[.]255[.]70[.]20, 5[.]188[.]33[.]135,		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-5217</u>		ServiceNow Now Platform	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	Nosedive, Raptor Train
ServiceNow Incomplete List of Disallowed Inputs Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter, T1588: Obtain Capabilities, T1190: Exploit Public-Facing Application	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313
	CWE-184		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4577</u>		PHP version: 5 -8.3.7	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*:*:*:*:*	Nosedive, Raptor Train
PHP-CGI OS Command Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.php.net/downloads
	CWE-78		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29973		NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*	Nosedive, Raptor Train
Zyxel Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.zyxel.com/global/en/support/download




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21762		Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*:*:*:*:*	Nosedive, Raptor Train
Fortinet FortiOS Out-of-Bound Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1203: Exploitation for Client Execution, T1588.005: Exploits, T1059.007: JavaScript	https://fortiguard.fortinet.com/psirt/FG-IR-24-015




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38035		Ivanti Sentry versions 9.18, 9.17, 9.16 and older versions	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*	Nosedive, Raptor Train
			
Ivanti Sentry Authentication Bypass Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035?language=en_US




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519		Citrix NetScaler ADC and NetScaler Gateway	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:citrix:adc:*:*:*:*:*:* cpe:2.3:a:citrix:gateway:*:*:*:*:*:*	Nosedive, Raptor Train
			
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://support.citrix.com/s/article/CTX561482-citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35081		Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	Nosedive, Raptor Train
Ivanti Endpoint Manager Mobile (EPM) Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://forum.s.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27997		Fortinet FortiOS and FortiProxy	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:**	Nosedive, Raptor Train
Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
CWE-122	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004:Application or System Exploitation, T1005:Data from Local System	https://www.fortiguard.com/psirt/FG-IR-23-097	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22515		Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*	Nosedive, Raptor Train
Atlassian Confluence Data Center and Server Broken Access Control Vulnerability			
	CWE ID	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://www.atlassian.com/software/confluence/download-archives
	CWE-269		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42475		Fortinet FortiOS	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*:*:*:*:*	Nosedive, Raptor Train
Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability			
	CWE ID	T1588.006: Vulnerabilities, T1059: Command and Scripting Interpreter, T1210: Exploitation of Remote Services	https://www.fortiguard.com/psirt/FG-IR-22-398
CWE-787			




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-26134</u>		Atlassian Confluence Server and Data Center	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:	Nosedive, Raptor Train
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://jira.atlassian.com/browse/CONFSE RVER-79016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>		Apache Log4j2	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apache:log4j:*:*:*:*:*:	Nosedive, Raptor Train
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-8515		DrayTek Vigor	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:draytek:vigor2960:- .*:.*:.*:.*:.*:.*	Nosedive, Raptor Train
Multiple DrayTek Vigor Routers Web Management Page Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.draytek.com/about/security-advisory/vigor3900/-vigor2960/-vigor300b-router-web-management-page-vulnerability-%28cve-2020-8515%29/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24229		DrayTek Vigor2960	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:draytek:vigor2960:- .*:.*:.*:.*:.*:.*	Nosedive, Raptor Train
DrayTek Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAIL
CWE-77 CWE-78	T1059: Command and Scripting Interpreter	<u>End-of-life</u>	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-38831</u>		WinRAR version 6.22 and older versions	SloppyLemming
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:rarlab:winrar:6.23:beta 1.*.*.*.*.*	-
RARLAB WinRAR Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1204.002: Malicious File	WinRAR version 6.23 or later


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-29824</u>		Ivanti Endpoint Manager 2022 SU5 and prior versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:endpoint_manager:*.*.*.*.*.*.*	-
Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting, T1562.010: Downgrade Attack	https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024


Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
 <p><u>FIN6 (aka Skeleton Spider, Gold Franklin, White Giant, ITG08, ATK 88, TAG-CR2, TAAL, Camouflage Tempest)</u></p>	Unknown	Recruitment	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
-	More_eggs	-	

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.001: Malicious Link; T1037: Boot or Logon Initialization Scripts; T1037.001: Logon Script (Windows); T1218: System Binary Proxy Execution; T1218.010: Regsvr32; T1016: System Network Configuration Discovery; T1497: Virtualization/Sandbox Evasion; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1082: System Information Discovery; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1036: Masquerading; T1047: Windows Management Instrumentation; T1057: Process Discovery; T1053: Scheduled Task/Job

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <p><u>Flax Typhoon</u> <u>(aka Ethereal Panda, RedJuliett)</u></p>	China	Military, Government, Higher Education, Telecommunications, Defense, Information Technology	Worldwide
	MOTIVE Information theft, Espionage		
	TOP TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	TOP AFFECTED PRODUCTS
	CVE-2024-5217, CVE-2024-4577, CVE-2024-29973, CVE-2024-21762, CVE-2023-38035, CVE-2023-3519, CVE-2023-35081, CVE-2023-27997, CVE-2023-22515, CVE-2022-42475, CVE-2022-26134, CVE-2021-44228, CVE-2020-8515, CVE-2023-24229	Nosedive, Raptor Train	RARLAB, Ivanti, ServiceNow, PHP-CGI, Zyxel, Fortinet, Citrix, Atlassian, Apache, DrayTek
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; TA0042: Resource Development; T1210: Exploitation of Remote Services; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1068: Exploitation for Privilege Escalation; T1071: Application Layer Protocol; T1505: Server Software Component; T1005: Data from Local System; T1571: Non-Standard Port; T1190: Exploit Public-Facing Application; T1204.002: Malicious File; T1027: Obfuscated Files or Information; T1496: Resource Hijacking; T1202: Indirect Command Execution; T1016: System Network Configuration Discovery; T1046: Network Service Discovery; T1104: Multi-Stage Channels; T1203: Exploitation for Client Execution; T1584.005: Botnet; T1584: Compromise Infrastructure; T1498: Network Denial of Service; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.001: Malware; T1587: Develop Capabilities; T1587.001: Malware			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SloppyLemming (aka Outrider Tiger, Fishing Elephant)	India	Construction, Defense, Education, Energy, Equipment operators, Foreign Affairs, Government, IT providers, Law enforcement, Legislative, Logistics, Technology, Telecommunications, Textile, Transportation	Afghanistan, Bangladesh, Bhutan, China, Hong Kong, Indonesia, Japan, Macau, Maldives, Mongolia, Nepal, North Korea, Pakistan, South Korea, Sri Lanka, Taiwan
	MOTIVE		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-38831	-	RARLAB WinRAR
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1562: Impair Defenses; T1055: Process Injection; T1212: Exploitation for Credential Access; T1580: Cloud Infrastructure Discovery; T1526: Cloud Service Discovery; T1530: Data from Cloud Storage; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1059.003: Windows Command Shell; T1068: Exploitation for Privilege Escalation; T1499: Endpoint Denial of Service; T1071: Application Layer Protocol			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **sixteen exploited vulnerabilities** and block the indicators related to the threat actors **FIN6, Flax Typhoon, SloppyLemming** and malware **XMRig, More_eggs, Nosedive, Raptor Train**.

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

- Run a Scan to discover the assets impacted by the **sixteen exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **FIN6, Flax Typhoon, SloppyLemming**, and malware **XMRig, More_eggs, Nosedive, Raptor Train** in Breach and Attack Simulation(BAS).

Threat Advisories

[Threat Actors Exploit Docker and Kubernetes for Crypto Mining](#)

[Recruitment Under Siege: The Rise of the More_eggs Malware](#)

[Raptor Train Paradox: A Multi-Tiered Botnet Phenomenon](#)

[SloppyLemming's Relentless Pursuit of Asian Targets](#)

[Critical Chromium Flaws Expose Systems to Code Execution Attacks](#)

[Active Exploitation of Critical Flaws in Ivanti EPM](#)

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>XMRig</u>	SHA256	505237e566b9e8f4a83edbe45986bbe0e893c1ca4c5837c97c6c4700cfa0930a, 0af1b8cd042b6e2972c8ef43d98c0a0642047ec89493d315909629bcf185dffdf, c5391314ce789ff28195858a126c8a10a4f9216e8bd1a8ef71d11c85c4f5175c
	URL	hxxps[:]//solscan[.]live/bin/64bit/xmrig, hxxps[:]//solscan[.]live/bin/xmrig, hxxps[:]//solscan[.]live/so/xmrig[.]so
<u>More_eggs</u>	SHA256	e1b4911959b6ca0db40873983e1f9d76e637818cb05d74e70b83701a5f4f4ef4, d207aebf701c7fb44fe06993f020ac3527680c7fa8492a0b5f6154ca
<u>Raptor Train</u>	IPv4	114[.]255[.]70[.]20, 5[.]188[.]33[.]135, 202[.]182[.]109[.]151, 5[.]188[.]33[.]228, 185[.]14[.]45[.]160, 185[.]207[.]154[.]253, 14[.]1[.]98[.]223, 223[.]98[.]159[.]112, 210[.]61[.]186[.]117, 104[.]244[.]89[.]157, 114[.]255[.]70[.]30, 140[.]82[.]14[.]222, 45[.]32[.]196[.]165, 66[.]42[.]118[.]156, 85[.]90[.]216[.]178, 85[.]90[.]216[.]184,

Attack Name	TYPE	VALUE
<u>Raptor Train</u>	IPv4	149[.]28[.]98[.]243, 66[.]42[.]83[.]4, 45[.]91[.]82[.]49, 45[.]91[.]82[.]78, 66[.]42[.]101[.]23, 92[.]223[.]30[.]61, 92[.]223[.]30[.]95, 216[.]128[.]183[.]154, 37[.]61[.]229[.]163, 37[.]61[.]229[.]171, 45[.]32[.]185[.]75, 45[.]65[.]9[.]216, 45[.]65[.]9[.]235, 45[.]65[.]9[.]28, 92[.]223[.]30[.]82, 216[.]128[.]128[.]245, 195[.]234[.]62[.]188, 195[.]234[.]62[.]192, 85[.]90[.]216[.]69, 195[.]234[.]62[.]184, 89[.]44[.]198[.]200, 207[.]148[.]68[.]131, 108[.]61[.]177[.]81, 45[.]80[.]215[.]149, 45[.]92[.]70[.]111, 45[.]13[.]199[.]140, 45[.]13[.]199[.]152, 45[.]13[.]199[.]207, 45[.]13[.]199[.]84, 45[.]13[.]199[.]96, 45[.]13[.]199[.]104, 45[.]13[.]199[.]45, 45[.]135[.]117[.]136, 45[.]10[.]58[.]133, 45[.]10[.]58[.]130, 85[.]90[.]216[.]111, 5[.]8[.]33[.]26, 45[.]10[.]58[.]128, 195[.]234[.]62[.]197, 45[.]92[.]70[.]68, 5[.]45[.]184[.]68, 195[.]234[.]62[.]198, 92[.]38[.]185[.]47, 92[.]38[.]185[.]43, 85[.]90[.]216[.]112, 45[.]10[.]58[.]129, 5[.]181[.]27[.]219, 92[.]38[.]185[.]44, 45[.]135[.]117[.]131, 85[.]90[.]216[.]110,

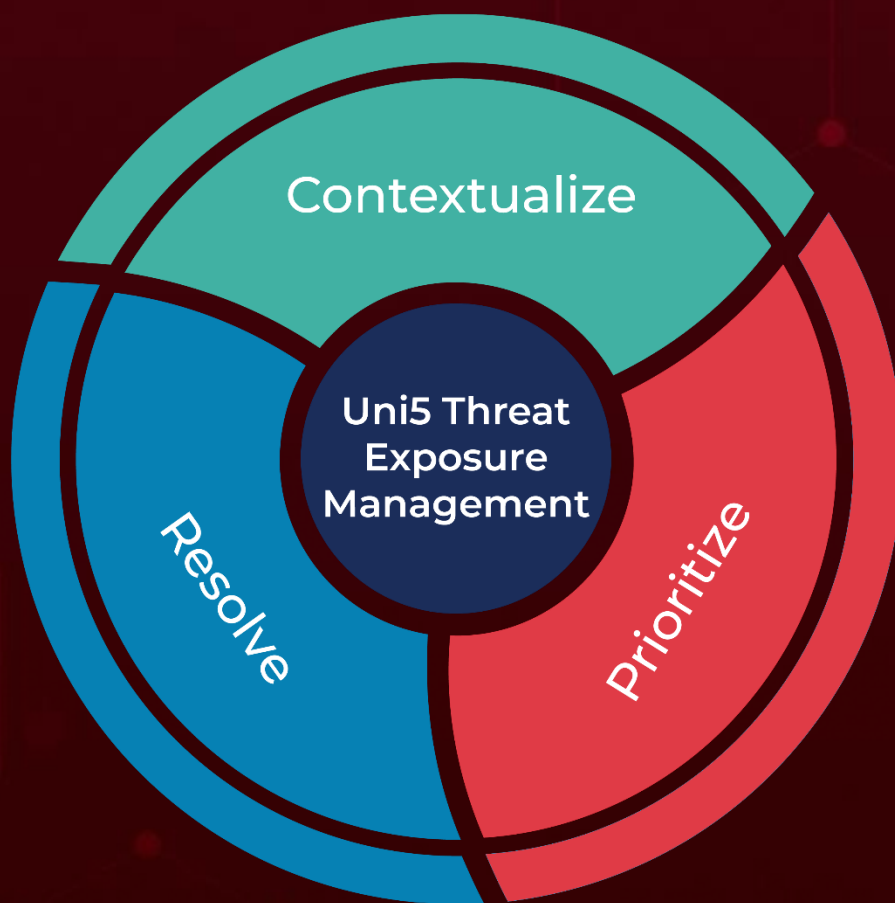
Attack Name	TYPE	VALUE
<u>Raptor Train</u>	IPv4	37[.]61[.]229[.]17, 37[.]9[.]35[.]89, 85[.]90[.]216[.]116, 37[.]61[.]229[.]15, 92[.]38[.]185[.]46, 45[.]80[.]215[.]186, 85[.]90[.]216[.]115, 45[.]10[.]58[.]132, 92[.]38[.]185[.]45, 45[.]92[.]70[.]71, 207[.]148[.]122[.]69, 91[.]216[.]190[.]154, 23[.]236[.]68[.]193, 91[.]216[.]190[.]247, 91[.]216[.]190[.]74, 45[.]80[.]215[.]47, 139[.]180[.]137[.]219, 149[.]248[.]51[.]22, 65[.]20[.]97[.]251, 45[.]77[.]231[.]209, 78[.]141[.]238[.]97, 155[.]138[.]133[.]56, 92[.]38[.]178[.]232, 92[.]223[.]30[.]233, 92[.]38[.]135[.]146, 92[.]223[.]30[.]232, 92[.]223[.]30[.]241, 155[.]138[.]151[.]225, 5[.]181[.]27[.]19, 5[.]181[.]27[.]6, 195[.]234[.]62[.]18, 45[.]80[.]215[.]153, 45[.]80[.]215[.]154, 45[.]80[.]215[.]156, 92[.]38[.]176[.]156, 45[.]80[.]215[.]151, 5[.]181[.]27[.]21, 45[.]92[.]70[.]113, 45[.]92[.]70[.]115, 195[.]234[.]62[.]19, 92[.]38[.]176[.]131, 45[.]92[.]70[.]112, 45[.]80[.]215[.]150, 45[.]80[.]215[.]155, 89[.]44[.]198[.]195, 45[.]80[.]215[.]152, 89[.]44[.]198[.]254, 91[.]216[.]190[.]2, 91[.]216[.]190[.]80, 23[.]236[.]68[.]213,

Attack Name	TYPE	VALUE
<u>Raptor Train</u>	IPv4	23[.]236[.]69[.]82, 23[.]236[.]68[.]161, 23[.]236[.]69[.]110, 23[.]236[.]68[.]229, 208[.]85[.]16[.]100, 222[.]186[.]48[.]201, 222[.]186[.]48[.]204, 37[.]9[.]35[.]91

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

October 07, 2024 • 10:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com