

Date of Publication
March 25, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

18 to 24 MARCH 2024

Table Of Contents

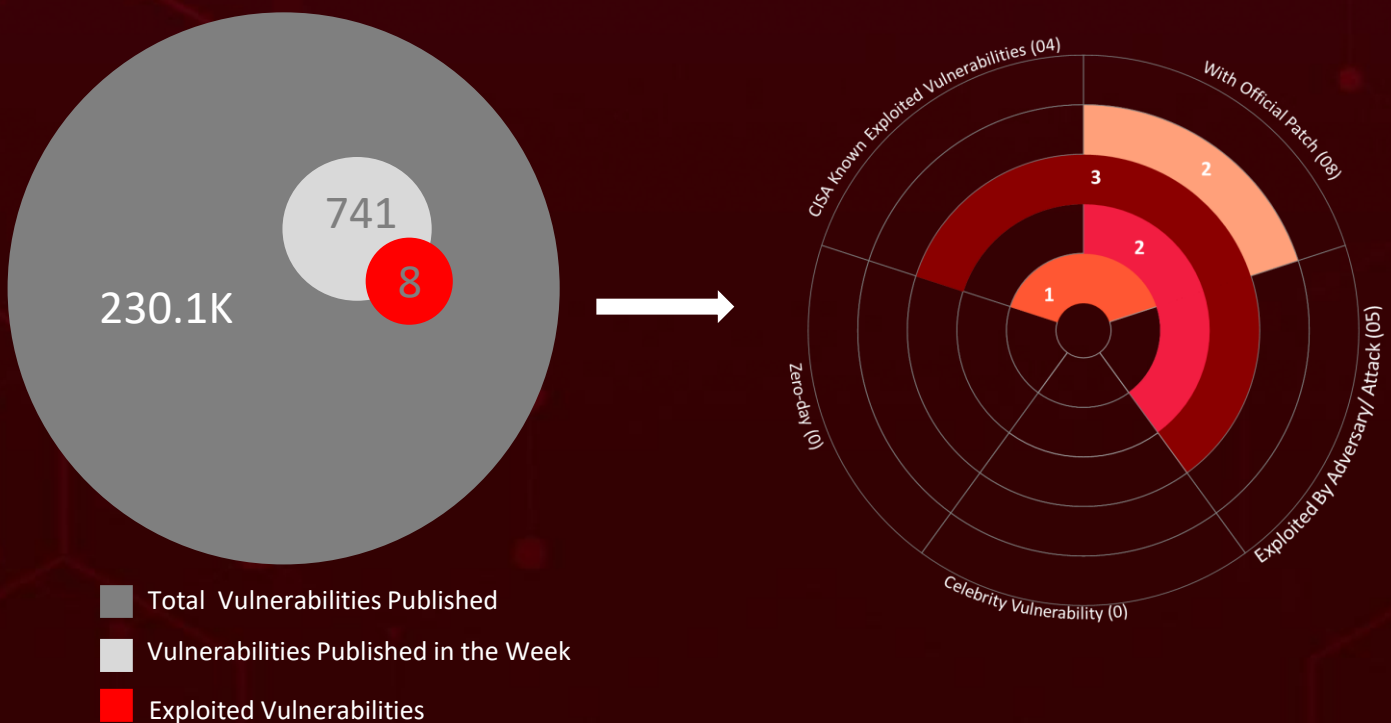
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	16
<u>Adversaries in Action</u>	20
<u>Recommendations</u>	24
<u>Threat Advisories</u>	25
<u>Appendix</u>	26
<u>What Next?</u>	32

Summary

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

Furthermore, HiveForce Labs uncovered a cybercriminal group **ShadowSyndicate**, aiming to exploit Aiohttp library vulnerability CVE-2024-23334 to access sensitive data on servers globally.

Meanwhile, critical vulnerabilities in JetBrains TeamCity (CVE-2024-27198, CVE-2024-27199), allow attackers to disseminate various malwares such as **Jasmin ransomware**, **XMRig cryptominers**, **SparkRAT backdoor**, and remote access trojans (RATs). Since the emergence of proof-of-concept (PoC) code for both vulnerabilities, multiple threat actors have been identified exploiting them in their malicious activities.



High Level Statistics

15

Attacks
Executed

8

Vulnerabilities
Exploited

5

Adversaries in
Action

- [RESHELL](#)
 - [XDealer](#)
 - [PlugX](#)
 - [ShadowPad](#)
 - [TutClient](#)
 - [TutRAT](#)
 - [xRAT](#)
 - [NetSupport RAT](#)
 - [BunnyLoader 3.0](#)
 - [AsukaStealer](#)
 - [Jasmin ransomware](#)
 - [XMRig](#)
 - [SparkRAT](#)
 - [AcidPour](#)
 - [AcidRain](#)
- [CVE-2024-2172](#)
 - [CVE-2023-32315](#)
 - [CVE-2022-21587](#)
 - [CVE-2024-23334](#)
 - [CVE-2023-41724](#)
 - [CVE-2024-27198](#)
 - [CVE-2024-27199](#)
 - [CVE-2024-1597](#)
- [Earth Krahang](#)
 - [Earth Lusca](#)
 - [ShadowSyndicate](#)
 - [Kimsuky group](#)
 - [UAC-0165](#)



Insights

Jasmin

ransomware, deployed by leveraging JetBrains TeamCity vulnerabilities

DEEP#GOSU

A multi-stage attack campaign linked to the North Korean Kimsuky group, using PowerShell and VBScript stagers to infiltrate systems discreetly

BunnyLoader3.0

a MaaS that has been steadily evolving with new features and updates

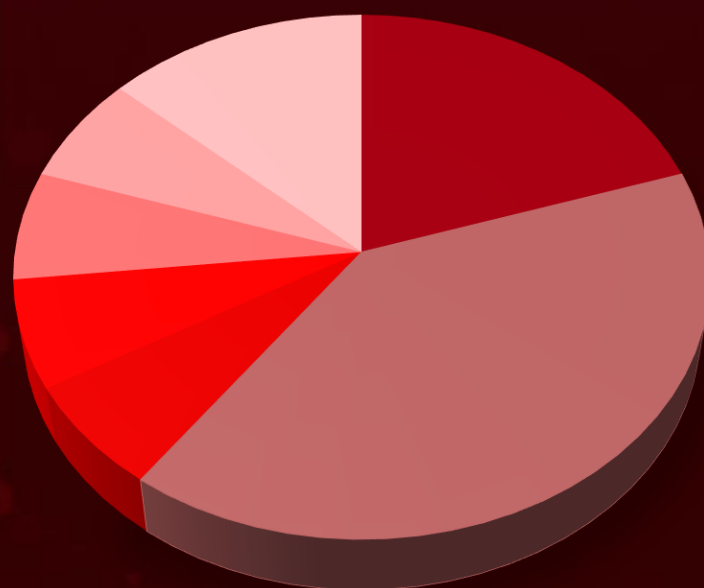
Earth Krahang, exploiting vulnerabilities in public-facing servers, in a campaign since 2022, targeting global government entities, employing spear phishing and server exploitation tactics

CVE-2024-2172 A critical security vulnerability in WordPress, urging users utilizing miniOrange's Malware Scanner and Web Application Firewall plugins to uninstall them from their websites.

Operation PhantomBlu

deploying NetSupport RAT By utilising OLE template manipulation

Threat Distribution



■ Backdoor ■ RAT ■ Modular ■ Stealer ■ Ransomware ■ Miner ■ Wiper

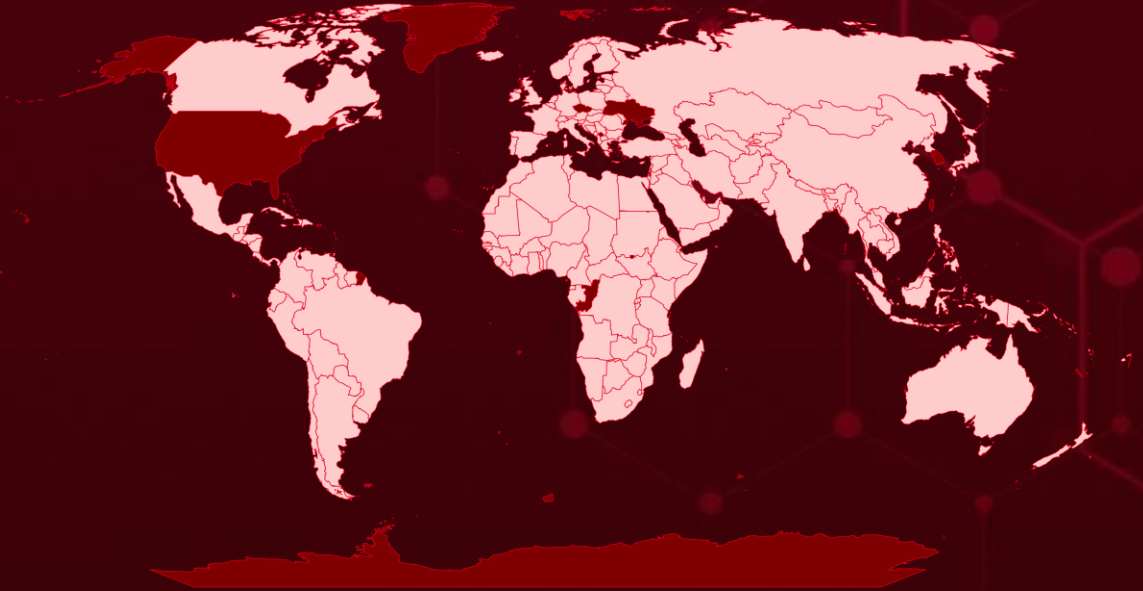


Targeted Countries

Most



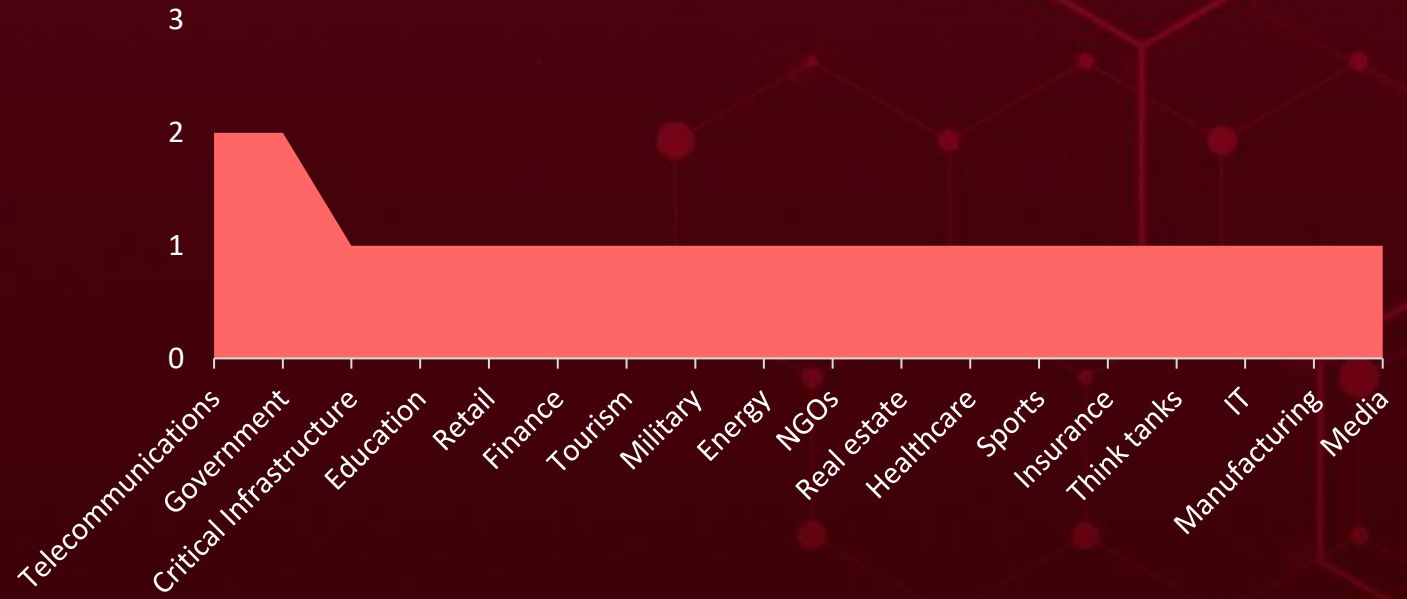
Least



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

Countries	Countries	Countries	Countries
South Korea	Malawi	Burkina Faso	Seychelles
Ukraine	Barbados	Maldives	Costa Rica
United States	Mexico	Burundi	Slovenia
Oman	Belarus	Mauritania	Côte d'Ivoire
Liechtenstein	Myanmar	Cabo Verde	Albania
Spain	Belgium	Moldova	Croatia
Angola	Nigeria	Cambodia	St. Vincent & Grenadines
Mongolia	Belize	Morocco	Cuba
Antigua and Barbuda	Papua New Guinea	Cameroon	Sweden
Samoa	Benin	Nauru	Cyprus
Argentina	Russia	Canada	Tanzania
Tunisia	Bhutan	Nicaragua	Czech Republic (Czechia)
Armenia	Senegal	Central African Republic	Tonga
Malta	Bolivia	North Macedonia	Denmark
Australia	Somalia	Chad	Turkmenistan
Netherlands	Bosnia and Herzegovina	Palau	Djibouti
Austria	Sudan	Chile	United Arab Emirates
Poland	Botswana	Peru	Dominica
Azerbaijan	Timor-Leste	China	Vietnam
Singapore	Brazil	Qatar	Dominican Republic
Bahamas	Uganda	Colombia	Afghanistan
Syria	Brunei	Saint Kitts & Nevis	DR Congo
Bahrain	Zambia	Comoros	Lithuania
Vanuatu	Bulgaria	Sao Tome & Principe	
Bangladesh	Luxembourg	Congo	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1190

Exploit Public-Facing Application

T1059.001

PowerShell

T1083

File and Directory Discovery

T1140

Deobfuscate/Decode Files or Information

T1082

System Information Discovery

T1588.006

Vulnerabilities

T1573

Encrypted Channel

T1567

Exfiltration Over Web Service

T1486

Data Encrypted for Impact

T1027

Obfuscated Files or Information

T1115

Clipboard Data

T1041

Exfiltration Over C2 Channel

T1212

Exploitation for Credential Access

T1047

Windows Management Instrumentation

T1566

Phishing

T1053.00

5
Scheduled Task

T1113

Screen Capture

T1056

Input Capture

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RESHELL</u>	<p>A simple .NET backdoor used in the initial stages of the attack. It is capable of collecting information, dropping files, or executing system commands. Its binaries are packed with ConfuserEX, and communication is encrypted with AES algorithm.</p>	Exploiting Vulnerabilities, Phishing	CVE-2023-32315 CVE-2022-21587
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Steal Data	Ignite Realtime Openfire, Oracle E-Business Suite
ASSOCIATED ACTOR			PATCH LINK
Earth Krahang and Earth Lusca			https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm , https://www.oracle.com/security-alerts/cpuoct2022.html
IOC TYPE	VALUE		
SHA256	1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c, 36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1, 46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2, 4cb020a66fdbbc99b0bce2ae24d5684685e2b1e9219fbd9da56b3aace4e8d5f66		

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>Xdealer</u> (<u>DinodasRAT</u>)	<p>It provides extensive backdoor capabilities and is available in both Windows and Linux versions. It is capable of taking screenshots, stealing clipboard data, and logging keystrokes. It can be delivered as DLL files packaged with an installer or as standalone executables.</p>	Exploiting Vulnerabilities, Phishing	CVE-2023-32315 CVE-2022-21587
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Steal Data	Ignite Realtime Openfire, Oracle E-Business Suite
ASSOCIATED ACTOR			PATCH LINK
Earth Krahang and Earth Lusca			https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm , https://www.oracle.com/security-alerts/cpuoct2022.html
IOC TYPE	VALUE		
SHA256	10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f, 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1, 1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3		

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
PlugX	<p>It is used for side-loading similar to the Cobalt Strike routine. It is capable of providing remote access to the compromised system.</p>	Exploiting Vulnerabilities	CVE-2023-32315 CVE-2022-21587
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote access	Ignite Realtime Openfire, Oracle E-Business Suite
ASSOCIATED ACTOR			PATCH LINK
Earth Krahang and Earth Lusca			https://github.com/ignite realtime/Openfire/security/advisories/GHS-A-gw42-f939-fhvm , https://www.oracle.com/security-alerts/cpuoct2022.htm !
IOC TYPE	VALUE		
SHA256	42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShadowPad	<p>ShadowPad is used for remote access and data exfiltration.</p>	Exploiting Vulnerabilities	CVE-2023-32315 CVE-2022-21587
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Steal data	Ignite Realtime Openfire, Oracle E-Business Suite
ASSOCIATED ACTOR			PATCH LINK
Earth Krahang and Earth Lusca			https://github.com/ignite realtime/Openfire/security/advisories/GHS-A-gw42-f939-fhvm , https://www.oracle.com/security-alerts/cpuoct2022.htm
IOC TYPE	VALUE		
SHA256	0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9		

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>TutClient</u>	The TutClient RAT is coded in C# and is open source and available to download through various platforms.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Steal Data	Windows
Kimsuky group			PATCH LINK
		-	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>TutRAT</u>	TutRAT is basically a PowerShell script. It has capabilities to record keystrokes, manage files, and facilitate remote control.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Steal Data	Windows
Kimsuky group			PATCH LINK
		-	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>xRAT</u>	xRAT is a remote access Trojan that includes extensive data collection capabilities and is associated with known mobile and Windows-targeting threats. It specifically developed to target political groups. It includes detection evasion and implements common spying features, including the ability to gather data from instant messaging applications.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Steal Data	Windows
Kimsuky group			PATCH LINK
		-	
IOC TYPE	VALUE		
SHA256	ef43b756295b1499b8fa6a9dd04bfd1f81e9bb4793d44a17e24d0b9a36ad5ec9		

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>NetSupport RAT</u>	NetSupport RAT is based on NetSupport Manager, a legitimate tool which is frequently used by actors for malicious purposes. NetSupport Manager, used maliciously or otherwise, provides full and complete control over the target device. Once the client has been installed, attackers can access, acquire, and manipulate any data on the device.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			-
ASSOCIATED ACTOR		Data Theft	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	fef8bdf50c19a012bfdc9da3f4ea4cab39075637ca527f24af79575007b2befe, 6600d29e025b7d8d8d6d8f472685b9f800e3418200fde2350f5c30a18aa34816, f17ffde17327433256debb5f6eb3b1a29cecf79af7565861182b4a684b8c936		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BunnyLoader 3.0</u>	The third generation of BunnyLoader is incorporating new denial-of-service (DoS) features to mount HTTP flood attacks against a target URL, but also splitting its stealer, clipper, keylogger, and DoS modules into distinct binaries.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular			Windows
ASSOCIATED ACTOR		Data Theft	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8, c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a		

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>AsukaStealer</u>	AsukaStealer, crafted in C++, boasts adaptable configurations and a user-friendly web-based interface, designed to harvest data from various sources.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			-
ASSOCIATED ACTOR		Data Theft	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	24bb4fc117aa57fd170e878263973a392d094c94d3a5f651fad7528d5d73b58a, 00cc1ef3d307750d5cdbc537da606101e90091b6020c71f696e454aee11c9a98, 5b2b8a4d5b8375a3ac2ce68b93cdbcfd8fd13d1cf4ea1a6a61bd784aa495dbfb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Jasmin Ransomware</u>	Jasmin ransomware gets its name from the extension it appends to encrypted files, typically ".jasmin". It distribute a ransom note named un-lock your files.html.	Exploiting Vulnerabilities	CVE-2024-27198 CVE-2024-27199
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			TeamCity On-Premises
ASSOCIATED ACTOR		Data Theft, Encrypt data	PATCH LINK
-			https://www.jetbrains.com/teamcity/download/
IOC TYPE	VALUE		
SHA256	56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a, 32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64		

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>	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.	Exploiting Vulnerabilities	CVE-2024-27198 CVE-2024-27199	
TYPE		IMPACT	AFFECTED PRODUCTS	
Miner				
ASSOCIATED ACTOR				TeamCity On-Premises
-				PATCH LINK
		Mining cryptocurrencies	https://www.jetbrains.com/teamcity/download/	
IOC TYPE	VALUE			
SHA256	7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b,01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>SparkRAT</u>	It is an open-source Golang based backdoor. SparkRAT is a feature-rich and multi-platform tool that supports the Windows, Linux, and macOS operating systems. SparkRAT uses the WebSocket protocol to communicate with the C2 server and features an upgrade system.	Exploiting Vulnerabilities	CVE-2024-27198 CVE-2024-27199	
TYPE		IMPACT	AFFECTED PRODUCTS	
Backdoor				
ASSOCIATED ACTOR				TeamCity On-Premises
-				PATCH LINK
		Data Theft	https://www.jetbrains.com/teamcity/download/	
IOC TYPE	VALUE			
SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697			




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>AcidPour</u>	AcidPour is a variant of AcidRain. AcidPour is a new Linux wiper. It is an ELF binary compiled for x86 architecture. AcidPour's capabilities enables it to better disable embedded devices including networking, IoT, large storage (RAIDs), and possibly ICS devices running Linux x86 distributions.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Wiper			
ASSOCIATED ACTOR		System Compromise	Linux
UAC-0165			PATCH LINK
		-	
IOC TYPE	VALUE		
IP	185[.]61[.]137[.]155		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AcidRain</u>	AcidRain is malware designed to wipe modems and routers. It performs an in-depth wipe of the filesystem and various known storage device files.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Wiper			
ASSOCIATED ACTOR		System Compromise	Linux
UAC-0165			PATCH LINK
		-	
IOC TYPE	VALUE		
SHA256	6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728		




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-2024-2172</u>		Malware Scanner: Versions <= 4.7.2, Web Application Firewall: Versions <= 2.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wordpress:MalwareScanner:*:*:*:*:*:* cpe:2.3:a:wordpress:WebApplicationFirewall:*:*:*:*:*:*	-
WordPress Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-280	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	Uninstall the plugins




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-32315</u>		Ignite Realtime Openfire	Earth Krahang and Earth Lusca
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad
Ignite Realtime Openfire Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-21587</u>		Oracle E-Business Suite	Earth Krahang and Earth Lusca
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:oracle:e-business_suite:*:*:*:*:*:* *	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad
Oracle E-Business Suite Unspecified Vulnerability			ASSOCIATED TTPs
	CWE ID	CWE-306	T1588.006: Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-23334</u>		aiohttp: Prior to version 3.9.2	ShadowSyndicate
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:aiohttp:aiohttp:*:* .*.*.*.*.*.*	-
Aiohttp Directory Traversal Vulnerability			ASSOCIATED TTPs
	CWE ID	CWE-22	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-41724</u>		Ivanti Standalone Sentry	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:standalonesentry:*:*:*:*:*	-
Ivanti Standalone Sentry Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1588.006: Vulnerabilities, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://help.ivanti.com/mi/help/en_us/SNTRY/9.x/rn/RelnotesStandaloneSentry/Software_download_%20for_Standalone%20Sentry.htm

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-27198</u>		TeamCity On-Premises	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*	Jasmin ransomware, XMRig, SparkRAT backdoor
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	https://www.jetbrains.com/teamcity/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-27199</u>		TeamCity On-Premises	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*. *.*.*.*.*.*.*.*	Jasmin ransomware, XMRIg, SparkRAT backdoor
JetBrains TeamCity Path Traversal Vulnerability			
	CWE ID	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://www.jetbrains.com/teamcity/download/
	CWE-23		


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-1597</u>		Bamboo Data Center and Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:postgresql:postgresql_jdbc_driver:*. *.*.*.*.*.*.*.*.*	-
Atlassian Bamboo Data Center and Server SQL injection Vulnerability			
	CWE ID	T1190: Exploit Public-Facing Application, T1565: Data Manipulation	https://www.atlassian.com/software/bamboo/download-archives
	CWE-89		

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Earth Krahang	China	Government, Education, Telecommunications, Finance, Insurance, Foundations, NGOs, Think tanks, Healthcare, IT, Manufacturing, Media, Military, Real estate, Retail, Sports, and Tourism	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-32315 CVE-2022-21587	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad	Ignite Realtime Openfire, Oracle E-Business Suite


TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.001: Domains; T1583.003: Virtual Private Server; T1586.002: Email Accounts; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1586: Compromise Accounts; T1583: Acquire Infrastructure; T1588.001: Malware; T1588.003: Code Signing Certificates; T1608.001: Upload Malware; T1608.002: Upload Tool; T1588: Obtain Capabilities; T1608.005: Link Target; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link T1595.001: Scanning IP Blocks; T1595.002: Vulnerability Scanning; T1595.003: Wordlist Scanning; T1592: Gather Victim Host Information; T1566: Phishing; T1059.006: Python; T1203: Exploitation for Client Execution; T1569.002: Service Execution; T1569: System Services; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1543.003: Windows Service T1133: External Remote Services; T1053.005: Scheduled Task; T1505.003: Web Shell; T1068: Exploitation for Privilege Escalation; T1078.003: Local Accounts; T1140: Deobfuscate/Decode Files or Information; T1574.002: DLL Side-Loading; T1656: Impersonation; T1036.005: Match Legitimate Name or Location; T1036.007: Double File Extension; T1112: Modify Registry; T1110.003: Password Spraying; T1003.001: LSASS Memory; T1003.002: Security Account Manager; T1539: Steal Web Session Cookie; T1087.001: Local Account; T1087.002: Domain Account; T1069.002: Domain Groups; T1057: Process Discovery; T1033: System Owner/User Discovery; T1007: System Service Discovery; T1210: Exploitation of Remote Services; T1534: Internal Spearphishing; T1021.006: Windows Remote Management; T1021: Remote Services; T1119: Automated Collection; T1114: Email Collection; T1071.001: Web Protocols; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1020: Automated Exfiltration; T1199: Trusted Relationship; T1078: Valid Accounts; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1590: Gather Victim Network Information

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p>Earth Lusca (aka Bronze University, Chromium, Charcoal Typhoon, Red Dev 10, Red Scylla)</p>	China	Casinos and Gambling, Education, Government, Media, telecommunications and Covid-19 research organizations, religious movements that are banned in Mainland China, pro-democracy and human rights political organizations and various cryptocurrency trading platforms	Worldwide
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
CVE-2023-32315 CVE-2022-21587	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad	Ignite Realtime Openfire, Oracle E-Business Suite	


TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.001: Domains; T1583.003: Virtual Private Server; T1586.002: Email Accounts; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1586: Compromise Accounts; T1583: Acquire Infrastructure; T1588.001: Malware; T1588.003: Code Signing Certificates; T1608.001: Upload Malware; T1608.002: Upload Tool; T1588: Obtain Capabilities; T1608.005: Link Target; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link T1595.001: Scanning IP Blocks; T1595.002: Vulnerability Scanning; T1595.003: Wordlist Scanning; T1592: Gather Victim Host Information; T1566: Phishing; T1059.006: Python; T1203: Exploitation for Client Execution; T1569.002: Service Execution; T1569: System Services; T1204.002: Malicious File; T1047: Windows Management Instrumentation; T1543.003: Windows Service T1133: External Remote Services; T1053.005: Scheduled Task; T1505.003: Web Shell; T1068: Exploitation for Privilege Escalation; T1078.003: Local Accounts; T1140: Deobfuscate/Decode Files or Information; T1574.002: DLL Side-Loading; T1656: Impersonation; T1036.005: Match Legitimate Name or Location; T1036.007: Double File Extension; T1112: Modify Registry; T1110.003: Password Spraying; T1003.001: LSASS Memory; T1003.002: Security Account Manager; T1539: Steal Web Session Cookie; T1087.001: Local Account; T1087.002: Domain Account; T1069.002: Domain Groups; T1057: Process Discovery; T1033: System Owner/User Discovery; T1007: System Service Discovery; T1210: Exploitation of Remote Services; T1534: Internal Spearphishing; T1021.006: Windows Remote Management; T1021: Remote Services; T1119: Automated Collection; T1114: Email Collection; T1071.001: Web Protocols; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1020: Automated Exfiltration; T1199: Trusted Relationship; T1078: Valid Accounts; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1590: Gather Victim Network Information

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ShadowSyndicate	-	All	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-23334	-	Aiohttp
TTPs			
TA0002: Execution; TA0042: Resource Development; TA0007: Discovery; TA0003: Persistence; TA0010: Exfiltration; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1588: Obtain Capabilities; T1082: System Information Discovery; T1588.002: Tool; T1587.004: Exploits; T1567: Exfiltration Over Web Service; T1083: File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses	Japan, South Korea, Thailand, USA and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	TutClient, TutRAT, and xRAT	Windows

TTPs			
TA0007: Discovery; TA0005: Defense Evasion; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0011: Command and Control; TA0009: Collection; T1132: Data Encoding; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1070.004: File Deletion; T1140: Deobfuscate/Decode Files or Information; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1059: Command and Scripting Interpreter; T1567: Exfiltration Over Web Service; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1102: Web Service; T1132.001: Standard Encoding; T1219: Remote Access Software; T1573: Encrypted Channel; T1115: Clipboard Data; T1056.001: Keylogging; T1056: Input Capture; T1204: User Execution; T1070: Indicator Removal; T1059.001: PowerShell; T1059.005: Visual Basic; T1204.001: Malicious Link; T1567.002: Exfiltration to Cloud Storage			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>UAC-0165</u>	Russia	Telecommunications, Critical Infrastructure, Energy, and Government	Ukraine
	MOTIVE Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	AcidPour, AcidRain	-
TTPs			
TA0040: Impact; TA0005: Defense Evasion; T1486: Data Encrypted for Impact; T1529: System Shutdown/Reboot; T1495: Firmware Corruption; T1070.004: File Deletion; T1070: Indicator Removal; T1498: Network Denial of Service; T1489: Service Stop; T1561: Disk Wipe			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actors **Earth Krahang, Earth Lusca, ShadowSyndicate, Kimsuky group, UAC-0165** and malware **RESHELL, Xdealer, PlugX, ShadowPad, TutClient, TutRAT, xRAT, NetSupport RAT, BunnyLoader 3.0, AsukaStealer, Jasmin ransomware, XMRig, SparkRAT, AcidPour, AcidRain**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Earth Krahang, Earth Lusca, ShadowSyndicate, Kimsuky group** and malware **Xdealer, RESHELL, TutClient, TutRAT, xRAT, NetSupport RAT, BunnyLoader 3.0, AsukaStealer** in Breach and Attack Simulation(BAS).

Threat Advisories

[Critical Flaw In WordPress Plugins Poses Risk Of Site Takeover](#)

[Earth Krahang APT Campaign Targeting Governments Globally](#)

[Aiohttp Vulnerability Leveraged by ShadowSyndicate](#)

[The Evolution of DEEP#GOSU Attack Campaign by Kimsuky Group](#)

[Operation PhantomBlu Deploys NetSupport RAT via OLE Template](#)

[Unveiling BunnyLoader 3.0 Enhanced Malware Capabilities](#)

[From Observer to Asuka - The Reinvention of Stealer](#)

[Critical Flaw In Ivanti Standalone Sentry Leads To Remote Code Execution](#)

[TeamCity Vulnerabilities Unleash Jasmin Ransomware and More](#)

[Unveiling AcidPour Evolution of Destructive Malware Targeting Ukraine](#)

[Critical SQL Injection Vulnerability Discovered in Atlassian Bamboo](#)

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>RESHELL</u>	SHA256	1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c, 36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1, 46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2, 4cb020a66fdb99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66, 67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355, 6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716, 804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3, 82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846, b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a, da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577, f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb
<u>XDealer</u>	SHA256	10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f, 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1, 1e278cfe8098f3bade5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3,

Attack Name	TYPE	VALUE
<u>XDealer</u>	SHA256	<p>244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a, 35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa, 3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815, 50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab, 57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829, 5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe, 6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2, 898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fc9b75afc34dce, c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c, d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578, d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3, e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213, e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36, ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272, 2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa, 8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d, 2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee, 521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a, 9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1, 9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82, bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4, d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b, fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39, 01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c, 05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243,</p>

Attack Name	TYPE	VALUE
<u>XDealer</u>	SHA256	<p>241737842eb17676b3603e2f076336b7bc6304accefc3057401264afb963bef8, 5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472, b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab, c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab, f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac, acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2, ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d, ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e, ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136, 4b653253049a65142f827706203de55f03abccbcdac3ed2171d79bf8186eda9, 63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d, 6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64, f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934, 992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e, bb6afc28d610bfdcd0cf3497c152c081f63137fea9914a1fd461a0706c74288, 15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45, 6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2, 98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541, a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91, bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff, ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e</p>
<u>PlugX</u>	SHA256	<p>42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956, 44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448, d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519,</p>

Attack Name	TYPE	VALUE
<u>ShadowPad</u>	SHA256	0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9, 4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014, 484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0
<u>NetSupport RAT</u>	SHA256	fef8bdf50c19a012bfdc9da3f4ea4cab39075637ca527f24af79575007b2befe, 6600d29e025b7d8d8d6d8f472685b9f800e3418200fde2350f5c30a18aa34816, f17ffde17327433256debb5f6eb3b1a29cecf79af7565861182b4a684b8c936
<u>BunnyLoader 3.0</u>	SHA256	1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8, c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
<u>AsukaStealer</u>	MD5	2d2b66d90495c1236f2e557172bf0f1c, 7ce0bd101d349bc88b668e380093e1a9, e9dda8ccde5385e8d0a7f0bdc361e51d, 28b7d6b0a793d772c953f529742ca91f, 9ce2a046a0698212c2963f2df91ff2e1, 20017810fba85ef8ac6e4230d0e67a07, 371e14f7e146ff22cb9ebe2f78cbfb7f, 1494c8bc32576cb008c33d6f0fd1e842, 75c79796fa147bf3f4d569b544ee0547, 2de37ffcae86c673de3cd2ee5e2ad3b1
	SHA1	a06d203ae9cbe26a3c2e389f1c361ac49ef54c08, 45fc72df60f39ebe77d4012f34a10e73eb2fd485, 863734caf0cb94dce610fe49eebe438a7096dfb, fc33fe3deb280d9ed94e3add58134660433bdb18, 69a2d82f13246761e6d5159efb78b8fa91856380, d7b6530a4c7d685e9ee6765231bab14fecdadeba, 2fde663b31a46e83f3034464674ad3f3a85f6972, 4b3cdfbeaa9f8dc3554a0f9a54fc0d16334a46ed, 5c6a4cd4b9271410cc45ccda00a2531631f35136, 09f2187f0228eed3df41c76c69d94da789c0f2f1
	SHA256	24bb4fc117aa57fd170e878263973a392d094c94d3a5f651fad7528d5d73b58a, 00cc1ef3d307750d5cdbe537da606101e90091b6020c71f696e454ae11c9a98, 5b2b8a4d5b8375a3ac2ce68b93cbbfcd8fd13d1cf4ea1a6a61bd784aa495dbfb, 5f2016f22935cea6fa5eafe1e185d6a9b4c14c4b2aa8619ec15a539358cac928, 6b0e95d68da6d029a4af645a408c0608218e853f11c8ba70a14b06ec2a005424, 9ac629ed8e07b6c99b05edd46b86e1795e5f96908ab1fe85a06282b0a982cd1b,

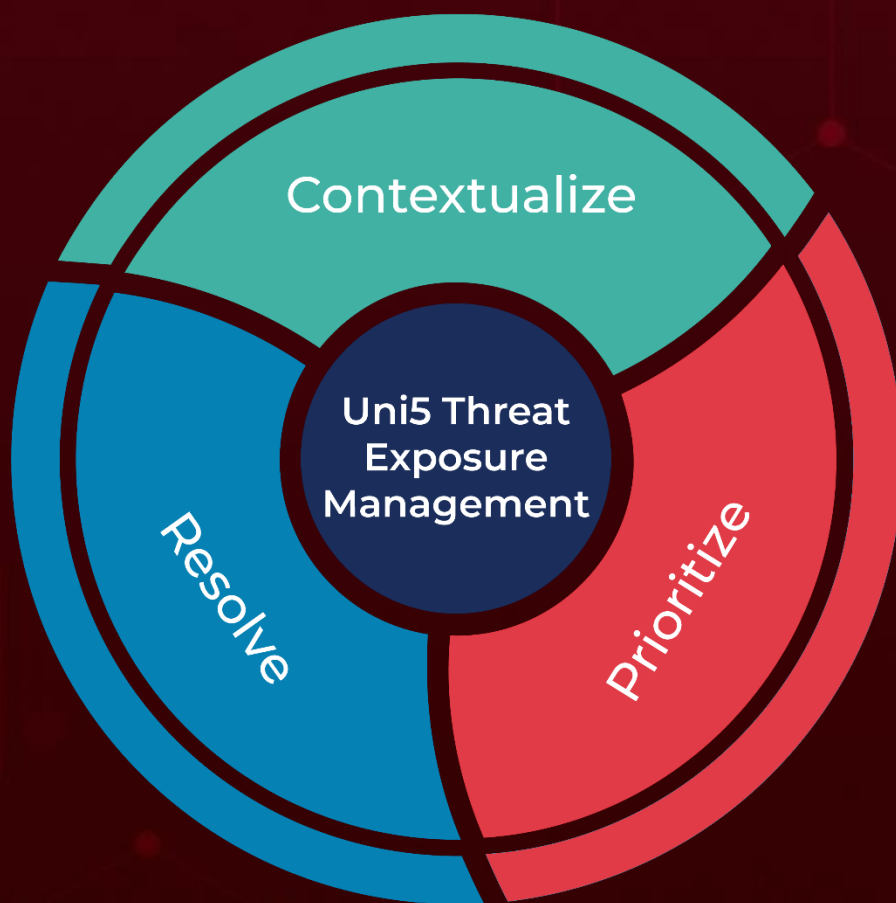
Attack Name	TYPE	VALUE
<u>AsukaStealer</u>	SHA256	bb17d47f10fefcee4c883f93f2989e753b969298dd70262ae00696d d482dc9b4, c534f184b8ea3887161ec2b364de15e61ee9a4053f8902450383d3f 4165fc818, dc723d302340d27529b8c3c880b4cf53534a02e2a71a68f39eec30f 239c2c988, e6430183aa7bbaffa89ffbef7bfac3aa54481e904556ab71ea20ccf55 dfce53f,
<u>AsukaStealer</u>	SHA256	0e5470a33fd87b813ecf72370f9e1f491515c12f41c8ea3c7bbc169a c56acda5, 476171dd2eb7f118d3e0aff32b7264d261ba4c2d9fa6c14ccff6d8d9 9b383db4
<u>Jasmin ransomware</u>	SHA256	56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a 0654f17b1a, 32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4a a384bf64
<u>XMRig</u>	SHA256	7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa6 81befe8c7b, 01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e24627 9f6ca61
<u>SparkRAT</u>	SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe 326e00697
<u>AcidRain</u>	MD5	1bde1e4ecc8a85cffe1cd4e5379aa44
	SHA1	b5de486086eb2579097c141199d13b0838e7b631
	SHA256	6a8824048417abe156a16455b8e29170f8347312894fde2aabe644 c4995d7728
<u>AcidPour</u>	IP	185[.]61[.]137[.]155
	Domains	solntsepek[.]com, solntsepek[.]info, solntsepek[.]org, solntsepek[.]ru
<u>xRAT</u>	SHA256	ef43b756295b1499b8fa6a9dd04bfd1f81e9bb4793d44a17e24d0b9 a36ad5ec9, 91ef2b2e677a31da2c612928fe4f8739cc5a480a6b6249c085a8ed9 ec8d8b0aa, fe347fb042b7e6317a8ff943e6019233bbae119d13028617c72e62d bfbad49f4, bf82a1616a1f282b948701e5f2fb63bae085ae39b7eb02921672aeb d252ef556, 8a87018ee3dea100ad87628ca9c895b5450b1ea405dbbceb9746c6 8ba514607b, db377e4193c8c1fd0d3ebffab816b1e3fdffd40fdd46378de7f5584c 164010ff, e76ffc328b95e3117f5b34bf10925b4afcac6dd2c21a67bc736c9249 9e670a25,

Attack Name	TYPE	VALUE
<p>xRAT</p>	<p>SHA256</p>	<p>9f2ed0f3f8a657063c12f442541e4130fd51bfa096fc1fe1809ec6b74b5ba2a0, a41e196cc8e426b7f3100e3683e0adfca4c6db99155d47f7ad035a522e9dd38a, 53cace88c1271c20edd6a445b1ee093c57678cd8c77ba0c7f117eb8bc0cff689, f39a48abb806b47dbc417775c18096c6a9131bf049a33c4b5f441c7a38ddf9b6, 0571e73e271c55ebaee39339c519d7263479f05ee2940ebef8a8f66f8e744c64, e7a3902c6bc36da4d9b75973790ae9b1b868ee10e07ba1443e8c893b70d41b16, bfd43fe95304c3ee54a74c00bac1e4a3cdd198ba2ca26345290fb1f6f7bbee8c, 3872dd2093334f00b3bedb4e9816934549f1dd0274cc8f6c31eb93f2b885acca, d150b62c99bb028179fda24cc176486817b4c38366ef132dea6b5b23d02d4ff6, ecb3e3068a9118565b6d18eb2e6533b327cbc2b90a2ad466e372a6d4eddc508d, 19ad3b30384fa1bc38095d1e0a46811cfef1f6d0b145f764cb048d2d72be57d3, 13b3b9ad32e283f54f4339d0d4849796003f1fd7cdd2f83c419b07e953758b1a, 71003754ffab0ae9d10ad27e290fa9317d377bc32403c3ab08e3c740069b5780, 71e4d35156e913340d32d565806004c2297bfbc05b747874279830e34056dbce, 9126b515fbd12299376087ce4ad5eb17570ce77f851abf7244756a2798a3bccb, 9d5f67efc28610cfa459199076c3580c6370d3b74526318b663429c2e9c08d87, 726b67b85e531994ac728d9dbc6c412208a1db0bcde5f29e8f58841b05c81429, f26e49e9ee43830c241200161ca59ddec1ac840745ce73a3d9163c190f41824c, 3becd141d8cc82cf81b106864a37f2e21d1f55d7d6a88af450aa5564245129da, b18b9fd76d06b0221f087447f2220d5e275814e460d36c7ce5b13937adf4c2a6, 7aca9b72f131a601f825051068927625e294b5f38dce44530c4cc68cc178662a, d2b79474e38f3a760729e3f5008febad36c81376ffd74234b5eef3b462f63e87, c38957198bc36ebfa50505e4089d324e857cbf63aab6b09b8f864f1d14ebfc31, b75d1f664da0541ce2d77fbfc31c653eba13fbf136a456eefe5ef417f0ff6f05, 6ea913e13d4e76ddcc6fa3b24feb283e165093d57fd6649fbcaa33fb14a6f7d3, 06091017eef3ee19006a38e4d966e2b0fb9dc359aa2d500edaa98c6b228ea3bd, 607f36b00f244eaede1939dee34708925c383b5c0a9934a95e801d2f539aea77</p>

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

March 25, 2024 • 7:20 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com