

Date of Publication  
April 1, 2024



HiveForce Labs

MONTHLY

# THREAT DIGEST

**Vulnerabilities, Attacks, and Actors**

MARCH 2024

# Table Of Contents

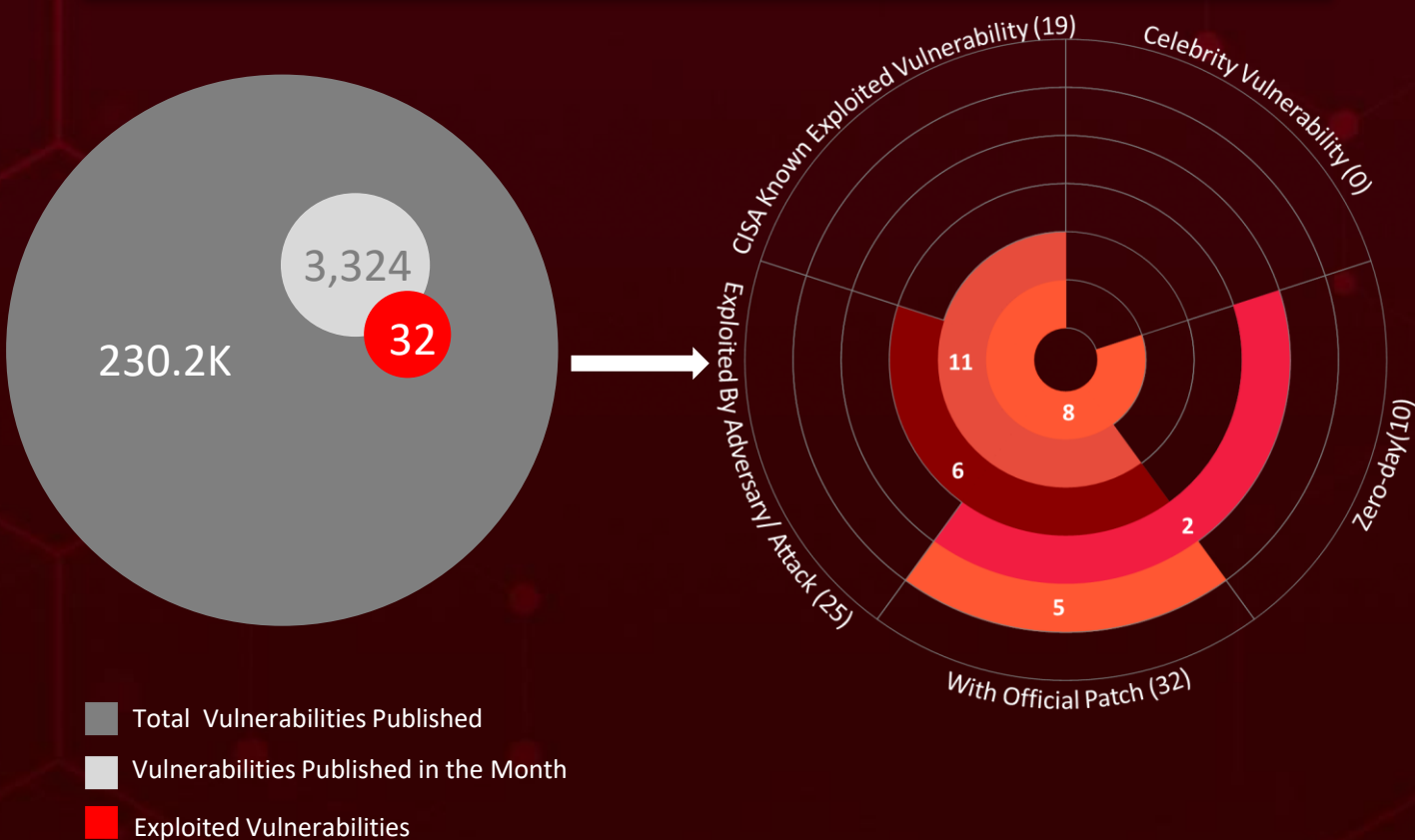
<u>Summary</u> .....	03
<u>Insights</u> .....	04
<u>Threat Landscape</u> .....	05
<u>Vulnerabilities Summary</u> .....	06
<u>Attacks Summary</u> .....	10
<u>Adversaries Summary</u> .....	14
<u>Targeted Products</u> .....	16
<u>Targeted Countries</u> .....	18
<u>Targeted Industries</u> .....	19
<u>Top MITRE ATT&amp;CK TTPs</u> .....	20
<u>Top Indicators of Compromise (IOCs)</u> .....	21
<u>Vulnerabilities Exploited</u> .....	24
<u>Attacks Executed</u> .....	41
<u>Adversaries in Action</u> .....	62
<u>MITRE ATT&amp;CK TTPS</u> .....	73
<u>Top 5 Takeaways</u> .....	77
<u>Recommendations</u> .....	78
<u>Hive Pro Threat Advisories</u> .....	79
<u>Appendix</u> .....	80
<u>Indicators of Compromise (IoCs)</u> .....	81
<u>What Next?</u> .....	96

# Summary

In March, the cybersecurity landscape witnessed a surge in attention due to the discovery of **ten zero-day** vulnerabilities. The **GhostSec** and **Stormous** ransomware factions have launched a sophisticated campaign, introducing the **GhostLocker 2.0 ransomware** and the STMX\_GhostLocker ransomware-as-a-service (RaaS) initiative, posing a significant threat to businesses primarily in the Middle East.

During the same period, ransomware attacks experienced a noticeable uptick, with strains such as **GhostLocker**, **Stormous**, **Jasmin**, **Agenda**, and **Evil Ant** actively targeting victims. As ransomware continues to advance in sophistication, organizations are urged to fortify their defenses by implementing robust backup and disaster recovery strategies. Additionally, employee training to recognize and thwart phishing attacks is crucial.

In parallel, **thirteen** adversaries were active across diverse campaigns. **Magnet Goblin**, characterized by its financial incentives, strategically **exploits zero-day vulnerabilities** within publicly accessible services by employing sophisticated malware sourced from the **Nerbian** family. Their primary objectives included extracting user credentials and initiating subsequent malicious activities. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



## Operation PhantomBlu

deploying NetSupport RAT By utilizing OLE template manipulation

## DEEP#GOSU

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

## Earth Krahang

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

## Money Talks:

**Magnet Goblin's** Hunt for Zero-Day Vulnerabilities and its Strategic Malware Tactics

## Apple 0-days

CVE-2024-23225 and CVE-2024-23296 zero-day vulnerabilities were found in iOS, exploited in attacks targeting Mobile devices, providing attackers with arbitrary kernel read and write privileges

## 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.

## JetBrains TeamCity

CVE-2024-27198 and CVE-2024-27199 Threat actors exploiting these vulnerabilities to breach and gain control of the impacted systems

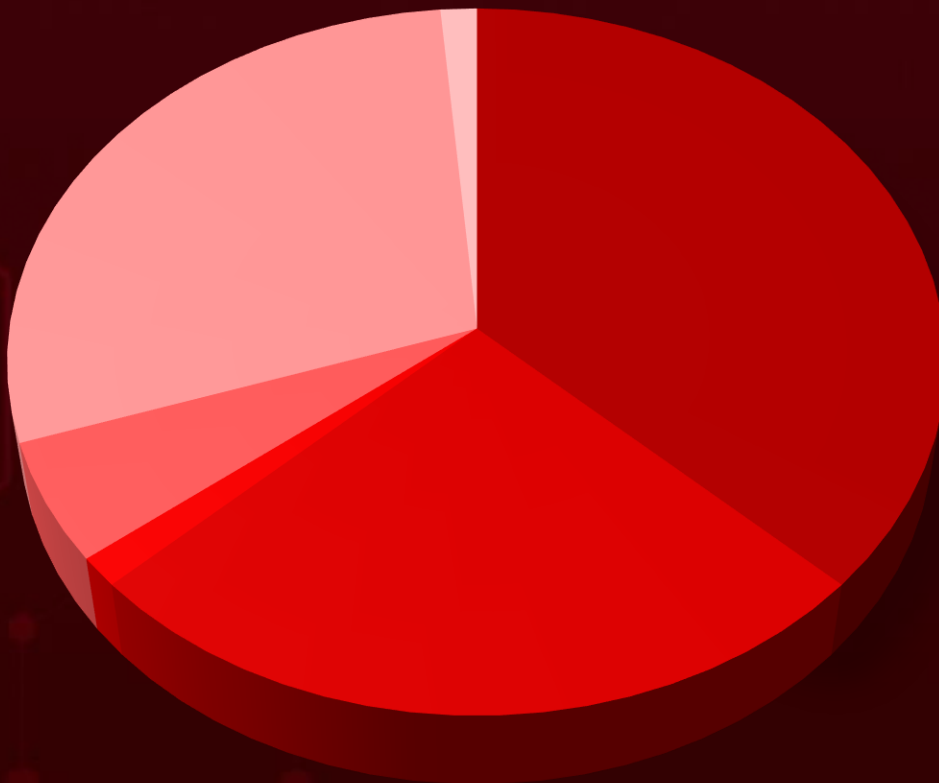
## Breaking Point:

Cisco's CVE-2024-20337 Vulnerability Threatens VPN Security

**In March 2024**, a geopolitical cybersecurity landscape unfolds, revealing the **United States, India, Egypt, Israel, Vietnam, and Hong Kong** as the top-targeted countries

Highlighted in **March 2024** is a cyber battleground encompassing the **Government, Finance, Energy, Defense, and Construction** sectors, designating them as the top industries

# Threat Landscape



- Malware Attacks
- Social Engineering
- Supply Chain Attacks
- Denial-of-Service Attack
- Injection Attacks
- Password Attack



# Vulnerabilities Summary
















CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	✓	✓	✓
CVE-2024-22024	Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways	✗	✗	✓
CVE-2024-21888	Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	✗	✗	✓
CVE-2024-27198	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity On-Premises versions upto 2023.11.3	✗	✓	✓
CVE-2024-23225	Apple iOS and iPadOS Memory Corruption Vulnerability	iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	✓	✓	✓
CVE-2024-23296	Apple iOS and iPadOS Memory Corruption Vulnerability	iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓
CVE-2024-20337	Cisco Secure Client Carriage Return Line Feed Injection Vulnerability	Cisco Secure Client: 4.10.04065 - 5.1	✗	✗	✓
CVE-2022-24086	Adobe Commerce and Magento OpenSource Improper Input Validation Vulnerability	Adobe Commerce and Magento Open Source	✓	✓	✓
CVE-2023-41265	Qlik Sense Enterprise Privilege escalation Vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-41266	Qlik Sense Enterprise path traversal Vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-48365	Qlik Sense Enterprise remote code Execution Vulnerability	Qlik Sense Enterprise for Windows	✗	✗	✓
CVE-2023-41724	Ivanti Standalone Sentry Remote Code Execution Vulnerability	Ivanti Standalone Sentry	✗	✗	✓
CVE-2024-27199	JetBrains TeamCity Path Traversal Vulnerability	TeamCity On-Premises	✗	✗	✓
CVE-2024-1597	Atlassian Bamboo Data Center and Server SQL injection Vulnerability	Bamboo Data Center and Server	✗	✗	✓



CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-2194	WordPress WP Statistics plugin Cross-Site Scripting Vulnerability	WordPress WP Statistics Plugin all versions up to 14.5			
CVE-2024-2172	WordPress Privilege Escalation Vulnerability	Malware Scanner: Versions <= 4.7.2, Web Application Firewall: Versions <= 2.1.1			
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Ignite Realtime Openfire			
CVE-2022-21587	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite			
CVE-2024-23334	Aiohttp Directory Traversal Vulnerability	aiohttp: Prior to version 3.9.2			
CVE-2017-9805	Apache Struts Deserialization of Untrusted Data Vulnerability	Apache Struts			
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Atlassian Confluence Data Center and Server			
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Data Center and Server			
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility			
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect			



CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-22518	Atlassian Confluence Improper Authorization Vulnerability	Confluence Data Center, Confluence Server			
CVE-2022-0185	Linux Kernel Vulnerability	FAS/AFF BMC, NetApp HCI BMC			
CVE-2022-30525	Zyxel Multiple Firewalls OS Command Injection Vulnerability	USG FLEX, ATP series, VPN series			
CVE-2024-2886	Google Chrome WebCodecs Use After Free Vulnerability	Google Chrome			
CVE-2024-2887	Google Chrome WebAssembly Type Confusion Vulnerability	Google Chrome			





# Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
MINIBIKE	Backdoor	-	-	-	Spear phishing and watering-hole attacks
MINIBUS	Backdoor	-	-	-	Spear phishing and watering-hole attacks
LIGHTRAIL	Tunneling	-	-	-	Spear phishing and watering-hole attacks
Bifrost (aka Bifrose)	RAT	-	Linux	-	Phishing
Pikabot	Loader	-	-	-	Malvertising
CHAVECLOAK	Trojan	-	Windows	-	Phishing
WogRAT	Backdoor	-	Windows and Linux	-	Via a Notepad
GhostLocker	Ransomware	-	-	-	Phishing
Stormous	Ransomware	-	-	-	Phishing
SapphireStealer	Info stealer	-	-	-	various public malware repositories
MgBot	Backdoor	-	-	-	Social Engineering
Nightdoor	Backdoor	-	-	-	Social Engineering
VCURMS	RAT	-	AWS and GitHub	-	Phishing
STRRAT	RAT	-	AWS and GitHub	-	Phishing
TimbreStealer	Information Stealer	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
NerbianRAT	RAT	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ		Exploiting Vulnerabilities
WARPWIRE	Information Stealer	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ		Exploiting Vulnerabilities
MiniNerbian	Backdoor	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ		Exploiting Vulnerabilities
RESHELL	Backdoor	CVE-2023-32315 CVE-2022-21587	Ignite Realtime Openfire, Oracle E Business Suite		Exploiting Vulnerabilities, Phishing
Xdealer	RAT	CVE-2023-32315 CVE-2022-21587	Ignite Realtime Openfire, Oracle E-Business Suite		Exploiting Vulnerabilities, Phishing
PlugX	RAT	CVE-2023-32315 CVE-2022-21587	Ignite Realtime Openfire, Oracle E-Business Suite		Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
ShadowPad	Backdoor	CVE-2023-32315 CVE-2022-21587	Ignite Realtime Openfire, Oracle E- Business Suite		Exploiting Vulnerabilities
TutClient	RAT	-	Windows	-	Phishing
TutRAT	RAT	-	Windows	-	Phishing
xRAT	RAT	-	Windows	-	Phishing
NetSupport RAT	RAT	-	-	-	Phishing
BunnyLoader 3.0	Modular	-	Windows	-	-
AsukaStealer	Stealer	-	-	-	-
Jasmin Ransomware	Ransomware	CVE-2024-27198 CVE-2024-27199	TeamCity On- Premises		Exploiting Vulnerabilities
XMRig	Miner	CVE-2024-27198 CVE-2024-27199 CVE-2017-9805 CVE-2023-22527 CVE-2021-26084	TeamCity On- Premises, Apache Struts, Atlassian Confluence		Exploiting Vulnerabilities
SparkRAT	Backdoor	CVE-2024-27198 CVE-2024-27199	TeamCity On- Premises		Exploiting Vulnerabilities
AcidPour	Wiper	-	Linux	-	-
AcidRain	Wiper	-	Linux	-	-
WINELOADER	Backdoor	-	Windows	-	Phishing emails
ROOTSAW	Dropper	-	Windows	-	Phishing emails
Evil Ant Ransomware	Ransomware	-	-	-	-
StreLaStealer	Information stealer	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Agenda ransomware	Ransomware	-	VMWare vCenter and ESXi servers	-	-
Sysrv Botnet	Botnet	CVE-2017-9805 CVE-2023-22527 CVE-2021-26084	Apache Struts, Atlassian Confluence		Exploiting network vulnerabilities
SNOWLIGHT	Dropper	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls		exploiting vulnerabilities
GOHEAVY	Hack Tool				
GOREVERSE	Backdoor				
SUPERSHELL	Hack Tool				
HackBrowserData	Information stealer	-	-	-	Slack channels

# Adversaries Summary











ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UTA0178	Information theft and espionage	-	CVE-2023-46805 CVE-2024-21887 CVE-2024-21893 CVE-2024-22024 CVE-2024-21888	-	Ivanti Connect Secure and Ivanti Policy Secure
UNC1549	Information theft and espionage	Affiliated to Iran	-	MINIBIKE, MINIBUS, LIGHTRAIL	-
TA577	Information Theft and Espionage	-	-	Pikabot	Windows
TA4903	Financial gain	-	-	-	-
Evasive Panda	Information theft and espionage	China	-	MgBot, Nightdoor	Windows and macOS
Magnet Goblin	Financial Gain	-	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893	NerbianRAT, WARPWIRE, MiniNerbian	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
Earth Krahang	Information theft and espionage	China	CVE-2023-32315 CVE-2022-21587	RESHELL, XDealer (Dinodas RAT), Cobalt Strike, PlugX, and Shadow Pad	Ignite Realtime Openfire, Oracle E-Business Suite

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Earth Lusca	Information theft and espionage, Financial gain	China	CVE-2023-32315 CVE-2022-21587	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad	Ignite Realtime Openfire, Oracle E-Business Suite
ShadowSyndicate	Information theft and espionage	-	CVE-2024-23334	-	Aiohttp
Kimsuky group	Information theft and espionage	North Korea	-	TutClient, TutRAT, and xRAT	Windows
UAC-0165	Information theft and espionage	Russia	-	AcidPour, AcidRain	-
APT29	Information theft and espionage	Russia	-	WINELOADER, ROOTSAW	Windows
UNC5174	Espionage	Affiliated to China	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





# Targeted Products

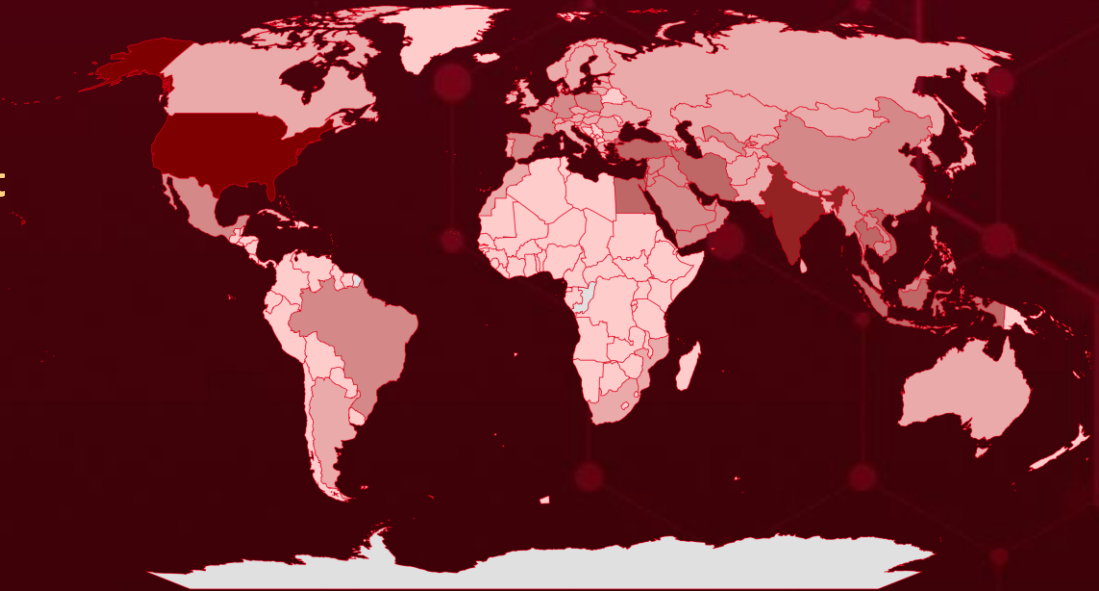
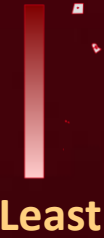
VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Application	Qlik Sense Enterprise for Windows
	Application	Adobe Commerce and Magento Open Source
	Application	Atlassian Confluence Data Center, Confluence Server, Bamboo Data Center and Server
	Application	Windows: 10 - 11 23H2, Windows Server: 2012 - 2022 23H2, Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018, Microsoft SharePoint Server: 2019, Microsoft SharePoint Server Subscription Edition: All versions, Microsoft SharePoint Enterprise Server: 2016
	Framework	Apache Struts
	Application	iPadOS: 17.4 and prior, 16.7.6 and prior, Apple iOS: 17.4 and prior, 16.7.6 and prior
	Application	TeamCity On-Premises
	Application	VMware ESXi- Before ESXi80U2sb-23305545 VMware Fusion: 13.x - 13.5, VMware Workstation: 17.x - 17.5
	Application	F5 BIG-IP Configuration Utility
	Software	ConnectWise ScreenConnect

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Security Appliance	USG FLEX, ATP series, VPN series
	Application	FortiClientEMS 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10, FortiOS version 7.4.0 through 7.4.1, FortiOS version 7.2.0 through 7.2.5, FortiOS version 7.0.0 through 7.0.12, FortiOS version 6.4.0 through 6.4.14, FortiOS version 6.2.0 through 6.2.15, FortiProxy version 7.4.0, FortiProxy version 7.2.0 through 7.2.6, FortiProxy version 7.0.0 through 7.0.12, FortiProxy version 2.0.0 through 2.0.13
	Browser	Google Chrome prior to 123.0.6312.86
	Application	Ivanti Standalone Sentry
	Application	Oracle E-Business Suite
	Application	Malware Scanner and Web Application Firewall Plugins, WordPress WP Statistics plugin
	Application	Cisco IOS XR Software: 7.3.2 - 7.10, 8000 Series Routers, IOS XRd Control Plane, IOS XRd vRouter, NCS 540 Series Routers, NCS 5700 Series Routers, Cisco IOS XR Software: 7.8 - 7.10 ASR 9000 Routers, ASR 9902 Routers ASR 9903 Routers, IOS XRd vRouters, IOS XRv 9000 Routers, Cisco IOS XR: 7.8 - 7.11, Cisco ASR 9000 Series Aggregation Services Routers: All versions, Cisco Secure Client



# Targeted Countries

Most



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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
Dark Red	United States	Dark Red	Saudi Arabia	Dark Red	Bhutan	Dark Red	Akrotiri and Dhekelia	Dark Red	North Korea
Dark Red	India	Dark Red	Cambodia	Dark Red	Albania	Dark Red	Croatia	Dark Red	Hungary
Dark Red	Egypt	Dark Red	Syria	Dark Red	Pakistan	Dark Red	Romania	Dark Red	Norway
Dark Red	Israel	Dark Red	China	Dark Red	Azerbaijan	Dark Red	Maldives	Dark Red	Lithuania
Dark Red	Vietnam	Dark Red	Malaysia	Dark Red	Finland	Dark Red	Estonia	Dark Red	Macao
Dark Red	Hong Kong	Dark Red	East Timor	Dark Red	Ireland	Dark Red	Malta	Dark Red	Sudan
Dark Red	Qatar	Dark Red	Myanmar	Dark Red	Switzerland	Dark Red	Slovakia	Dark Red	Saba
Dark Red	Taiwan	Dark Red	France	Dark Red	Italy	Dark Red	Cuba	Dark Red	Aruba
Dark Red	Thailand	Dark Red	Palestine	Dark Red	Armenia	Dark Red	South Africa	Dark Red	Guatemala
Dark Red	Cyprus	Dark Red	Germany	Dark Red	Japan	Dark Red	Mongolia	Dark Red	British Indian Ocean Territory
Dark Red	Turkey	Dark Red	Poland	Dark Red	Belgium	Dark Red	Georgia	Dark Red	Guernsey
Dark Red	Indonesia	Dark Red	Iraq	Dark Red	Bulgaria	Dark Red	Morocco	Dark Red	Gambia
Dark Red	Iran	Dark Red	Singapore	Dark Red	Russia	Dark Red	Sweden	Dark Red	Guinea
Dark Red	Lebanon	Dark Red	Jordan	Dark Red	Kazakhstan	Dark Red	Mozambique	Dark Red	Pitcairn Islands
Dark Red	Mexico	Dark Red	Spain	Dark Red	Slovenia	Dark Red	Austria	Dark Red	Guinea-Bissau
Dark Red	South Korea	Dark Red	Kuwait	Dark Red	Australia	Dark Red	Afghanistan	Dark Red	Samoa
Dark Red	Philippines	Dark Red	United Arab Emirates	Dark Red	Sri Lanka	Dark Red	Argentina	Dark Red	Guyana
Dark Red	Bahrain	Dark Red	Laos	Dark Red	Kyrgyzstan	Dark Red	Nepal	Dark Red	Falkland Islands
Dark Red	Uzbekistan	Dark Red	Yemen	Dark Red	Tajikistan	Dark Red	Ukraine	Dark Red	Haiti
Dark Red	Brazil	Dark Red	Portugal	Dark Red	Canada	Dark Red	Netherlands	Dark Red	Tanzania
Dark Red	Oman	Dark Red	Turkmenistan	Dark Red	Greece	Dark Red	United Kingdom	Dark Red	Heard Island and McDonald Islands
Dark Red	Brunei	Dark Red		Dark Red	Latvia	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Czech Republic	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Bangladesh	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Denmark	Dark Red		Dark Red	
Dark Red		Dark Red		Dark Red	Luxembourg	Dark Red		Dark Red	

# Targeted Industries

Most



Government



Financial



Energy



Defence



Construction



Manufacturing



Technology



Tele-communications



Banking



Real Estate



Aviation



Education



Healthcare



Retail



Utilities



Think-Tanks



Research Organizations



Transportation



Gaming



Hotels



Engineering



NGOs



Food products



Professional Services



Aerospace



Insurance



Legal



E-commerce



Media



Political Entities



Pharmaceutical

Least

# TOP 25 MITRE ATT&CK TTPS

## T1059

Command and Scripting Interpreter

## T1140

Deobfuscate/Decode Files or Information

## T1027

Obfuscated Files or Information

## T1566

Phishing

## T1588

Obtain Capabilities

## T1204.002

Malicious File

## T1036

Masquerading

## T1588.006

Vulnerabilities

## T1083

File and Directory Discovery

## T1190

Exploit Public-Facing Application

## T1204

User Execution

## T1082

System Information Discovery

## T1041

Exfiltration Over C2 Channel

## T1071.001

Web Protocols

## T1566.001

Spearphishing Attachment

## T1070

Indicator Removal

## T1057

Process Discovery

## T1574.002

DLL Side-Loading

## T1071

Application Layer Protocol

## T1059.001

PowerShell

## T1204.001

Malicious Link

## T1105

Ingress Tool Transfer

## T1573

Encrypted Channel

## T1055

Process Injection

## T1560

Archive Collected Data



# Top Indicators of Compromise (IOCs)




Attack Name	TYPE	VALUE
<u><a href="#">MINIBIKE</a></u>	MD5	01cbadd7a269521bf7b80f4a9a1982f, 054c67236a86d9ab5ec80e16b884f733, 1d8a1756b882a19d98632bc6c1f1f8cd, 2c4cdc0e78ef57b44f11f7ec2f6164cd, 3b658afa91ce3327dbfa1cf665529a6d, 409c2ac789015e76f9886f1203a73bc0, 601eb396c339a69e7d8c2a3de3b0296d, 664cfda4ada6f8b7bb25a5f50cccf984, 68f6810f248d032bbb65b391cdb1d5e0, 691d0143c0642ff783909f983ccb8ffd, 710d1a8b2fc17c381a7f20da5d2d70fc, 75d2c686d410ec1f880a6fd7a9800055, 909a235ac0349041b38d84e9aab3f3a1, a5e64f196175c5f068e1352aa04bc5fa, adef679c6aa6860aa89b775dceb6958b, bfd024e64867e6ca44738dd03d4f87b5, c12ff86d32bd10c6c764b71728a51bce, cf32d73c501d5924b3c98383f53fda51, d94ffe668751935b19eaeb93fed1cdbe, e3dc8810da71812b860fc59aeaddcc350, e9ed595b24a7eeb34ac52f57eeec6e2b, eadbaabe3b8133426bcf09f7102088d4
<u><a href="#">MINIBUS</a></u>	MD5	ef262f571cd429d88f629789616365e4, 816af741c3d6be1397d306841d12e206, c5dc2c75459dc99a42400f6d8b455250, 05fcace605b525f1bece1813bb18a56c, 4ed5d74a746461d3faa9f96995a1eec8, f58e0dfb8f915fa5ce1b7ca50c46b51b
<u><a href="#">LIGHTRAIL</a></u>	MD5	0a739dbdbcf9a5d8389511732371ecb4, 36e2d9ce19ed045a9840313439d6f18d, aaef98be8e58be6b96566268c163b6aa, c3830b1381d95aa6f97a58fd8ff3524e, c51bc86beb9e16d1c905160e96d9fa29, a5fdf55c1c50be471946de937f1e46dd
<u><a href="#">CHAVECLOAK</a></u>	SHA256	51512659f639e2b6e492bba8f956689ac08f792057753705bf4 b9273472c72c4, 48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3c b86b4ebb5a028, 4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c 57dcb684703006,




Attack Name	TYPE	VALUE
<b><u>CHAVECLOAK</u></b>	SHA256	131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff, 8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c, 634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9, 2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55
	URLs	hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfjrWEWGFG09t5H6854JHGJUUR[.].zip, hxxps://goo[.]su/FTD9owO
	Domains	mariashow[.]ddns[.]net, comunidadebet20102[.]hopto[.]org
<b><u>MgBot</u></b>	SHA256	34395ced1d44af75c510c6709bff51c94417558304daff35a9d07c8e628d6624, ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024, 2500aa8729f9e82765443141111614c73867f162c28b2e2283749bc208ad9e70, a4387c36bf1a150ac3a0f6d7a3ea55170fe63e772dac41ca0bc0b775a968498a, ab9c9017e53be3382867562915a2082cb4b3fdedc624a20d2dac584cb714c8d1, 00e9025b7353e427cdd0c090859ce5bd2c51a94f8f30d9a017c50c5360cc0467, 15400a1d426333b9463f425e44af721c1005962ac245df40d63c5995524d4434, 2b479ea7e5433c25905e872b8a397fb9c9cab9a9a5b02a636f2f507f55446dd1, 22a7a71608d99c76caf05a3212eb724c0cda6a40f84059fbbfe313a11448c66e, 8a9b2dadd7643cf02a4fe4ad9c6adca2f2eba158f3c3f6853f60ee6f8a789ecb, 43a9db4a84fb27d942a67a7aac15c2d5d4ed1598d73830558f5ac072b4bd9c36, 40e34f73c1efb1de8760e0fb6af044b81fa89ff1de44e0b7e3eb8f7b51ca623a
<b><u>Nightdoor</u></b>	SHA1	7a3fc280f79578414d71d70609fbdb49ec6ad648, 70b743e60f952a1238a469f529e89b0eb71b5ef7, 59aa9be378371183ed419a0b24c019ccf3da97ec, 8591a7ee00fb1bb7cc5b0417479681290a51996e, 82b99ad976429d0a6c545b64c520be4880e1e4b8
	Filename	pidgin.dll, memmgrset.dll,









Attack Name	TYPE	VALUE
<u>Nightdoor</u>	Filename	default_ico_1.exe, UjGnsPwFaEtl.exe, default_ico.exe
<u>STRRAT</u>	SHA256	97e67ac77d80d26af4897acff2a3ff6075e0efe7997a67d8194e 799006ed5efc9, 8d72ca85103f44742d04ebca02bff65788fe6b9fc6f5a411c707 580d42bbd249, 38a74520d86f5dd21bf5c447c92a9e5c0c3f69db84b1666e33d 5d86784bead3a, 2743fa7e35da259564a4f879b20487577921a3e669d6deb3fa 5cca3193f73952, 7ccc38e2616bfb5aef446213a4cab27cffd99e91ba1e0358573 44a8d5c9454b3, 595ab2d1b7478b6c6a18fec3698cb131d8115c346b0408c666 7aa6561a443c2b, 7aabe909ac93d7930bc1195f092cd2f0fb7ca8dbbb543e4a3d4 42f6bb13121a0, 1d3219b6ccc538b8cbecb13eb9c23ce00a6ed315a2a7fecb9b7 91e9cd1888bd8, a36323cc7633934af9b10f0c56841e483bb886836ca94fc52ce 37ca3f0cfd190, 8efa0e193fb08adf90ba95c2e7f2de6453c3276cd8ae154c4af1 17a48a668ef3, d38b806812c7610cc3349a2ec4b60b0fcf61a92295fe7eea72d a2a255b204b5e, 26104fcd8de196afcbaf13b7a6aa150855ee64060ec9e9444db 0448b3524cf80, 85ea19ebad6e8cebdbd3c188964228fab7512b8668633f621b f0d660b8f92a33




# Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-46805</a>		Ivanti Connect Secure and Policy Secure	UTA0178, Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability		CWE ID	ASSOCIATED TTPs
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21887</u></a>		Ivanti Connect Secure and Policy Secure	UTA0178, Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure-:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
			
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21893</u></a>		Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	UTA0178, Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure-:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
			
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy, T1135: Network Share Discovery, T1005: Data from Local System	<a href="https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-22024</u></a>		Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways	UTA0178
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1046: Network Service Discovery	<a href="https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US">https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21888</u></a>		Ivanti Connect Secure and Ivanti Policy Secure	UTA0178, Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:-:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	<a href="https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-27198</a>		TeamCity On-Premises versions upto 2023.11.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jetbrains:TeamCity:*:*:*:*:*:*	Jasmin ransomware, XMRig, SparkRAT backdoor
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1556 : Modify Authentication Process, T1190 : Exploit Public-Facing Application	<a href="https://www.jetbrains.com/teamcity/download/">https://www.jetbrains.com/teamcity/download/</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-23225</a>		iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apple:*:*:*:*:*:*	-
Apple iOS and iPadOS Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1211 : Exploitation for Defense Evasion, T1106 : Native API	<a href="https://support.apple.com/en-us/HT214081">https://support.apple.com/en-us/HT214081</a> ; <a href="https://support.apple.com/en-us/HT214082">https://support.apple.com/en-us/HT214082</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-23296</u></a>		iPadOS: 17.4 and prior, 16.7.6 and prior Apple iOS: 17.4 and prior, 16.7.6 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:*:*:*:*:*:*	-
Apple iOS and iPadOS Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1211 : Exploitation for Defense Evasion, T1106 : Native API	<a href="https://support.apple.com/en-us/HT214081">https://support.apple.com/en-us/HT214081</a> ; <a href="https://support.apple.com/en-us/HT214082">https://support.apple.com/en-us/HT214082</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2022-26134</u></a>		Atlassian Confluence Server and Data Center	APT 28, DarkPink, Konni, APT 40, Sandworm and APT 29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*	AvosLocker ransomware
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1190 : Exploit Public-Facing Application, T1203 : Exploitation for Client Execution	<a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-20337</u></a>		Cisco Secure Client: 4.10.04065 - 5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:cisco:anyconnect_secure_mobility_client cpe:2.3:a:cisco:secure_client	-
Cisco Secure Client Carriage Return Line Feed Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter, T1133: External Remote Service	<a href="https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/series.html#tab-downloads">https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/series.html#tab-downloads</a>
	CWE-93		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-2194</u></a>		WordPress WP Statistics Plugin all versions up to 14.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:wp_statistics_plugin:wp_statistics_plugin:14.0:*:*:*:*:*	-
WordPress WP Statistics plugin Cross-Site Scripting Vulnerability			
	CWE ID	T1189: Drive-by Compromise, T1204.001: Malicious Link	<a href="https://wordpress.org/plugins/wp-statistics/">https://wordpress.org/plugins/wp-statistics/</a>
	CWE-79		









CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2022-24086</a>		Adobe Commerce and Magento Open Source	Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:adobe:commerce:*:*:*:*:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Adobe Commerce and Magento OpenSource Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow	<a href="https://helpx.adobe.com/security/products/magento/apsb22-12.html">https://helpx.adobe.com/security/products/magento/apsb22-12.html</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-41265</a>		Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:qlik:qlik_sense:august_2022:*:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise Privilege escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1068: Exploitation for Privilege Escalation	<a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-41266</a>		Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise path traversal Vulnerability			
	CWE ID	T1005: Data from Local System, T1222: File and Directory Permissions Modification	<a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a>
	CWE-20		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-48365</a>		Qlik Sense Enterprise for Windows	Magnet Goblin
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	NerbianRAT, WARPWIRE, MiniNerbian
Qlik Sense Enterprise remote code execution Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	<a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510</a>
	CWE-444		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-2172</u></a>		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
<a href="#"><u>CVE-2023-32315</u></a>		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	<a href="https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm">https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2022-21587</u></a>		Oracle E-Business Suite	Earth Krahang and Earth Lusca
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:e-business_suite:*:*:*:*:*:* *	RESHELL, XDealer (DinodasRAT), Cobalt Strike, PlugX, and ShadowPad
Oracle E-Business Suite Unspecified Vulnerability			CWE ID
	CWE-306	T1588.006: Vulnerabilities	<a href="https://www.oracle.com/security-alerts/cpuoct2022.html">https://www.oracle.com/security-alerts/cpuoct2022.html</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-23334</u></a>		aiohttp: Prior to version 3.9.2	ShadowSyndicate
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:aiohttp:aiohttp:*:* .*:*:*:*:*.*	-
Aiohttp Directory Traversal Vulnerability			CWE ID
	CWE-22	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	<a href="https://github.com/aio-lib/aiohttp/security/advisories/GHSA-5h86-8mv2-1q9f">https://github.com/aio-lib/aiohttp/security/advisories/GHSA-5h86-8mv2-1q9f</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2024-27199</u></b>		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	<a href="https://www.jetbrains.com/teamcity/download/">https://www.jetbrains.com/teamcity/download/</a>
	CWE-23		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2024-1597</u></b>		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	<a href="https://www.atlassian.com/software/bamboo/download-archives">https://www.atlassian.com/software/bamboo/download-archives</a>
	CWE-89		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2017-9805</u></a>		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	<a href="https://cwiki.apache.org/confluence/display/WW/S2-052"><u>https://cwiki.apache.org/confluence/display/WW/S2-052</u></a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-22527</u></a>		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	<a href="https://jira.atlassian.com/browse/CONFSERVER-93833"><u>https://jira.atlassian.com/browse/CONFSERVER-93833</u></a>




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

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









CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-1709</u></a>		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			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	<a href="https://screenconnect.com/connectwise.com/download"><u>https://screenconnect.com/connectwise.com/download</u></a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2023-22518</u></a>		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			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1574: Hijack Execution Flow, T1190: Exploit Public-Facing Application	<a href="https://www.atlassian.com/software/confluence/download-archives"><u>https://www.atlassian.com/software/confluence/download-archives</u></a>

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			ASSOCIATED TTPs
	CWE ID	T1574: Hijack Execution Flow, T1211: Exploitation for Defense Evasion	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2</a>
	CWE-191 CWE-190		

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			ASSOCIATED TTPs
	CWE ID	T1059: Command and Scripting Interpreter	<a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a>
	CWE-78		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-2886</a>		Google Chrome prior to 123.0.6312.86	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome	
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: <a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-2887</a>		Google Chrome prior to 123.0.6312.86	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome	
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: <a href="https://www.google.com/intl/en/chrome/?standalone=1">https://www.google.com/intl/en/chrome/?standalone=1</a>

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

# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<b><u>MINIBIKE</u></b>	MINIBIKE, a custom C++ backdoor first identified in June 2022, facilitates file exfiltration, command execution, and more, communicating through Azure cloud infrastructure.	Spear phishing and watering-hole attacks	-	
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
<b>TYPE</b> Backdoor		Espionage	-	
			<b>ASSOCIATED ACTOR</b>	<b>PATCH LINK</b>
			UNC1549	-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<b><u>MINIBUS</u></b>	MINIBUS, documented in August 2023, offers a more versatile code-execution interface and enhanced reconnaissance features compared to MINIBIKE.	Spear phishing and watering-hole attacks	-	
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>	
<b>TYPE</b> Backdoor		Espionage	-	
			<b>ASSOCIATED ACTOR</b>	<b>PATCH LINK</b>
			UNC1549	-

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
<b><u>LIGHTRAIL</u></b>	A tunneler first seen in November 2022, likely based on an open-source Socks4a proxy, that communicates using Azure cloud infrastructure	Spear phishing and watering-hole attacks	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Espionage	-
Tunneling			<b>PATCH LINK</b>
<b>ASSOCIATED ACTOR</b>			-
UNC1549			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>Bifrost (aka Bifrose)</u></b>	A new Linux variant of the Bifrost RAT evades detection using a deceptive VMware domain, aiming to compromise systems. This persistent threat spreads through malicious emails and sites, harvesting sensitive data and now includes an ARM version, emphasizing the need for vigilant countermeasures to safeguard against evolving malware.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		System Disruption	Linux
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-

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>Pikabot</u>	Pikabot is a sophisticated piece of multi-stage malware with a loader and core module within the same file. Pikabot, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader			-
ASSOCIATED ACTOR			PATCH LINK
TA577			Data Theft, Downloading other malware

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>CHAVECLOAK</u>	The CHAVECLOAK banking trojan is purposefully crafted to target the banking credentials of individuals in Brazil, highlighting the ongoing focus of cyber criminals on the nation's financial sector.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Trojan			Windows	
ASSOCIATED ACTOR			Financial gain and Data Theft	PATCH LINK
-			-	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>WogRAT</u>	WogRAT, a backdoor malware targeting both Windows and Linux, spreads through aNotepad, an online notepad service. It disguises itself as system tools to trick users into downloading it, mainly targeting users in Asia.	Via aNotepad	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Backdoor			Windows and Linux	
ASSOCIATED ACTOR			Data Theft	PATCH LINK
-			-	

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
<a href="#"><u>GhostLocker</u></a>	GhostLocker is ransomware-as-a-Service (RaaS) - developed by the hacktivist group GhostSec, it's now offered to other cybercriminals for a fee. It's features are military-grade encryption, self-deletion to avoid detection, and even attempts to escalate privileges to gain more control over your system.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Data Theft and System Disruption	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Stormous</u></a>	Stormous ransomware primarily known for deploying ransomware attacks, often targeting Western companies and organizations. It has been partnered with other hacking groups like GhostSec, forming the "Five Families" alliance. This collaboration allows them to launch more complex attacks.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware		Data Theft and System Disruption	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>SapphireStealer</u></a>	SapphireStealer is a information-stealing malware. It runs on Windows and steals logins, browsing data, screenshots, and specific files. As it's open-source, it's easy to customize and new versions are constantly emerging, making it difficult to detect.	various public malware repositories	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Info stealer		Data Theft	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-

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
<a href="#"><u>MgBot</u></a>	MgBot is a modular backdoor malware framework that is actively maintained and equipped with various plugins, allowing attackers to gather extensive information from compromised machines, indicating that the attackers' primary objective was information-gathering.	Social Engineering	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		System Compromise, Information theft	<b>PATCH LINK</b>
Evasive Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Nightdoor</u></a>	The Nightdoor backdoor talks with its C&C server via UDP or the Google Drive API. Each message sent between Nightdoor and the C&C server is stored as a file.	Social Engineering	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>		System Compromise, Information theft	<b>PATCH LINK</b>
Evasive Panda			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>STRRAT</u></a>	STRRAT, also a Java-built RAT, has been observed in the wild since 2020, frequently propagated through deceptive JAR files.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Information theft, Espionage	<b>PATCH LINK</b>
-			-

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>VCURMS</u>	VCURMS bears similarities to another Java-based infostealer called Rude Stealer. This similarity encompasses the ability to execute arbitrary commands, gather system data, search and transmit files of interest, and acquire additional information stealer and keylogger modules from the same AWS endpoint.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			AWS and GitHub
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Information theft, Espionage	-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>TimbreStealer</u>	TimbreStealer is an advanced malware designed to Collect credential information from the victim's machine, Search for Files, Collect OS information, Search for file extensions, Look for URLs Accessed, Disable System Protections, Look for Remote Desktop Software, POST data to remote site.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information Stealer			-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		Information theft, System Compromise	-

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>NerbianRAT</u>	<p>NerbianRAT was first publicly disclosed in 2022. NerbianRAT stands as a versatile remote access trojan (RAT), customized for both Windows and Linux environments, accompanied by MiniNerbian, a compact yet potent Linux-based backdoor.</p>	Exploiting Vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		Espionage, Financial Gains	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Magnet Goblin			<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a> , <a href="https://helpx.adobe.com/security/products/magento/apsb22-12.html">https://helpx.adobe.com/security/products/magento/apsb22-12.html</a> , <a href="https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a> , <a href="https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a> , <a href="https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510">https://community.glik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510</a> , <a href="https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure</a>

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>WARPWIRE</u>	<p>WARPWIRE, a JavaScript-based credential theft tool further enables access to accounts for lateral movement or espionage by capturing plaintext login credentials.</p>	Exploiting Vulnerabilities	<p>CVE-2023-46805            CVE-2024-21887            CVE-2022-24086            CVE-2023-41265            CVE-2023-41266            CVE-2023-48365            CVE-2024-21888            CVE-2024-21893</p>
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information Stealer		<p>Information theft, Espionage, Financial Gains</p>	Ivanti, Magento, Qlik Sense, and Apache ActiveMQ
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Magnet Goblin			<p><a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a>,  <a href="https://helpx.adobe.com/security/products/magento/apsb22-12.html">https://helpx.adobe.com/security/products/magento/apsb22-12.html</a>,  <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a>,  <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a>,  <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510</a>,  <a href="https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure</a></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
<b>MiniNerbian</b>	MiniNerbian, a compact yet potent Linux-based backdoor. MiniNerbian is a simplified version of NerbianRAT, which has one main functionality which is command execution.	Exploiting Vulnerabilities	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Espionage, Financial Gains	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Magnet Goblin			<a href="https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US">https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</a> , <a href="https://helpx.adobe.com/security/products/magento/apsb22-12.html">https://helpx.adobe.com/security/products/magento/apsb22-12.html</a> , <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a> , <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801</a> , <a href="https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510">https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510</a> , <a href="https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure">https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure</a>

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
<b><u>RESHELL</u></b>	<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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Steal Data	Ignite Realtime Openfire, Oracle E-Business Suite
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Krahang and Earth Lusca			<a href="https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm">https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm</a> , <a href="https://www.oracle.com/security-alerts/cpuoct2022.html">https://www.oracle.com/security-alerts/cpuoct2022.html</a>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>ShadowPad</u></b>	<p>ShadowPad is used for remote access and data exfiltration.</p>	Exploiting Vulnerabilities	CVE-2023-32315 CVE-2022-21587
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Steal data	Ignite Realtime Openfire, Oracle E-Business Suite
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Krahang and Earth Lusca			<a href="https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm">https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm</a> , <a href="https://www.oracle.com/security-alerts/cpuoct2022.html">https://www.oracle.com/security-alerts/cpuoct2022.html</a>

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
<b>Xdealer</b> <b>(DinodasRAT)</b>	<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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		Steal Data	Ignite Realtime Openfire, Oracle E-Business Suite
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Krahang and Earth Lusca			<a href="https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm">https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm</a> , <a href="https://www.oracle.com/security-alerts/cpuoct2022.html">https://www.oracle.com/security-alerts/cpuoct2022.html</a>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b>PlugX</b>	<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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT		Remote access	Ignite Realtime Openfire, Oracle E-Business Suite
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
Earth Krahang and Earth Lusca			<a href="https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm">https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm</a> , <a href="https://www.oracle.com/security-alerts/cpuoct2022.html">https://www.oracle.com/security-alerts/cpuoct2022.html</a>

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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Steal Data	<b>PATCH LINK</b>
Kimsuky group			

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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Steal Data	<b>PATCH LINK</b>
Kimsuky group			

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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
RAT			
<b>ASSOCIATED ACTOR</b>		Steal Data	<b>PATCH LINK</b>
Kimsuky group			

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
<a href="#"><u>NetSupport RAT</u></a>	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
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>BunnyLoader 3.0</u></a>	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
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>AsukaStealer</u></a>	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
-			-

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>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				PATCH LINK
-				<a href="https://www.jetbrains.com/teamcity/download/">https://www.jetbrains.com/teamcity/download/</a>

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 CVE-2017-9805 CVE-2023-22527 CVE-2021-26084	
TYPE		IMPACT	AFFECTED PRODUCTS	
Miner				TeamCity On-Premises, Apache Struts, Atlassian Confluence
ASSOCIATED ACTOR				PATCH LINK
-				<a href="https://www.jetbrains.com/teamcity/download/">https://www.jetbrains.com/teamcity/download/</a> <a href="https://cwiki.apache.org/confluence/display/WW/S2-052">https://cwiki.apache.org/confluence/display/WW/S2-052</a> <a href="https://jira.atlassian.com/browse/CONFSERVER-93833">https://jira.atlassian.com/browse/CONFSERVER-93833</a> <a href="https://jira.atlassian.com/browse/CONFSERVER-67940">https://jira.atlassian.com/browse/CONFSERVER-67940</a>

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>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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>			
-			
	Data Theft	TeamCity On-Premises	
		<b>PATCH LINK</b>	
		<a href="https://www.jetbrains.com/teamcity/download/">https://www.jetbrains.com/teamcity/download/</a>	

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.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Wiper			
<b>ASSOCIATED ACTOR</b>			
UAC-0165			
	System Compromise	Linux	
		<b>PATCH LINK</b>	
		-	

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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor			
<b>ASSOCIATED ACTOR</b>			
APT29			
	Date Loss, System Compromise	Windows	
		<b>PATCH LINK</b>	
		-	

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
<a href="#"><u>ROOTSAW</u></a>	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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Dropper			
<b>ASSOCIATED ACTOR</b>		Date Loss, System Compromise	Windows
APT29			<b>PATCH LINK</b>
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>Evil Ant Ransomware</u></a>	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.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			
<b>ASSOCIATED ACTOR</b>		Date Loss, Financial Loss	-
-			<b>PATCH LINK</b>
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<a href="#"><u>StrelaStealer</u></a>	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	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information Stealer			
<b>ASSOCIATED ACTOR</b>		Date Loss	-
-			<b>PATCH LINK</b>
			-

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><a href="#">Agenda ransomware (aka Qilin, Water Galura)</a></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>	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Ransomware			
<b>ASSOCIATED ACTOR</b>		Date Loss, Financial Loss	<b>PATCH LINK</b>
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u><a href="#">Sysrv Botnet</a></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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Botnet			
<b>ASSOCIATED ACTOR</b>		Date Loss, System Compromise, Financial Loss	<b>PATCH LINK</b>
-			<a href="https://cwiki.apache.org/confluence/display/WW/S2-052">https://cwiki.apache.org/confluence/display/WW/S2-052</a> <a href="https://jira.atlassian.com/browse/CONFSERVER-93833">https://jira.atlassian.com/browse/CONFSERVER-93833</a> <a href="https://jira.atlassian.com/browse/CONFSERVER-67940">https://jira.atlassian.com/browse/CONFSERVER-67940</a>

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>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.	-	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Wiper			
<b>ASSOCIATED ACTOR</b>		System Compromise	<b>PATCH LINK</b>
UAC-0165			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>SNOWLIGHT</u>	SNOWLIGHT is a 64-bit ELF Dropper 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.	Exploiting vulnerabilities	CVE-2023-46747 CVE-2024-1709 CVE-2023-22518 CVE-2022-0185 CVE-2022-30525
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Dropper			
<b>ASSOCIATED ACTOR</b>		Data Loss, System Compromise	<b>PATCH LINK</b>
UNC5174 (aka Uteus)			<a href="https://my.f5.com/manage/s/article/K000137353">https://my.f5.com/manage/s/article/K000137353</a> <a href="https://screenconnect.connectwise.com/download">https://screenconnect.connectwise.com/download</a> <a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a> <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2</a> <a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a>

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

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
<b><u>GOREVERSE</u></b>	<p>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.</p>	Exploiting vulnerabilities	<p>CVE-2023-46747            CVE-2024-1709            CVE-2023-22518            CVE-2022-0185            CVE-2022-30525</p>
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		<p>Data Loss, System Compromise</p>	<p>F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls</p>
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5174 (aka Uteus)			<p><a href="https://my.f5.com/manage/s/article/K000137353">https://my.f5.com/manage/s/article/K000137353</a>  <a href="https://screenconnect.connectwise.com/download">https://screenconnect.connectwise.com/download</a>  <a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a>  <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2</a>  <a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a></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
<b><u>SUPERSHELL</u></b>	<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
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Hack Tool		Data Loss, System Compromise	F5 BIG-IP, ConnectWise, Atlassian Confluence, Linux Kernel, Zyxel Multiple Firewalls
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNC5174 (aka Uteus)			<a href="https://my.f5.com/manage/s/article/K000137353">https://my.f5.com/manage/s/article/K000137353</a> <a href="https://screenconnect.connectwise.com/download">https://screenconnect.connectwise.com/download</a> <a href="https://www.atlassian.com/software/confluence/download-archives">https://www.atlassian.com/software/confluence/download-archives</a> <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2</a> <a href="https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls">https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls</a>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<b><u>HackBrowserData</u></b>	<p>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.</p>	Slack channels	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Information stealer		Data Loss, System Compromise	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-			-


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


# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>UTA0178</b>	-	Government, Military, Telecommunications, Defense, Technology, Banking, Finance, Accounting, Aerospace, Aviation, Engineering	Worldwide
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2023-46805 CVE-2024-21887 CVE-2024-21893 CVE-2024-22024 CVE-2024-21888	-	Ivanti Connect Secure and Ivanti Policy Secure

## TTPs


TA0008: Lateral Movement; TA0003: Persistence; TA0006: Credential Access; TA0002: Execution; TA0001: Initial Access; TA0042: Resource Development; TA0004: Privilege Escalation; T1505: Server Software Component; T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1068: Exploitation for Privilege Escalation; T1059.001: PowerShell; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1505.003: Web Shell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>UNC1549</b>	Affiliated to Iran	Aerospace, Aviation, and Defense	Akrotiri and Dhekelia, Albania, Bahrain, Cyprus, Egypt, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	MINIBIKE, MINIBUS, LIGHTRAIL	-	
<b>TTPs</b>			
TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and: Control; TA0040: Impact; T1055: Process Injection; T1204.002: Malicious File; T1562: Impair Defenses; T1059: Command and: Scripting Interpreter; T1057: Process Discovery; T1083: File and Directory: Discovery; T1027: Obfuscated Files or: Information; T1598.002: Spearphishing: Attachment; T1070: Indicator Removal; T1574.002: DLL Side-Loading; T1041: Exfiltration Over C2: Channel; T1036: Masquerading; T1001: Data Obfuscation; T1027.010: Command: Obfuscation; T1555.003: Credentials from Web: Browsers; T1578: Modify Cloud: Compute: Infrastructure			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>TA577</b>	-	-	Worldwide
	<b>MOTIVE</b>		
	Information Theft and Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	Pikabot	Windows


**TTPs**

TA0001: Initial Access, TA0002: Execution, TA0008: Lateral Movement, TA0003: Persistence, TA0005: Defense Evasion, TA0006: Credential Access, T1021.002: SMB/Windows Admin Shares, T1021: Remote Services, T1566.001: Spearphishing Attachment, T1566: Phishing, T1204.002: Malicious File, T1204: User Execution, T1555: Credentials from Password Stores, T1574: Hijack Execution Flow , T1555.004: Windows Credential Manager

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>TA4903</b>	-	Government, Construction, Healthcare, Manufacturing, Energy, Finance, Agriculture, Transportation, Commerce, Food and Beverage	United States of America
	<b>MOTIVE</b>		
	Financial gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	-	-


**TTPs**


TA0001: Initial Access, TA0002: Execution, TA0040: Impact, TA0003: Persistence, TA0005: Defense Evasion, TA0006: Credential Access, T1021.002: SMB/Windows Admin Shares, T1021: Remote Services, T1566.001: Spearphishing Attachment, T1566: Phishing, T1204.002: Malicious File, T1204: User Execution, T1555: Credentials from Password Stores, T1574: Hijack Execution Flow , T1555.004: Windows Credential Manager

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b><u>Evasive Panda (aka Daggerfly, Bronze Highland)</u></b></p>	China	All	India, Taiwan, Hong Kong, Australia, USA
	<b>MOTIVE</b>		
	Information Theft and Espionage	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	<b>TARGETED CVEs</b>		
-	MgBot, Nightdoor	Windows and macOS	

**TTPs**

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.004: Server; T1583.006: Web Services; T1584.004: Server; T1585.003: Cloud Accounts; T1587.001: Malware; T1588.003: Code Signing Certificates; T1608.004: Drive-by Target; T1189: Drive-by Compromise; T1195.002: Compromise Software Supply Chain; T1106: Native API; T1053.005: Scheduled Task; T1543.003: Windows Service; T1574.002: DLL Side-Loading; T1140: Deobfuscate/Decode Files or Information; T1562.004: Disable or Modify System Firewall; T1070.004: File Deletion; T1070.009: Clear Persistence; T1036.004: Masquerade Task or Service; T1036.005: Match Legitimate Name or Location; T1027.009: Embedded Payloads; T1055.001: Dynamic-link Library Injection; T1620: Reflective Code Loading; T1087.001: Local Account; T1083: File and Directory Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1049: System Network Connections Discovery; T1560: Archive Collected: Data; T1119: Automated Collection; T1005: Data from Local System; T1074.001: Local Data Staging; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1571: Non-Standard Port; T1572: Protocol Tunneling; T1102: Web Service; T1020: Automated Exfiltration; T1567.002: Exfiltration to Cloud Storage


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><b><u>Magnet Goblin</u></b></p>	-	All	Worldwide
	<b>MOTIVE</b>		
	Financial Gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2023-46805 CVE-2024-21887 CVE-2022-24086 CVE-2023-41265 CVE-2023-41266 CVE-2023-48365 CVE-2024-21888 CVE-2024-21893	NerbianRAT, WARPWIRE, MiniNerbian	Ivanti, Magento, Qlink Sense, and Apache ActiveMQ
<b>TTPs</b>			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1041: Exfiltration Over C2 Channel; T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1573.001: Symmetric Cryptography; T1071.001: Web Protocols; T1573: Encrypted Channel; T1071: Application Layer Protocol; T1588.006: Vulnerabilities; T1588.001: Malware; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>Earth Krahang</b>	China	Government, Education, Telecommunications, Finance, Insurance, Foundations, NGOs, Think tanks, Healthcare, IT, Manufacturing, Media, Military, Real estate, Retail, Sports, and Tourism	Worldwide
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	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><b>Earth Lusca (aka Bronze University, Chromium, Charcoal Typhoon, Red Dev 10, Red Scylla)</b></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
	<b>MOTIVE</b>		
	Information theft and espionage, Financial gain		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
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><b>ShadowSyndicate</b></p>	-	All	Worldwide
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2024-23334	-	Aiohttp
<b>TTPs</b>			
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
 <p><b>Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)</b></p>	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
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	TutClient, TutRAT, and xRAT	Windows
<b>TTPs</b>			
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><b>UAC-0165</b></u>	Russia	Telecommunications, Critical Infrastructure, Energy, and Government	Ukraine
	<b>MOTIVE</b> Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	-	AcidPour, AcidRain	-
	<b>TTPs</b>		
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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u><a href="#">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, Crane-fly, TEMP.Monkeys, Cloaked Ursa, Blue Dev 5, NobleBaron, Solar Phoenix)</a></u></p>	Russia	Diplomatic, Political, Government, and Civil Society	Germany
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	WINELOADER, ROOTSAW	Windows	

### TTPs

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

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
	<b>MOTIVE</b>		
	Espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	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

# MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
<b>TA0043: Reconnaissance</b>	T1592: Gather Victim Host Information	T1595.001: Scanning IP Blocks
		T1595.002: Vulnerability Scanning
		T1595.003: Wordlist Scanning
	T1590: Gather Victim Network Information	
<b>TA0042: Resource Development</b>	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.002: Tool
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.003: Install Digital Certificate
		T1608.001: Upload Malware
		T1608.005: Link Target
		T1608.004: Drive-by Target
	T1587.004: Develop Capabilities	T1608.002: Upload Tool
		T1587.004: Exploits
	T1583: Acquire Infrastructure	T1587.001: Malware
		T1583.001: Domains
		T1583.004: Server
		T1583.006: Web Services
	T1586: Compromise Accounts	T1583.003: Virtual Private Server
		T1586.002: Email Accounts
		T1588.001: Malware
	T1585: Establish Accounts	T1588.003: Code Signing Certificates
		T1585.003: Cloud Accounts
<b>TA0001: Initial Access</b>	T1566: Phishing	T1584.004: Server
		T1566.002: Spearphishing Link
	T1190: Exploit Public-Facing Application	T1566.001: Spearphishing Attachment
	T1133: External Remote Services	
	T1199: Trusted Relationship	
	T1189: Drive-by Compromise	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1078: Valid Accounts	T1078.003: Local Accounts
<b>TA0002: Execution</b>	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.001: PowerShell
		T1059.006: Python
		T1059.005: Visual Basic
		T1059.003: Windows Command Shell
T1059.007: JavaScript		

Tactic	Technique	Sub-technique
<b>TA0002: Execution</b>	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1047: Windows Management Instrumentation	
	T1106: Native API	
	T1569: System Services	T1569.002: Service Execution
	T1129: Shared Modules	
<b>TA0003: Persistence</b>	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1098: Account Manipulation	
	T1176: Browser Extensions	
	T1133: External Remote Services	
	T1136.002: Create Account	T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
T1543.004: Launch Daemon		
<b>TA0004: Privilege Escalation</b>	T1098: Account Manipulation	
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
T1078: Valid Accounts	T1078.002: Domain Accounts	
T1484: Domain Policy Modification	T1484.001: Group Policy Modification	
<b>TA0005: Defense Evasion</b>	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1036: Masquerading	T1036.007: Double File Extension
		T1036.008: Masquerade File Type
		T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
T1027: Obfuscated Files or Information	T1027.009: Embedded Payloads	

Tactic	Technique	Sub-technique
<b>TA0005: Defense Evasion</b>	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1562: Impair Defenses	
	T1221: Template Injection	
	T1202: Indirect Command Execution	
	T1480: Execution Guardrails	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec T1218.005: Mshta
	T1070: Indicator Removal	T1070.006: Timestamp
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1564: Hide Artifacts	T1564.002: Hidden Users
	T1622: Debugger Evasion	
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1134: Access Token Manipulation	
	T1220: XSL Script Processing	
	<b>TA0006: Credential Access</b>	T1003: OS Credential Dumping
T1110: Brute Force		
T1552: Unsecured Credentials		
T1539: Steal Web Session Cookie		
T1040: Network Sniffing		
T1056: Input Capture		T1056.001: Keylogging
T1556: Modify Authentication Process		T1556.008: Network Provider DLL
T1555: Credentials from Password Stores		T1555.003: Credentials from Web Browsers T1555.004: Windows Credential Manager
T1558: Steal or Forge Kerberos Tickets		T1558.001: Golden Ticket
T1606: Forge Web Credentials		
T1557: Adversary-in-the-Middle		
<b>TA0007: Discovery</b>	T1018: Remote System Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1046: Network Service Discovery	
	T1087: Account Discovery	
	T1016: System Network Configuration Discovery	
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1622: Debugger Evasion	



Tactic	Technique	Sub-technique
<b>TA0007: Discovery</b>	T1007: System Service Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1040: Network Sniffing	
	T1518: Software Discovery	T1518.001: Security Software Discovery
<b>TA0008: Lateral Movement</b>	T1021: Remote Services	T1021.006: Windows Remote Management
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
<b>TA0009: Collection</b>	T1056: Input Capture	T1056.001: Keylogging
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1074: Data Staged	T1074.001: Local Data Staging
	T1114: Email Collection	T1114.002: Remote Email Collection
		T1114.003: Email Forwarding Rule
	T1005: Data from Local System	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
<b>TA0011: Command and Control</b>	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.004: DNS
	T1659: Content Injection	
	T1105: Ingress Tool Transfer	
	T1104: Multi-Stage Channels	
	T1572: Protocol Tunneling	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1568: Dynamic Resolution	
	T1008: Fallback Channels	
T1571: Non-Standard Port		
<b>TA0010: Exfiltration</b>	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
	T1029: Scheduled Transfer	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1048: Exfiltration Over Alternative Protocol	
<b>TA0040: Impact</b>	T1657: Financial Theft	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1498: Network Denial of Service	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
	T1489: Service Stop	



# Top 5 Takeaways

**#1**

In **March**, **ten zero-day vulnerabilities** were identified across various platforms, including **Ivanti Connect Secure, Apple, Google, Atlassian, Adobe,** and **ConnectWise ScreenConnect**. These vulnerabilities were actively exploited in attacks by adversaries.

**#2**

Throughout the month, ransomware strains including **GhostLocker, Stormous, Jasmin, Agenda,** and **Evil Ant** actively targeted victims.

**#3**

Numerous malware families have been observed targeting victims in the wild. These include **MINIBIKE, MINIBUS, LIGHTRAIL, Bifrost, MgBot, Nightdoor, VCURMS, STRRAT,** and **TimbreStealer**.

**#4**

There were a total of **13 active adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: **Government, Finance, Energy, Defense,** and **Construction**

**#5**

The **DEEP#GOSU** campaign, associated with the North Korean **Kimsuky group**, utilizes sophisticated multi-stage attacks. By employing PowerShell and VBScript, the attackers gain control over compromised hosts using remote access trojan (RAT) software.

# Recommendations

## Security Teams










































This digest can be used as a guide to help security teams prioritize the **32 significant vulnerabilities** and block the indicators related to the **13 active threat actors**, **44 active malware**, and **252 potential MITRE TTPs**.

## Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **32 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors**, **active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

# Hive Pro Threat Advisories (MARCH 2024)

MONDAY		TUESDAY		WEDNESDAY		THURSDAY		FRIDAY		SATURDAY		SUNDAY	
									1		2		3
													
	4		5		6		7		8		9		10
													
	11		12		13		14		15		16		17
													
	18		19		20		21		22		23		24
													
	25		26		27		28		29		30		31
													

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

# 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 malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

**Social engineering:** is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

**Supply chain attack:** Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

**Eavesdropping:** Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

## Glossary:

**CISA KEV** - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities

**CVE** - Common Vulnerabilities and Exposures

**CPE** - Common Platform Enumeration

**CWE** - Common Weakness Enumeration

## ✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>MINIBIKE</u>	MD5	01cbadd7a269521bf7b80f4a9a1982f, 054c67236a86d9ab5ec80e16b884f733, 1d8a1756b882a19d98632bc6c1f1f8cd, 2c4cdc0e78ef57b44f11f7ec2f6164cd, 3b658afa91ce3327dbfa1cf665529a6d, 409c2ac789015e76f9886f1203a73bc0, 601eb396c339a69e7d8c2a3de3b0296d, 664cfda4ada6f8b7bb25a5f50ccccf984, 68f6810f248d032bbb65b391cdb1d5e0, 691d0143c0642ff783909f983ccb8ffd, 710d1a8b2fc17c381a7f20da5d2d70fc, 75d2c686d410ec1f880a6fd7a9800055, 909a235ac0349041b38d84e9aab3f3a1, a5e64f196175c5f068e1352aa04bc5fa, adef679c6aa6860aa89b775dceb6958b, bfd024e64867e6ca44738dd03d4f87b5, c12ff86d32bd10c6c764b71728a51bce, cf32d73c501d5924b3c98383f53fda51, d94ffe668751935b19eae93fed1cdbe, e3dc8810da71812b860fc59aeaddcc350, e9ed595b24a7eeb34ac52f57eeec6e2b, eadbaabe3b8133426bcf09f7102088d4
<u>MINIBUS</u>	MD5	ef262f571cd429d88f629789616365e4, 816af741c3d6be1397d306841d12e206, c5dc2c75459dc99a42400f6d8b455250, 05fcace605b525f1bece1813bb18a56c, 4ed5d74a746461d3faa9f96995a1eec8, f58e0dfb8f915fa5ce1b7ca50c46b51b
<u>LIGHTRAIL</u>	MD5	0a739dbdbcf9a5d8389511732371ecb4, 36e2d9ce19ed045a9840313439d6f18d, aaef98be8e58be6b96566268c163b6aa, c3830b1381d95aa6f97a58fd8ff3524e, c51bc86beb9e16d1c905160e96d9fa29, a5fdf55c1c50be471946de937f1e46dd
<u>Bifrost</u>	SHA256	8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00 250a4a2fe4729, 2aeb70f72e87a1957e3bc478e1982fe608429cad4580737abe 58f6d78a626c05
	IPv4	45.91.82[.]127
	Domain	download.vmfare[.]com

Attack Name	TYPE	VALUE
<u>Pikabot</u>	SHA256	4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b, fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de, 29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8
<u>CHAVECLOAK</u>	SHA256	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4, 48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028, 4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006, 131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff, 8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c, 634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9, 2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55
	URLs	hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrwEWGFG09t5H6854JHGJUUR[.].zip, hxxps://goo[.]su/FTD9owO
	Domains	mariashow[.]ddns[.]net, comunidadebet20102[.]hopto[.]org
<u>WogRAT</u>	Domains	w.linuxwork[.]net, linuxwork[.]net
	MD5	290789ea9d99813a07294ac848f808c9, 1aebf536268a9ed43b9c2a68281f0455, 194112c60cb936ed1c195b98142ff49d, 1341e507f31fb247c07beeb14f583f4f, fff21684df37fa7203ebe3116e5301c1, f97fa0eb03952cd58195a224d48f1124, f271e0ae24a9751f84c5ae02d29f4f0e, e9ac99f98e8fbd69794a9f3c5afdcb52, da3588a9bd8f4b81c9ab6a46e9cddedd, a35c6fbe8985d67a69c918edcb89827e, 929b8f0bdbb2a061e4cf2ce03d0bbc4c, 7bcfea3889f07f1d8261213a77110091, 655b3449574550e073e93ba694981ef4, 5769d2f0209708b4df05aec89e841f31, 3669959fdb0f83239dba1a2068ba25b3

Attack Name	TYPE	VALUE
<u>WogRAT</u>	URLs	hxxps://t0rguard[.]net/c/ hxxps://w.newujs[.]com/c/ hxxps://newujs[.]com/tt.php?fuckyou=1, hxxp://newujs[.]com/dddddd_oo, hxxp://newujs[.]com/abc, hxxp://newujs[.]com/a14407a2, hxxps://js.domaiso[.]com/jquery.min-2.js, hxxps://jp.anotepad[.]com/note/read/b896abi9, hxxp://newujs[.]com/cff/wins.jpg
<u>GhostLocker</u>	SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282e b24b7c55f, 8b758ccdffbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f4 43779e9,
<u>Stormous</u>	SHA256	a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282e b24b7c55f, 8b758ccdffbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f4 43779e9,
	MD5	b15a8047abd9a3af013cf6c77ce15acf
	SHA1	aa62afd6a48d3c42ed66d4f5b9189be847ec055b
<u>SapphireStealer</u>	SHA256	850a99d2039dad0c15442b40c90aa4dac16319114455ab5904aa5 1e062fe6e1, c816d0be8d180573d14d230b438a22d7dda6368b1ef1733754eda9 804f295a2f
	SHA1	6b44ab6c246c077ee0e6f51300654b3eec2fddc7, b396a8d5e30fb179f3139d28b843b57bb8ae3f47
	MD5	5c025a9e86a125bf2f2ca5c1b29b42a6, 55bb772aea4303ca373fd8940663b6bd
<u>MgBot</u>	SHA256	34395ced1d44af75c510c6709bff51c94417558304daff35a9d07c8e 628d6624, ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e 20701024, 2500aa8729f9e82765443141111614c73867f162c28b2e2283749bc 208ad9e70, a4387c36bf1a150ac3a0f6d7a3ea55170fe63e772dac41ca0bc0b775 a968498a, ab9c9017e53be3382867562915a2082cb4b3fdedc624a20d2dac58 4cb714c8d1, 00e9025b7353e427cdd0c090859ce5bd2c51a94f8f30d9a017c50c5 360cc0467, 15400a1d426333b9463f425e44af721c1005962ac245df40d63c599 5524d4434, 2b479ea7e5433c25905e872b8a397fb9c9cab9a9a5b02a636f2f507f 55446dd1, 22a7a71608d99c76caf05a3212eb724c0cda6a40f84059fbbfe313a1 1448c66e,



Attack Name	TYPE	VALUE
<u>MgBot</u>	SHA256	8a9b2dadd7643cf02a4fe4ad9c6adca2f2eba158f3c3f6853f60ee6f8a789ecb, 43a9db4a84fb27d942a67a7aac15c2d5d4ed1598d73830558f5ac072b4bd9c36, 40e34f73c1efb1de8760e0fb6af044b81fa89ff1de44e0b7e3eb8f7b51ca623a
<u>Nightdoor</u>	SHA1	7a3fc280f79578414d71d70609fbdb49ec6ad648, 70b743e60f952a1238a469f529e89b0eb71b5ef7, 59aa9be378371183ed419a0b24c019ccf3da97ec, 8591a7ee00fb1bb7cc5b0417479681290a51996e, 82b99ad976429d0a6c545b64c520be4880e1e4b8
	Filename	pidgin.dll, memmgrset.dll, default_ico_1.exe, UjGnsPwFaEtl.exe, default_ico.exe
<u>STRRAT</u>	SHA256	97e67ac77d80d26af4897acff2a3f6075e0efe7997a67d8194e799006ed5efc9, 8d72ca85103f44742d04ebca02bff65788fe6b9fc6f5a411c707580d42bbd249, 38a74520d86f5dd21bf5c447c92a9e5c0c3f69db84b1666e33d5d86784bead3a, 2743fa7e35da259564a4f879b20487577921a3e669d6deb3fa5cca3193f73952, 7ccc38e2616bfb5aef446213a4cab27cffd99e91ba1e035857344a8d5c9454b3, 595ab2d1b7478b6c6a18fec3698cb131d8115c346b0408c6667aa6561a443c2b, 7aabe909ac93d7930bc1195f092cd2f0fb7ca8dbbb543e4a3d442f6bb13121a0, 1d3219b6ccc538b8cbecb13eb9c23ce00a6ed315a2a7fecb9b791e9cd1888bd8, a36323cc7633934af9b10f0c56841e483bb886836ca94fc52ce37ca3f0cfd190, 8efa0e193fb08adf90ba95c2e7f2de6453c3276cd8ae154c4af117a48a668ef3, d38b806812c7610cc3349a2ec4b60b0fcf61a92295fe7eea72da2a255b204b5e, 26104fcd8de196afcbaf13b7a6aa150855ee64060ec9e9444db0448b3524cf80, 85ea19ebad6e8cebdbd3c188964228fab7512b8668633f621bf0d660b8f92a33
<u>TimbreStealer</u>	SHA256	e87325f4347f66b21b19cfb21c51fbf99ead6b63e1796fcb57cd2260bd720929,



Attack Name	TYPE	VALUE
<u>TimbreStealer</u>	SHA256	<p>103d3e03ce4295737ef9b2b9dfef425d93238a09b1eb738ac0e05da0c6c50028,  a579bd30e9ee7984489af95cffb2e8e6877873fd881aa18d7f5a2177d76f7bf2,  010b48762a033f91b32e315ebcefb8423d2b20019516fa8f2f3d54d57d221bdb,  024f3c591d44499afb8f477865c557fc15164ab0f35594e0cfdfa76245459762,  03cd17df83a7bdf459f16677560e69143d1788ce1fc7927200a09f82859d90ea,  075910c802f755d3178a8f1f14ee4cd7924fd4463c7491277bdf2681b16e593c,  12bff33da7d9807252bb461d65828154b9b5b1dca505e8173893e3d410d40dd0,  1aaa4fb29a88c83495de80893cd2476484af561bb29e8cdfc73ce38f6cd61a84,  23b9e4103141d6a898773b1342269334e569bcf576cdbc4a905f24e26320cdab,  27c1e41fde9bc0d5027a48ccada1af8c9c8f59937bf5f77edd21e49bd28f29a2,  2a225784289f31adbaa8be0b8770495fa8950fce2b7352a0c7a566fc79067547,  2a38b75e88f91f9cd28ef478e82c3b44f50e57cb958ba63e58f134d8bd368812,  2a3f869e9e78b4d7945a60ceec27586c07bc8b0770be64463358fffe3b6b7395,  2e04c36b7ddd6939b7bef258bfeba6f91a5c37a43389dd6d9a88eff5863df5ed,  43e99539e4b966dde2f9de8dc1ffb4a22bc560e54c01de9aef6b15fac1412714,  46226d4fb7ffe15ba8167e3724f991c543731672e19ef40bb43fddc6df648d0a,  46cc07a9287da26e238a74734d87e0aae984f4648a80a26547afa0de8c850afb,  51be3a3b4ebd15c305c0f9b57388c449f88f0d6d2d46a0a838f046f0fd21b78f,  55b0247b9b574978a4c9abd19c3bcc04ea78598398b9f8aeb35bd51cbd877576,  56612bb0ab00cbb7af24326b027a55ff25852ddab1f1c8e24471b7ce97003505,  5831f4f8ce715d4a021284e68af1b6d8040a2543484ac84b326eea20c543552e,  58562e49c1612f08e56e7d7b3ca6cd78285948018b2998e45bd425b4c79ce1f4,  62495620b0d65d94bc3d68dec00ffbe607eacd20ab43dc4471170aa292cc9b1a,  682546addb38a938982f0f715b27b4ba5cda4621e63f872f19110d174851c4e9,  69019b7b64deb5cc91a58b6a3c5e6b1b6d6665bd40be1381a70690ba2b305790,  6bf082f001f914824a6b33f9bdd56d562c081097692221fb887035e80926d583,</p>

Attack Name	TYPE	VALUE
<u>TimbreStealer</u>	SHA256	<p>7923d409959acffab49dda63c7c9c15e1bdd2b5c16f7fcfe8ef3e3108e08df87,  7ac22989021082b9a377dcc582812693ce0733e973686b607e8fc2b52dcf181d,  8420d77ba61925b03a1ad6c900a528ecacbb2c816b3e6bc62def40fc14e03b78,  850dd47a0fb5e8b2b4358bf3aa1abd7ebaae577b6fc4b6b4e3d7533313c845b8,  96363b2b9e4ed8044cb90b6619842ba8897b4392f9025cbfdccfda1ea7a14a58,  97157c8bbeb8769770c4cb2201638d9ad0103ba2fdfed9bdbd03c53bd7a5fcb9,  a103b0c604ef32e7aabb16c2a7917fd123c41486d8e0a4f43dcf6c48d76de425,  a82fb82f3aa2f6123d2c0fb954ae558ac6e8862ef756b12136fbe8d533b30573,  a92934c014a7859bd122717f4c87f6bd31896cb87d28c9fac1a6af57ff8110f6,  ab2a2465fccd7294580c11492c29a943c54415e0c606f41e08ce86d69e254ee4,  ababe815e11b762089180e5fb0b1eaffa6a035d630d7aaf1d8060bd5d9a87ea5,  b04a0a4a1520c905007a5d370ed2b6c7cb42253f4722cc55a9e475ae9ece1de7,  c29b9f79b0a34948bde1dfca3acecca6965795917c7d3444fcacba12f583fb98,  c99237a5777a2e8fa7da33460a5b477d155cc26bc2e297a8563516a708323ead,  ca652fc3a664a772dbf615abfe5df99d9c35f6a869043cf75736e6492fbd4bea,  b5a272acd842154b2069b60aab52568bbfde60e59717190c71e787e336598912,  ce135a7e0410314126cacb2a2dba3d6d4c17d6ee672c57c097816d64eb427735,  d3ff98b196717e66213ccf009cbeed32250da0e2c2748d44f4ee8fb4f704407,  feb9c5ede3964fdb3b53307a3d5ef7b0e222705a3bb39bef58e28aaba5eed28,  Ff3769c95b8a5cdcba750fda5bbbb92ef79177e3de6dc1143186e893e68d45a4</p>
<u>NerbianRAT</u>	IPv4	<p>172.86.66[.]165,  45.153.240[.]73</p>
	SHA256	<p>027d03679f7279a2c505f0677568972d30bc27daf43033a463fafee0d7234f6,  9cb6dc863e56316364c7c1e51f74ca991d734dacef9029337dde5ca684c1106,  9d11c3cf10b20ff5b3e541147f9a965a4e66ed863803c54d93ba8a07c4aa7e50</p>

Attack Name	TYPE	VALUE
<u>WARPIRE</u>	SHA256	1079e1b6e016b070ebf3e1357fa23313dcb805d3a6805088db c3ab6d39330548, e134e053a80303d1fde769e50c2557ade0852fa827bed9199e 52f67bac0d9efc
<u>MiniNerbian</u>	SHA256	d3fbae7eb3d38159913c7e9f4c627149df1882b57998c8acaac 5904710be2236, df91410df516e2bddfd3f6815b3b4039bf67a76f20aecabccffb1 52e5d6975ef, 99fd61ba93497214ac56d8a0e65203647a2bc383a2ca271601 5b3014a7e0f84d, 9ff0dcce930bb690c897260a0c5aaa928955f4ffba080c580c13 a32a48037cf7, 3367a4c8bd2bcd0973f3cb22aa2cb3f90ce2125107f9df29358 31419444d5276, f23307f1c286143b974843da20c257901cf4be372ea21d1bb5 dea523a7e2785d, f1e7c1fc06bf0ea40986aa20e774d6b85c526c59046c452d98e 48fe1e331ee4c, 926aeb3fda8142a6de8bc6c26bc00e32abc603c21acd0f9b572 ec0484115bb89, 894ab5d563172787b052f3fea17bf7d51ca8e015b0f873a893a f17f47b358efe
<u>RESHELL</u>	SHA256	1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602 576270df590b2c, 36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e 96462121c4ac1, 46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f 816bf48bff3e2, 4cb020a66fdbbc99b0bce2ae24d5684685e2b1e9219fbdfda56b 3aace4e8d5f66, 67ad30c3359b377d1964a5add97d2dc96b855940685131b30 2d5ba2c907ef355, 6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a 0f3ef809fa2716, 804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721 da402062f95a9e3, 82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1f a9ff4312846, b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b 3652df783be03a, da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92f e8d46fd2b1577, f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b153 94f22fd7315cb

Attack Name	TYPE	VALUE
<u>XDealer</u>	SHA256	10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f, 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1, 1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3, 244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a, 35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa, 3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815, 50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab, 57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829, 5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe, 6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2, 898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fca9b75afc34dce, c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c, d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578, d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3, e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213, e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36, ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272, 2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa, 8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d, 2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee, 521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a, 9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1,

Attack Name	TYPE	VALUE
<u>XDealer</u>	SHA256	9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82, bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4, d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b, fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39, 01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcd66c, 05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243, 241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8, 5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472, b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab, c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab, f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac, acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2, ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d, ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e, ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136, 4b653253049a65142f827706203de55f03abccbcdac3ed2171d79bf8186eda9, 63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d, 6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64, f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934, 992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e, bb6afc28d610bfdcd0cf3497c152c081f63137fea9914a1fd461a0706c74288, 15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45,

Attack Name	TYPE	VALUE
<u>XDealer</u>	SHA256	6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2, 98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541, a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91, bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff, ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e
<u>PlugX</u>	SHA256	42fecaa47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956, 44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448, d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519,
<u>ShadowPad</u>	SHA256	0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9, 4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014, 484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0
<u>NetSupport RAT</u>	SHA256	fef8bdf50c19a012bfdc9da3f4ea4cab39075637ca527f24af79575007b2befe, 6600d29e025b7d8d8d6d8f472685b9f800e3418200fde2350f5c30a18aa34816, f17ffde17327433256debb5f6eb3b1a29cecf79af7565861182b4a684b8c936
<u>BunnyLoader 3.0</u>	SHA256	1a5ad9ae7b0dc2ed7e93556f2c59c84f113879df380d95835fb8ea3914ed8, c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
<u>AsukaStealer</u>	MD5	2d2b66d90495c1236f2e557172bf0f1c, 7ce0bd101d349bc88b668e380093e1a9, e9dda8ccde5385e8d0a7f0bdc361e51d, 28b7d6b0a793d772c953f529742ca91f, 9ce2a046a0698212c2963f2df91ff2e1, 20017810fba85ef8ac6e4230d0e67a07, 371e14f7e146ff22cb9ebe2f78cbfb7f, 1494c8bc32576cb008c33d6f0fd1e842, 75c79796fa147bf3f4d569b544ee0547, 2de37ffcae86c673de3cd2ee5e2ad3b1
	SHA1	a06d203ae9cbe26a3c2e389f1c361ac49ef54c08, 45fc72df60f39ebe77d4012f34a10e73eb2fd485, 863734caf0cb94dce610fe49eebe438a7096dfb,

Attack Name	TYPE	VALUE
<u>AsukaStealer</u>	SHA1	fc33fe3deb280d9ed94e3add58134660433bdb18,69a2d82f13246761e6d5159efb78b8fa91856380,d7b6530a4c7d685e9ee6765231bab14fecdadeba,2fde663b31a46e83f3034464674ad3f3a85f6972,4b3cdfbeaa9f8dc3554a0f9a54fc0d16334a46ed,5c6a4cd4b9271410cc45ccda00a2531631f35136,09f2187f0228eed3df41c76c69d94da789c0f2f1
	SHA256	24bb4fc117aa57fd170e878263973a392d094c94d3a5f651fad7528d5d73b58a,00cc1ef3d307750d5cdbe537da606101e90091b6020c71f696e454aee11c9a98,5b2b8a4d5b8375a3ac2ce68b93cdbfcd8fd13d1cf4ea1a6a61bd784aa495dbfb,5f2016f22935cea6fa5eafe1e185d6a9b4c14c4b2aa8619ec15a539358cac928,6b0e95d68da6d029a4af645a408c0608218e853f11c8ba70a14b06ec2a005424,9ac629ed8e07b6c99b05edd46b86e1795e5f96908ab1fe85a06282b0a982cd1b,bb17d47f10fefcee4c883f93f2989e753b969298dd70262ae00696dd482dc9b4,c534f184b8ea3887161ec2b364de15e61ee9a4053f8902450383d3f4165fc818,dc723d302340d27529b8c3c880b4cf53534a02e2a71a68f39eec30f239c2c988,e6430183aa7bbaffa89ffbef7bfac3aa54481e904556ab71ea20ccf55dfce53f,0e5470a33fd87b813ecf72370f9e1f491515c12f41c8ea3c7bbc169ac56acda5,476171dd2eb7f118d3e0aff32b7264d261ba4c2d9fa6c14ccff6d8d99b383db4
<u>Jasmin ransomware</u>	SHA256	56942b36d5990f66a81955a94511298fd27cb6092e467110a7995a0654f17b1a,32a630decb8fcc8a7ed4811f4293b9d5a242ce7865ab10c19a16fc4aa384bf64
<u>SparkRAT</u>	SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697
<u>AcidRain</u>	MD5	1bde1e4ecc8a85cffef1cd4e5379aa44
	SHA1	b5de486086eb2579097c141199d13b0838e7b631
	SHA256	6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728
<u>AcidPour</u>	IP	185[.]61[.]137[.]155
	Domains	solntsepek[.]com, solntsepek[.]info, solntsepek[.]org, solntsepek[.]ru



Attack Name	TYPE	VALUE
<u>xRAT</u>	SHA256	ef43b756295b1499b8fa6a9dd04bfd1f81e9bb4793d44a17e24d0b9a36ad5ec9, 91ef2b2e677a31da2c612928fe4f8739cc5a480a6b6249c085a8ed9ec8d8b0aa, fe347fb042b7e6317a8ff943e6019233bbae119d13028617c72e62dbfbad49f4, bf82a1616a1f282b948701e5f2fb63bae085ae39b7eb02921672aebd252ef556, 8a87018ee3dea100ad87628ca9c895b5450b1ea405dbbceb9746c68ba514607b, db377e4193c8c1fd0d3ebffab816b1e3fdffd40 added46378de7f5584c164010ff, e76ffc328b95e3117f5b34bf10925b4afcac6dd2c21a67bc736c92499e670a25, 9f2ed0f3f8a657063c12f442541e4130fd51bfa096fc1fe1809ec6b74b5ba2a0, a41e196cc8e426b7f3100e3683e0adfca4c6db99155d47f7ad035a522e9dd38a, 53cace88c1271c20edd6a445b1ee093c57678cd8c77ba0c7f117eb8bc0cff689, f39a48abb806b47dbc417775c18096c6a9131bf049a33c4b5f441c7a38ddf9b6, 0571e73e271c55ebaae39339c519d7263479f05ee2940ebef8a8f66f8e744c64, e7a3902c6bc36da4d9b75973790ae9b1b868ee10e07ba1443e8c893b70d41b16, bfd43fe95304c3ee54a74c00bac1e4a3cdd198ba2ca26345290fb1f6f7bbee8c, 3872dd2093334f00b3bedb4e9816934549f1dd0274cc8f6c31eb93f2b885acca, d150b62c99bb028179fda24cc176486817b4c38366ef132dea6b5b23d02d4ff6, ecb3e3068a9118565b6d18eb2e6533b327cbc2b90a2ad466e372a6d4eddc508d, 19ad3b30384fa1bc38095d1e0a46811cfef1f6d0b145f764cb048d2d72be57d3, 13b3b9ad32e283f54f4339d0d4849796003f1fd7cdd2f83c419b07e953758b1a, 71003754ffab0ae9d10ad27e290fa9317d377bc32403c3ab08e3c740069b5780, 71e4d35156e913340d32d565806004c2297bfb05b747874279830e34056dbce, 9126b515fbd12299376087ce4ad5eb17570ce77f851abf7244756a2798a3bccb, 9d5f67efc28610cfa459199076c3580c6370d3b74526318b663429c2e9c08d87, 726b67b85e531994ac728d9dbc6c412208a1db0bcde5f29e8f58841b05c81429,



Attack Name	TYPE	VALUE
<u>xRAT</u>	SHA256	f26e49e9ee43830c241200161ca59ddec1ac840745ce73a3d9163c190f41824c, 3becd141d8cc82cf81b106864a37f2e21d1f55d7d6a88af450a a5564245129da, b18b9fd76d06b0221f087447f2220d5e275814e460d36c7ce5 b13937adf4c2a6, 7aca9b72f131a601f825051068927625e294b5f38dce44530c4 cc68cc178662a, d2b79474e38f3a760729e3f5008febad36c81376ffd74234b5e ef3b462f63e87, c38957198bc36ebfa50505e4089d324e857cbf63aab6b09b8f8 64f1d14ebfc31, b75d1f664da0541ce2d77fbfc31c653eba13fbf136a456eefe5ef 417f0ff6f05, 6ea913e13d4e76ddcc6fa3b24feb283e165093d57fd6649fbca a33fb14a6f7d3, 06091017eef3ee19006a38e4d966e2b0fb9dc359aa2d500eda a98c6b228ea3bd, 607f36b00f244eaede1939dee34708925c383b5c0a9934a95e 801d2f539aea77
<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
	SHA256	0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d 34ce58d5f799a, e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c 026d6d55b9a1, f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f 5619b30f3a2e,

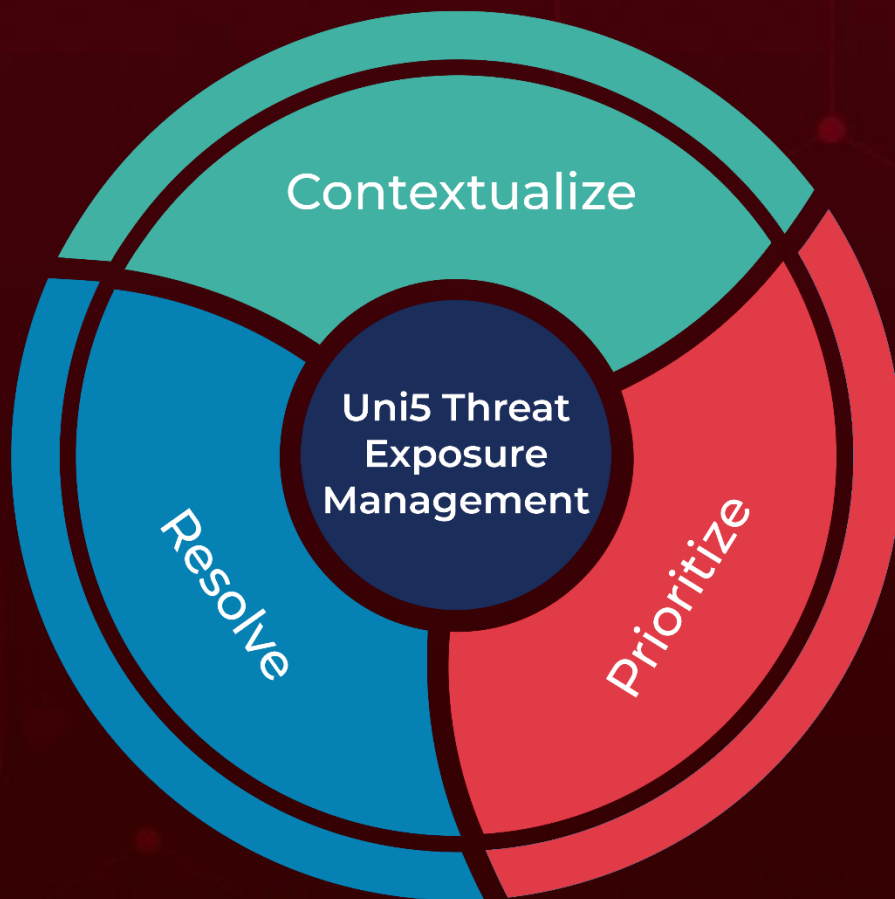
Attack Name	TYPE	VALUE
<u>StrelaStealer</u>	SHA256	aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054, b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680, 3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b, 544887bc3f0dcc610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45
<u>Agenda ransomware</u>	SHA256	73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a, e4cbee73bb41a3c7efc9b86a58495c5703f08d4b36df849c5bebc046d4681b70, afe7b70b5d92a38fb222ec93c51b907b823a64daf56ef106523bc7acc1442e38
<u>Sysrv Botnet</u>	SHA256	1ba8f42d8db461bb45f9d3e991c137b7b504aee5213cfe7a12cd4b366512696e,
<u>XMRig</u>	SHA256	6fb9b4dced1cf53a9533ed497f38550915f9e448e62a6f43e9d8b696bd5375dc, f0a299b93f1a2748edd69299f694d3a12edbe46485d29c1300172d4ac4fd09d4, 495500dcd8b3fa858335f0c85ddcc265f09ed638d87226e8bce8b53ef626464e, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b, 7cbe0c55b3ca5d12be640e519e4399469399b3eaada20705342fa681befe8c7b, 01db4578f5fb7b29800f7b07a31fda7ff812309f62f7148fca0e246279f6ca61
<u>SNOWLIGHT</u>	MD5	c867881c56698f938b4e8edafe76a09b, df4603548b10211f0aa77d0e9a172438, 0951109dd1be0d84a33d52c135ba9c97, 0ba435460fb7622344eec28063274b8a, a78bf3d16349eba86719539ee8ef562d
<u>SUPERSHELL</u>	URL	hxxp[:]//[172.245.68[.]110:8888
<u>GOREVERSE</u>	SHA256	9e1527fc21622f99b1bce657cda6ad243b0854763eaa0cec45b2c6a64cae9846, 2b54d1c064892a22f48b5742ba6da55bf62b73e5b1e0649e8b7880b286498735, 4d3570a0c63109786a10ff66eaf0c6c134715dc33e5c85e701ba0cc8cf139df2

Attack Name	TYPE	VALUE
<u>HackBrowserData</u>	SHA256	4dd0b10dac5966bb0126269e2bd65216980f054e77047fcfff126ae6b20484a6, 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 • 10:30 PM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)