

Date of Publication
March 1, 2024



HiveForce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

FEBRUARY 2024

Table Of Contents

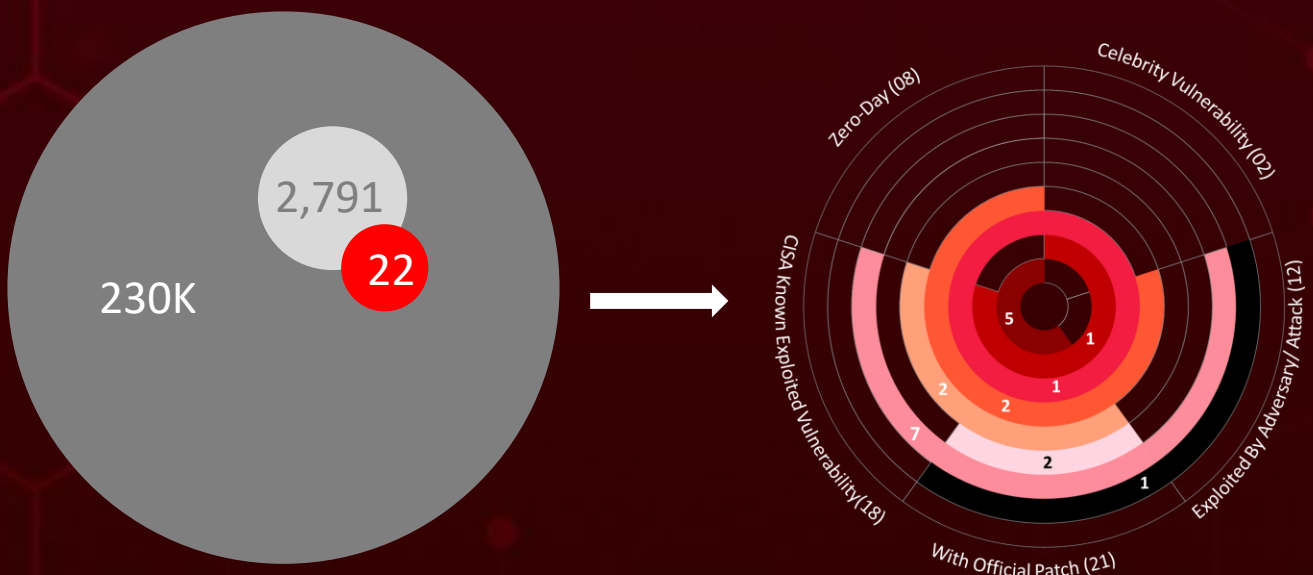
<u>Summary</u>	03
<u>Insights</u>	04
<u>Threat Landscape</u>	05
<u>Vulnerabilities Summary</u>	06
<u>Attacks Summary</u>	09
<u>Adversaries Summary</u>	13
<u>Targeted Products</u>	15
<u>Targeted Countries</u>	17
<u>Targeted Industries</u>	18
<u>Top MITRE ATT&CK TTPs</u>	19
<u>Top Indicators of Compromise (IOCs)</u>	20
<u>Vulnerabilities Exploited</u>	24
<u>Attacks Executed</u>	36
<u>Adversaries in Action</u>	52
<u>MITRE ATT&CK TTPS</u>	65
<u>Top 5 Takeaways</u>	71
<u>Recommendations</u>	72
<u>Hive Pro Threat Advisories</u>	73
<u>Appendix</u>	74
<u>Indicators of Compromise (IoCs)</u>	75
<u>What Next?</u>	88

Summary

In **February**, the cybersecurity landscape witnessed a surge in attention due to the discovery of **eight zero-day** vulnerabilities. Zero-Day in Ivanti, ScreenConnect, and Microsoft are currently under widespread exploitation. Particularly concerning is the exploitation of ScreenConnect by various threat actors, who are deploying ransomware, RATs, and other malware. Security teams are urged to promptly patch their systems to mitigate these risks.

During the same period, ransomware attacks experienced a noticeable uptick, with strains such as **Blackcat, Abyss Locker, LockBit and Akira** 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, **fourteen adversaries** were active across diverse campaigns. The **LockBit Gang** has resurged following enforcement takedowns, while **BlackCat** has made a significant comeback, causing critical disruptions in the US healthcare sector. Organizations must promptly patch vulnerabilities and implement robust cybersecurity measures to effectively defend against such persistent threats.



- Total Vulnerabilities Published
- Vulnerabilities Published in the Month
- Exploited Vulnerabilities

Volt Typhoon

PRC-affiliated threat actor targeting United States critical infrastructure employing LOTL techniques

Ivanti continues to bleed with **Zero-day**, CVE-2024-21893, an SSRF flaw in the SAML component chained with CVE-2024-21887 to achieve unauthenticated RCE

FritzFrog Botnet

FritzFrog Golang-based botnet reveal in its iterations, the employment of an exploit called Frog4Shell, capitalizing on the Log4Shell vulnerability

UAC-0027

Targets Ukrainian organization, affecting over 2000 computers with DIRTYMOE (PURPLEFOX) malware

Uninstall VMware EAP Plug-in

Vmware urged admins to uninstall the outdated Enhanced Authentication Plug-in owing to newly found critical vulnerabilities enabling session hijacking and authentication relay attacks

CVE-2024-1709 critical vulnerability in ScreenConnect exploited in wild by many threat actors including Ransomware groups like BlackBasta, B100dy and Blackcat

Blackcat

Blackcat strikes US healthcare, causing widespread disruption and chaos

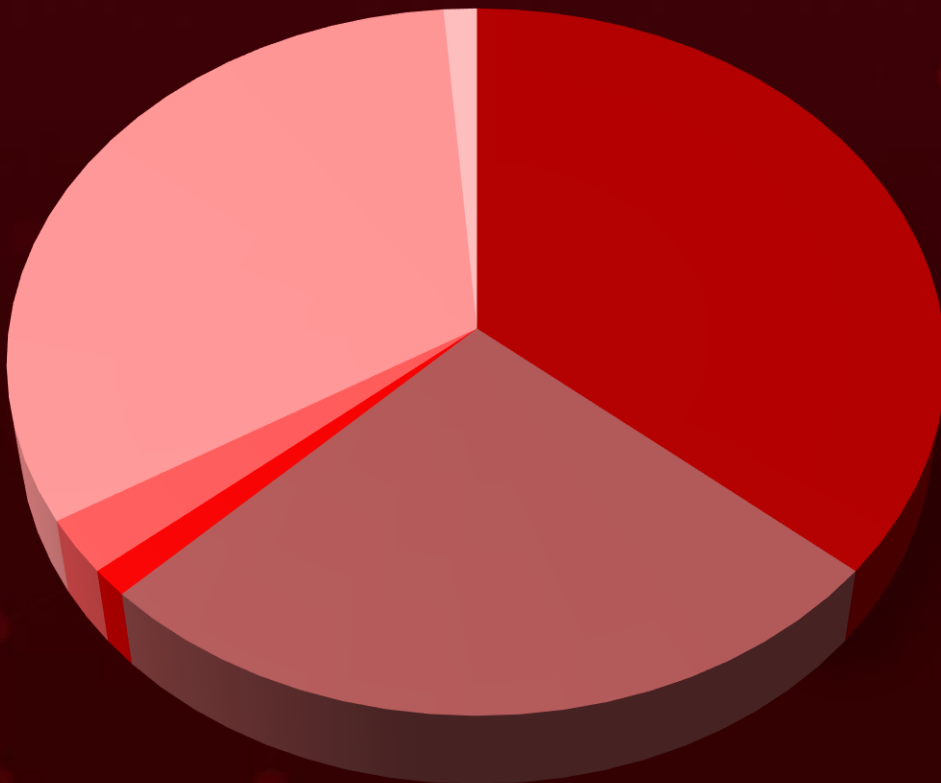
Lockbit

has resurfaced within a week despite significant crackdowns by enforcement agencies

In February 2024, a geopolitical cybersecurity landscape unfolds, revealing **Germany, US, Italy, and Belgium** as the top-targeted countries

Highlighted in February 2024 is a cyber battleground encompassing the **Financial, Technology, Engineering, Construction, and Energy** sectors, designating them as the top industries

Threat Landscape










































- Malware Attacks
- Man-in-the-Middle Attack
- Injection Attacks
- Social Engineering
- Denial-of-Service Attack
- Password Attack



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons ServerSide Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA			
CVE-2021-4034	PwnKit (Polkit's Privilege Escalation Vulnerability)	Polkit pkexec utility			
CVE-2021-44228	Log4Shell (Apache Remote Code Execution Vulnerabilities)	Apache Log4j			
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows			
CVE-2024-23917	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity			
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-2024-21762	Fortinet FortiOS SSL-VPN Out-of-Bounds Write Vulnerability	Fortinet FortiOSSSL-VPN			
CVE-2024-21351	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows SmartScreen			
CVE-2024-21412	Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Internet Shortcut Files			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	WinRAR			
CVE-2024-21410	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server			
CVE-2020-3259	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)			
CVE-2024-22245	VMware Arbitrary Authentication Relay Vulnerability	Enhanced Authentication Plug-in (EAP): All versions			
CVE-2024-1708	ConnectWise ScreenConnect Path-Traversal Vulnerability	ScreenConnect			
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ScreenConnect			
CVE-2023-43770	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube			
CVE-2024-23204	Apple Security features bypass Vulnerability	MacOS and iOS devices			
CVE-2016-0099	Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability	Microsoft Windows			
CVE-2019-7481	SonicWall SMA100 SQL Injection Vulnerability	SonicWall SMA100			
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server			
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server			






Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
EMPTYSPACE	Downloader	-	-	-	Phishing
QUIETBOARD	Backdoor	-	-	-	Phishing
DSLog backdoor	Backdoor	CVE-2024-21893, CVE-2024-21888	Connect Secure, Policy Secure, and Ivanti Neurons for ZTA		Exploiting Vulnerabilities
DIRTYMOE	Modular malware	-	Windows	-	-
FritzFrog	Botnet	CVE-2021-4034, CVE-2021-44228	Polkit pkexec utility, Apache Log4j		Log4Shell vulnerability
Mispadu	Infostealer	CVE-2023-36025	Windows		Exploiting vulnerability
XPhase	Clipper	-	-	-	Social Engineering, Phishing
Albatat	Ransomware	-	AWS, Office365, PayPal, Sendgrid, and Twilio	-	Social Engineering
Coyote	Trojan	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Zardoor	Backdoor	-	-	-	-
RustDoor	Backdoor	-	MacOS	-	-
Rhysida	Ransomware	-	-	-	Phishing
DarkMe	RAT	CVE-2024-21412, CVE-2023-36025	Windows		Phishing
TinyTurla-NG	Backdoor	-	-	-	Phishing
TurlaPower-NG	Backdoor	-	-	-	Phishing
Bumblebee	Loader	-	-	-	Phishing
SNS Sender	Hack Tool	-	-	-	Phishing
Akira	Ransomware	CVE-2020-3259	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)		Exploiting Vulnerabilities
POWERSTAR	Backdoor	-	-	-	Through deceptive webinar portal
POWERLESS	Backdoor	-	-	-	Through deceptive webinar portal
NOKNOK	Backdoor	-	-	-	Through deceptive webinar portal
BASICSTAR	Backdoor	-	-	-	Through deceptive webinar portal

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
EYEGLOSS	Backdoor	-	-	-	Through deceptive webinar portal
TrollAgent	Infostealer	-	Windows	-	Phishing
MrAgent	Hack Tool	-	-	-	-
Mario	Ransomware	-	-	-	Infected email attachments (macros), torrent websites, malicious ads
VietCredCare	Infostealer	-	-	-	-
DOPLUGS	Modular	-	-	-	Spearphishing Emails
LockBit	Ransomware	CVE-2024-1708 CVE-2024-1709	ConnectWise ScreenConnect		Exploiting Vulnerabilities
AsyncRAT	RAT	CVE-2024-1708 CVE-2024-1709	ConnectWise ScreenConnect	-	Exploiting Vulnerabilities, spear-phishing, malvertising, exploit kit
Migo	Miner	-	-	-	Phishing
Abyss Locker	Ransomware	-	Windows, Linux	-	SSH brute force attacks
Xeno RAT	RAT	-	Windows	-	Social Engineering
Blackcat Ransomware	Ransomware	CVE-2016-0099 CVE-2019-7481 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 CVE-2024-1709 CVE-2024-1708	Windows, Linux, and VMware ESXi, ConnectWise ScreenConnect	-	Social Engineering and Remote Access Tools

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BlackBasta Ransomware	Ransomware	CVE-2024-1708 CVE-2024-1709	ConnectWise ScreenConnect		Phishing, Exploiting Vulnerabilities
BLOODY Ransomware	Ransomware	CVE-2024-1708 CVE-2024-1709	ConnectWise ScreenConnect		Exploiting Vulnerabilities
XWORM	RAT	CVE-2024-1708 CVE-2024-1709	ConnectWise ScreenConnect		Exploiting Vulnerabilities
WINELOADER	Backdoor	-	-	-	Phishing












Adversaries Summary





ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNC4990	Financial gain	Unknown	-	EMPTYSPACE, QUIETBOARD	-
UAC-0027	Financial gain, Information Theft and Espionage	-	-	DIRTYMOE	Windows
Volt Typhoon	Information theft and espionage	China	-	-	-
Water Hydra	Financial gain and Espionage	-	-	DarkMe RAT	Windows
Turla	Information theft and espionage	Russia	-	TinyTurla-NG (TTNG) and TurlaPower-NG	-
Charming Kitten	Information theft and espionage	Iran	-	POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLOSS	-
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	-	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Kimsuky group	Information theft and espionage	North Korea	-	TrollAgent	-
RansomHouse group	Information theft and espionage	-	-	MrAgent, Mario Ransomware	-
Earth Preta	Information theft and espionage	China	-	DOPLUGS	-
LockBit Gang	Financial gain	Unknown	-	LockBit Ransomware	Windows, Linux, MacOS and VMware Exsi
Doppelgänger	Information theft and espionage	Russia	-	-	-
Blackcat	Financial gain	-	CVE-2016-0099 CVE-2019-7481 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 CVE-2024-1709	Blackcat Ransomware	Windows, Linux, and VMware ESXi
SPIKEDWINE	Information theft and espionage	-	-	WINELOADER	-



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Security Solution	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA
	Software	Runc and BuildKit
	System Software	Runc and BuildKit
	Operating System	Microsoft Windows
	Software	Microsoft Windows SmartScreen
	Operating System	Microsoft Exchange Server
	System Software	Polkit pkexec utility
	Software	Apache Log4j
	Software	JetBrains TeamCity
	VPN	Fortinet FortiOS SSL-VPN
	Software Program	Zoom Desktop Client, Zoom VDI Client, Zoom Rooms Client and Zoom Meeting SDK for Windows
	Software	RARLAB WinRAR
	Security Solution	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
 CONNECTWISE	Software	ConnectWise ScreenConnect
	Software	Roundcube Webmail
	Operating System	MacOS and iOS devices
 by Broadcom	Utility	VMware Enhanced Authentication Plug-in (EAP)

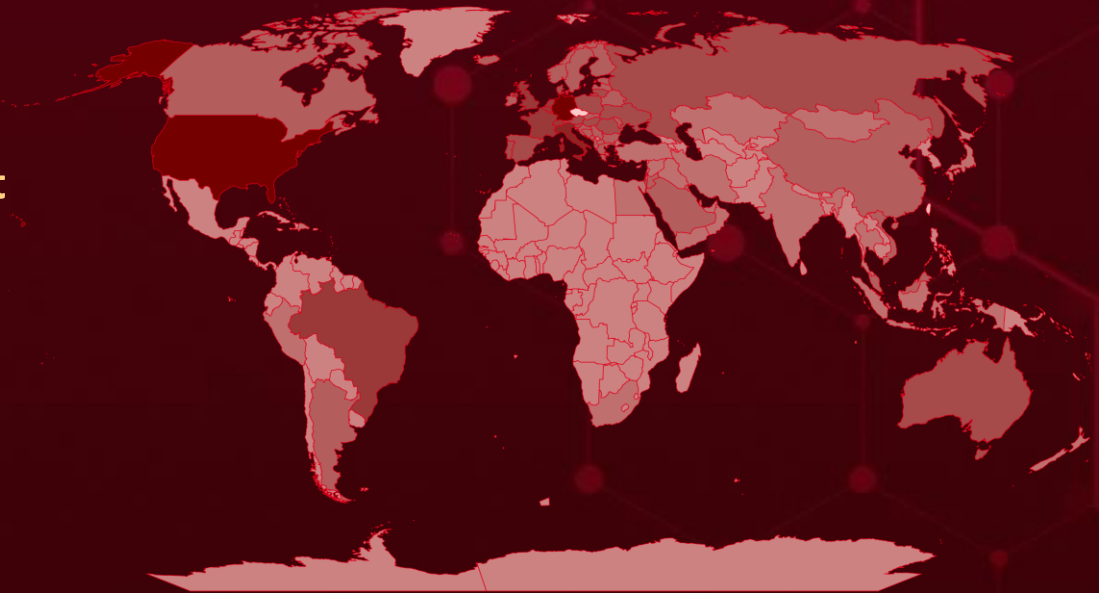


Targeted Countries

Most



Least



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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
Dark Red	Germany	Dark Red	Lithuania	Dark Red	San Marino	Dark Red	Egypt	Dark Red	Colombia
Dark Red	United States	Dark Red	Liechtenstein	Dark Red	Malta	Dark Red	Iran	Dark Red	Ghana
Dark Red	Italy	Dark Red	North Macedonia	Dark Red	Serbia	Dark Red	Kazakhstan	Dark Red	Comoros
Dark Red	Belgium	Dark Red	Saudi Arabia	Dark Red	Moldova	Dark Red	Thailand	Dark Red	Guinea
Dark Red	Netherlands	Dark Red	Qatar	Dark Red	Iceland	Dark Red	Mongolia	Dark Red	Kenya
Dark Red	Brazil	Dark Red	Czech Republic (Czechia)	Dark Red	Argentina	Dark Red	Oman	Dark Red	Haiti
Dark Red	Switzerland	Dark Red	Ireland	Dark Red	Sweden	Dark Red	Singapore	Dark Red	Kiribati
Dark Red	France	Dark Red	Bulgaria	Dark Red	Montenegro	Dark Red	Peru	Dark Red	Tunisia
Dark Red	United Kingdom	Dark Red	Canada	Dark Red	Croatia	Dark Red	India	Dark Red	Congo
Dark Red	Spain	Dark Red	Belarus	Dark Red	Albania	Dark Red	Indonesia	Dark Red	Cambodia
Dark Red	Portugal	Dark Red	China	Dark Red	Jordan	Dark Red	Yemen	Dark Red	Kyrgyzstan
Dark Red	Monaco	Dark Red	Latvia	Dark Red	Kuwait	Dark Red	Gabon	Dark Red	Eswatini
Dark Red	Denmark	Dark Red	Slovakia	Dark Red	Syria	Dark Red	Timor-Leste	Dark Red	Laos
Dark Red	Russia	Dark Red	Vietnam	Dark Red	South Africa	Dark Red	Somalia	Dark Red	Antigua and Barbuda
Dark Red	Australia	Dark Red	Bosnia and Herzegovina	Dark Red	United Arab Emirates	Dark Red	Algeria	Dark Red	Costa Rica
Dark Red	Luxembourg	Dark Red	Andorra	Dark Red	Bahrain	Dark Red	Venezuela	Dark Red	Saint Kitts & Nevis
Dark Red	Hungary	Dark Red	Norway	Dark Red	Lebanon	Dark Red	Central African Republic	Dark Red	Côte d'Ivoire
Dark Red	Poland	Dark Red	Estonia	Dark Red	Cyprus	Dark Red	Senegal	Dark Red	Sao Tome & Principe
Dark Red	Israel	Dark Red	Greece	Dark Red	Turkey	Dark Red	Chad	Dark Red	Barbados
Dark Red	Romania	Dark Red	Finland	Dark Red	Dominican Republic	Dark Red	Sudan	Dark Red	Seychelles
Dark Red	Austria	Dark Red	Holy See	Dark Red	Iraq	Dark Red	Chile	Dark Red	Zambia
Dark Red	Slovenia	Dark Red		Dark Red	Japan	Dark Red	Uganda	Dark Red	Grenada
Dark Red		Dark Red		Dark Red	New Zealand	Dark Red	Ethiopia	Dark Red	Libya
Dark Red		Dark Red		Dark Red		Dark Red	Bangladesh	Dark Red	
Dark Red		Dark Red		Dark Red		Dark Red	Samoa	Dark Red	

Targeted Industries

Most



Financial



Technology



Engineering



Construction



Energy



Healthcare



Manufacturing



Government



Education



Transportation



Cryptocurrency



NGOs



Media



Banking



Defence



Agriculture



Professional Services



Utilities



Retail



Real Estate



Automotive



Electrical



Tele-communications



Logistics



Oil & Gas



Legal



Research Organizations



Think-Tanks



Hospitality



Aerospace



Consumers



Food products



Pharmaceutical



Gaming



Political Entities



Aviation

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1027

Obfuscated Files or Information

T1566

Phishing

T1588.006

Vulnerabilities

T1082

System Information Discovery

T1588

Obtain Capabilities

T1036

Masquerading

T1055

Process Injection

T1190

Exploit Public-Facing Application

T1204

User Execution

T1105

Ingress Tool Transfer

T1041

Exfiltration Over C2 Channel

T1204.001

Malicious Link

T1486

Data Encrypted for Impact

T1059.001

PowerShell

T1204.002

Malicious File

T1059.003

Windows Command Shell

T1566.002

Spearphishing Link

T1068

Exploitation for Privilege Escalation

T1083

File and Directory Discovery

T1140

Deobfuscate/Decode Files or Information

T1078

Valid Accounts

T1562

Impair Defenses

T1588.005

Exploits

T1555

Credentials from Password Stores



Top Indicators of Compromise (IOCs)




Attack Name	TYPE	VALUE
<u>FritzFrog</u>	SHA256	f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d, fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291
<u>Albat</u>	SHA256	e1c399c29b9379f9d1d3f17822d4496fce8a5123f57b33f00150f287740049e9, ce5c3ec17ce277b50771d0604f562fd491582a5a8b05bb35089fe466c67eef54, 483e0e32d3be3d2e585463aa7475c8b8ce254900bacfb9a546a5318fff024b74, 614a7f4e0044ed93208cbd4a5ab6916695e92ace392bc352415b24fe5b2d535c, bfb8247e97f5fd8f9d3ee33832fe29f934a09f91266f01a5fed27a3cc96f8fbb
	File Path	%USERPROFILE%\Albatat\Albatat.ekey, %USERPROFILE%\Albatat\Albatat_Logs.log, %USERPROFILE%\Albatat\personal_id.txt, %USERPROFILE%\Albatat\readme\README.html, %USERPROFILE%\Albatat\readme\assets\banner.jpg, %USERPROFILE%\Albatat\readme\assets\script.js, %USERPROFILE%\Albatat\readme\assets\style.css, %USERPROFILE%\Albatat\readme\pages\faq.html, %USERPROFILE%\Albatat\wallpaper_albatat.jpg
<u>Rhysida</u>	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f, f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab, 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd, 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31efceb7f6, 3d2013c2ba0aa1c0475cab186ddf3d9005133fe5f88b5d8604b46673b96a40d8, 67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d9401928ba5, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595, 3518195c256aa940c607f8534c91b5a9cd453c7417810de3cd4d262e2906d24f, d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee




Attack Name	TYPE	VALUE
<u>DarkMe RAT</u>	SHA256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc, b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb, bf9c3218f5929dfecbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c, dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54
<u>Bumblebee</u>	SHA256	a5b39fc06464b347af81f13c5994c2bcef15001b35b4e78e4f4677ea b858cb1d, 8695f4936f2942d322e2936106f78144f91602c7acace080e48c97e97b888377, f5eb4c8c087cc070b23ebbd5b58c781e843436932a10fae1966c642a0ef83820
	URL	hxxp[:]//213[.]139.205.131/w_ver.dat
	Domain	q905hr35[.]life
	IP	49.13.76[.]144:443
<u>Akira</u>	SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddcccd5bb37857e7bde6d2eb7, 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f, f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92, ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af, aca0f5e76dacc4b9145c17a25a639aeb2e4cf76b7859bcb27224c42e404013a2,

Attack Name	TYPE	VALUE
<u>Akira</u>	SHA256	08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba, ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab, 030db5fb2a639b0c1a63bbd209bd1f043dbc4dbb306102f1726cdd4a6500fb83, b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2, 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3, 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db, 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4, 5009343ce7e6e22a777b22440480fe2eb26098d4a2ecc62e6df4498819e26b5c
<u>BASICSTAR</u>	SHA1	cdce8a3e723c376fc87be4d769d37092e6591972, 1f974d7634103536e524a41a79046785ca7ae3d6, 729346dfdd2203a9943119bac03419d63554c4b8, 09b527ddb848d7697f34ab34c2bce30da6f24238, 2a2610344bf8db66b1e13302e54e4ef77712aada, 25005352eff725afc93214cac14f0aa8e58ca409
	MD5	2edea0927601ef443fc31f9e9f8e7a77, 78e4975dc56e62226f4c56850efb452b, 3fbf3ce1a9b452421970810bd6b6b37a, a517bcb4d8c24dfe750110a91252c26c, e851147f1d5dc5236ed2085cd5e513e7, 853687659483d215309941dae391a68f
<u>DOPLUGS</u>	SHA256	651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859, f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5, 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6, b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb, 88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b, 12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd, 71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591Bf573f3787, 3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b, a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916, 17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82,

Attack Name	TYPE	VALUE
<u>DOPLUGS</u>	SHA256	d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc, d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adb e27724c4, c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1 a08320692, 39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c61 19f901a, 42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdc dfa44ad5, 9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f 2478c1c58




Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21893		Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*.:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*.:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1588.006: Vulnerabilities	https://forums.ivanti.com/s/product-downloads/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4034		Polkit pkexec utility	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:polkit_project:polkit:*.:*:*:*:*	FritzFrog Botnet
PwnKit (Polkit's Privilege Escalation Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125 CWE-787	T1068: Exploitation for Privilege Escalation	https://access.redhat.com/security/vulnerabilities/RHSB-2022-001




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>		Apache Log4j: 2.0 - 2.14.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:* *:*:*:*	FritzFrog Botnet
Log4Shell (Apache Remote Code Execution Vulnerabilities)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917 CWE-502 CWE-20 CWE-400	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-36025</u>		Windows: 10 - 11 23H2 & Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server-*:*:*:*:* cpe:2.3:o:microsoft:windows_*:*:*:*:*	Mispadu infostealer
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
CWE-254	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-23917</u>		TeamCity: 2017.1 - 2023.11.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity: *	-
			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
JetBrains TeamCity Authentication Bypass Vulnerability	CWE-288 CWE-306	T1190: Exploit Public-Facing Application, T1588: Obtain Capabilities	https://www.jetbrains.com/teamcity/download/other.html https://download.jetbrains.com/teamcity/plugins/internal/fix CVE 2024 23917.zip https://download.jetbrains.com/teamcity/plugins/internal/fix CVE 2024 23917_pre2018




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-22024</u>		Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1), Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1588: Obtain Capabilities, T1190: Exploit Public-Facing Application, T1005: Data from Local System, T1046: Network Service Discovery	https://forums.ivanti.com/s/product-downloads/




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




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21351		Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	-
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.002 User Execution: Malicious File, T1553.005 Subvert Trust Controls: Mark-of-the-Web Bypass	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21412		Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	Water Hydra (aka DarkCasino)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*	DarkMe RAT
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.001 User Execution: Malicious Link, T1036.008 Masquerading: Masquerade File Type	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-38831</u>		WinRAR version 6.22 and older versions	APT 28, DarkPink, Konni, APT 40, Sandworm and APT 29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*	BumbleBee, DarkMe, GuLoader, Remcos RAT, SmokeLoader, Nanocore RAT, Crimson RAT, AgentTesla, BOXRAT and Rhadamanthysinfo stealer
WinRAR Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1204.001 User Execution: Malicious Link, T1203 : Exploitation for Client Execution	Update WinRAR version to 6.23 or later versions Link: https://www.winrar.com/signlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21410</u>		Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2016:cu23:*:*:*:*:*	-
Microsoft Exchange Server Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-668	T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21410




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-3259</u>		Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*	Akira Ransomware
Cisco ASA and FTD Information Disclosure Vulnerability		cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-22245</u>		Enhanced Authentication Plug-in (EAP): All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:Enhanced AuthenticationPlug-in:*:*:*:*:*:*	-
VMware Arbitrary Authentication Relay Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1588.006: Vulnerabilities, T1068: Exploitation for Privilege Escalation	Uninstall the EAP Plugin




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
<u>CVE-2024-1708</u>		ScreenConnect 23.9.7 and prior	-	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*.*	LockBit Ransomware, BlackBasta Ransomware, BLOODY Ransomware, Blackcat Ransomware, XWORM, and AsyncRAT	
ConnectWise ScreenConnect Path-Traversal Vulnerability			ASSOCIATED TTPs	PATCH DETAILS
	CWE ID		T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://screenconnect.connectwise.com/download




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
<u>CVE-2024-1709</u>		ScreenConnect 23.9.7 and prior	Blackcat	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*.*	LockBit Ransomware, BlackBasta Ransomware, BLOODY Ransomware, Blackcat Ransomware, XWORM, and AsyncRAT	
ConnectWise ScreenConnect Authentication Bypass Vulnerability			ASSOCIATED TTPs	PATCH LINK
	CWE ID		T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities, T1068: Exploitation for Privilege Escalation	https://screenconnect.connectwise.com/download




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-43770</u>		Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	
Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1588.006: Vulnerabilities, T1204: User Execution	https://roundcube.net/news/2023/09/15/security-update-1.6.3-released




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-23204</u>		macOS and iOS devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*	
Apple Security features bypass Vulnerability		cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*	-
		cpe:2.3:o:apple:macos:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1588.006: Vulnerabilities, T1204: User Execution, T1083: File and Directory Discovery	https://support.apple.com/en-us/HT214061 , https://support.apple.com/en-us/HT214060 , https://support.apple.com/en-us/HT214059

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2016-0099</u>		Microsoft Windows	Blackcat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows .*.*.*.*.*.*.*	Blackcat Ransomware
Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	https://learn.microsoft.com/en-us/securityupdates/securitybulletins/2016/ms16-032

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-7481</u>		SonicWall SMA100	Blackcat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_100 _firmware:.*.*.*.*.*.*.* cpe:2.3:h:sonicwall:sma_100 :.*.*.*.*.*.*.*	Blackcat Ransomware
SonicWall SMA100 SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1055.002 Process Injection	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-31207</u>		Microsoft Exchange Server	Blackcat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.:*:*:*:*	Blackcat Ransomware
Microsoft Exchange Server Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1588.006: Vulnerabilities	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34473</u>		Microsoft Exchange Server	Blackcat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.:*:*:*:*	Blackcat Ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34523</u>		Microsoft Exchange Server	Blackcat
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_*.~*~*~*~*~*	Blackcat Ransomware
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523

✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>EMPTYSPACE (aka VETTA Loader and BrokerLoader)</u>	EMPTYSPACE is a downloader that can execute any payload served by the command and control (C2) server, and deliver backdoor.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Deploy Backdoor	-
ASSOCIATED ACTOR			PATCH LINK
UNC4990			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>QUIETBOARD</u>	QUIETBOARD is a Python-based pre-compiled multi-component backdoor. It includes the ability to execute arbitrary commands, manipulate clipboard content for cryptocurrency theft, infect USB or removable drives, capture screenshots, gather system information, and communicate with a C2 server.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
UNC4990			-

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>DSLog backdoor</u>	The DSLog backdoor operates by injecting encoded commands into SAML authentication requests, enabling attackers to execute operations such as system information retrieval and filesystem permissions manipulation.	Exploiting Vulnerabilities	CVE-2024-21893 CVE-2024-21888
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	Connect Secure, Policy Secure, and Ivanti Neurons for ZTA
ASSOCIATED ACTOR			PATCH LINK
-			https://forums.ivanti.com/s/product-downloads

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>DIRTYMOE (aka PURPLEFOX)</u>	The DIRTYMOE malware, also known as PURPLEFOX, is modular and has been a prominent player in the cyber threat landscape for over half a decade. It utilizes a rootkit to hinder removal and self-propagates by exploiting vulnerabilities and using authentication data.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular malware		Data Theft, and DDoS	Windows
ASSOCIATED ACTOR			PATCH LINK
UAC-0027			-

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>FritzFrog</u>	The FritzFrog Golang-based botnet reveals in its iterations, the employment of an exploit called 'Frog4Shell,' capitalizing on the Log4Shell vulnerability.	Log4Shell vulnerability	CVE-2021-4034 CVE-2021-44228
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet			Polkit pkexec utility, Apache Log4j
ASSOCIATED ACTOR			PATCH LINK
-			https://access.redhat.com/security/vulnerabilities/RHSB-2022-001 https://logging.apache.org/log4j/2.x/security.html
		Data theft and Financial Loss	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mispadu</u>	The Mispadu Stealer, an infostealer that emerged in 2019. The malware employs sophisticated techniques to evade detection, including bypassing SmartScreen warnings by utilizing crafted .url files pointing to malicious binaries on a threat actor's network share.	Leverages the CVE-2023-36025 vulnerability	CVE-2023-36025
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer			Windows
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025
		Data Theft	

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>Xphase</u>	The XPhase Clipper malware replaces cryptocurrency wallet addresses copied by users with addresses under the control of the attacker. Enabling attackers to reroute funds to their wallets instead of the intended recipients.	Social Engineering, Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Clipper		Harvest credentials, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Albatat (aka White Bat)</u>	Albatat ransomware, made its debut in November 2023, emerging as a financially motivated threat crafted in Rust. Victims are then directed to a ransom note, instructing them to initiate contact with the perpetrator, with demands for a ransom of 0.0015 Bitcoin.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Financial Loss	AWS, Office365, PayPal, Sendgrid, and Twilio.
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Coyote</u>	Coyote is a new banking trojan and is currently targeting more than 60 banking institutions, primarily in Brazil. The malware distributes itself using the Squirrel installer and executes its infection process using Node.js and Nim, a relatively new multi-platform programming language.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Financial loss and System Disruption	-
ASSOCIATED ACTOR			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>Zardoor</u>	Zardoor is a backdoor malware program that was first discovered in March 2021. It's designed to give attackers remote access to a compromised system, allowing them to steal data, install other malware, or launch further attacks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RustDoor</u>	RustDoor is a backdoor malware program that specifically targets macOS devices. It was first discovered in November 2023 and has been linked to the ALPHV/BlackCat and Black Basta ransomware groups.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			MacOS
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Rhysida</u>	The Rhysida ransomware-as-a-service (RaaS) group poses a significant global threat, targeting diverse sectors. Recently, researchers developed a decryptor for it, enabling victims of the Rhysida ransomware to recover their encrypted data without any cost.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			-
ASSOCIATED ACTOR			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>DarkMe RAT</u>	DarkMe RAT, short for Remote Access Trojan, is a malicious program developed by the Evilnum APT group. It has been in circulation since at least September 2021 and has evolved significantly over time, becoming increasingly sophisticated and dangerous.	Phishing	CVE-2024-21412 CVE-2023-36025
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			Windows
ASSOCIATED ACTOR			PATCH LINK
Water Hydra (aka DarkCasino)			Data Theft and install other malware

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>TinyTurla-NG (TTNG)</u>	TinyTurla-NG (TTNG) is a new backdoor malware developed by the Turla APT group, a Russian cyberespionage group active since at least 2004. It was first discovered in December 2023 targeting a Polish non-governmental organization (NGO).	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Turla			Data Theft and install other malware

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>TurlaPower-NG</u>	TurlaPower-NG is a malicious PowerShell script used by the Turla APT group to exfiltrate data from compromised systems. It was discovered in December 2023 and is associated with the TinyTurla-NG backdoor malware. TurlaPower-NG specifically targets files related to password management software, indicating an intent to steal login credentials.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>Bumblebee</u>	BumbleBee, a malicious loader discovered in March 2022, resurfaced in the cyber threat landscape on February 8, 2024, after a four-month hiatus. Unlike in previous campaigns, this attack chain diverges from conventional techniques.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Loader			-	
ASSOCIATED ACTOR			Data Theft and install other malware	PATCH LINK
-			-	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>SNS Sender</u>	SNS Sender, a Python script that uses AWS Simple Notification Service (SNS) to send bulk SMS messages for the purpose of phishing, aka Smishing.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
Hack Tool			-	
ASSOCIATED ACTOR			Smishing	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>Akira Ransomware</u>	<p>Akira ransomware operations were initiated in March 2023. It operates through a Ransomware-as-a-Service (RaaS) model, featuring distinctive payment choices and double extortion methods. Actors behind Akira practice multi-extortion tactics and host a TOR-based (.onion) website where victims are listed along with any stolen data should a victim fail to comply with the ransom demands.</p>	Exploiting Vulnerabilities	CVE-2020-3259
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
ASSOCIATED ACTOR			PATCH LINK
-		Encrypts files, System Compromise	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>POWERSTAR</u>	<p>POWERSTATS is a backdoor written in powershell. Its capabilities, include the ability to remotely execute PowerShell and CSharp commands, establish persistence through diverse methods, dynamically update configurations, utilize multiple C2 channels, and conduct system reconnaissance and monitoring of existing persistence mechanisms.</p>	Through deceptive webinar portal	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten		Steal Data	-

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>POWERLESS</u>	POWERLESS is a PowerShell backdoor that contains a broad feature set including AES-encrypted communication, downloading executables, downloading files, executing shell commands, screenshot capture.	Through deceptive webinar portal	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Execute file and commands, capture Screenshots	-
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>NOKNOK</u>	NokNok is a backdoor that infiltrates Mac computers, often disguised as a legitimate app, stealing files and collecting user information. It can capture screenshots, record videos and audio, and install other viruses on the infected Mac, often without the user's knowledge.	Through deceptive webinar portal	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BASICSTAR</u>	BASICSTAR, a Visual Basic Script (VBS) malware, is capable of gathering basic system information, remotely executing commands relayed from a command-and-control (C2) server, and downloading and displaying a decoy PDF file.	Through deceptive webinar portal	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Exfiltrate data and System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten			-

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>EYEGLOSS</u>	EYEGLOSS malware is capable of extracting sensitive information from compromised hosts. EYEGLOSS had been set up as the default handler for the TIF file extension	Through deceptive webinar portal	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Data Theft	PATCH LINK
Charming Kitten			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>TrollAgent</u>	TrollAgent Infostealer provides the ability to steal a variety of information related to web browsers, including credential information, cookies, bookmarks, history, and extensions stored in Chrome and Firefox web browsers.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer			
ASSOCIATED ACTOR		Data Theft	PATCH LINK
Kimsuky group			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>MrAgent</u>	A new tool named 'MrAgent' is created by Ransomhouse group that automates the deployment of its data encrypter across multiple VMware ESXi hypervisors. MrAgent's core function is to identify the host system, turn off its firewall, and then automate the ransomware deployment process across multiple hypervisors simultaneously, compromising all managed VMs.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Hack Tool			
ASSOCIATED ACTOR		Data Theft	PATCH LINK
RansomHouse 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
<u>Mario Ransomware</u>	Mario ransomware is operated by Ransom House. It was found in a Joint Campaign with BianLian and White Rabbit targeting publicly-traded financial services firms. It uses .emario extension for its files.	Infected email attachments (macros), torrent websites, malicious ads	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypts files, System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
RansomHouse group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>VietCredCare</u>	VietCredCare's core functionality to filter out Facebook credentials. VietCredCare is marketed as a Stealer-as-a-Service, making it "alarmingly" accessible to cybercriminals who wish to exploit stolen data.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>DOPLUGS</u>	It is a customized version of the PlugX backdoor known as DOPLUGS. DOPLUGS is a downloader with four backdoor commands, one of the commands is designed to download the general type of the PlugX malware.	Spearphishing Emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular		Data Theft, execute commands	-
ASSOCIATED ACTOR			PATCH LINK
Earth Preta			-

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>LockBit Ransomware</u>	LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network.	Exploiting Vulnerabilities	CVE-2024-1708 CVE-2024-1709
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
-		Encrypts files, System Compromise	https://screenconnect.connectwise.com/download

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>AsyncRAT</u>	AsyncRAT is a remote access trojan (RAT) released in 2019, primarily as a credential stealer and loader for other malware, including ransomware. It is designed to remotely monitor and control other computers through a secure encrypted connection.	Exploiting Vulnerabilities, spear-phishing, malvertising, exploit kit	CVE-2024-1708 CVE-2024-1709
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
Earth Preta		Encrypt data, System Compromise	https://screenconnect.connectwise.com/download

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Migo</u>	Migo is a novel Golang ELF binary that comes fitted with compile-time obfuscation and the ability to persist on Linux machines. It aims to compromise Redis servers for the purpose of mining cryptocurrency on the underlying Linux host.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Miner			-
ASSOCIATED ACTOR			PATCH LINK
-		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
<p><u>Abyss Locker ransomware (aka AbyssLocker)</u></p> <p>TYPE</p> <p>Ransomware</p> <p>ASSOCIATED ACTOR</p> <p>-</p>	<p>Abyss Locker ransomware surfaced in July 2023, deriving from the HelloKitty ransomware source code. The Abyss Locker threat actor steals victims' data before deploying and running its ransomware malware for file encryption. The ransomware is also capable of deleting Volume Shadow Copies and system backups.</p>	SSH brute force attacks	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt files, System Compromise	Windows, Linux
			PATCH LINK
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<p><u>Xeno RAT</u></p> <p>TYPE</p> <p>RAT</p> <p>ASSOCIATED ACTOR</p> <p>-</p>	<p>Xeno-RAT is an open-source RAT developed in C#, has been made available on GitHub. It has a SOCKS5 reverse proxy and real-time audio recording capability, as well as a Hidden Virtual Network Computing (HVNC) module.</p>	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		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>Blackcat Ransomware</u>	<p>BlackCat is the first prominent malware written in the Rust programming language. It is operated as a ransomware-as-a-service (RaaS). Its campaigns often employ a triple-extortion tactic: making individual ransom demands for the decryption of infected files; for not publishing stolen data; and for not launching denial of service (DoS) attacks.</p>	Social Engineering and Remote Access Tools	CVE-2016-0099 CVE-2019-7481 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 CVE-2024-1709
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data, System Compromise	Windows, Linux, and VMware ESXi, ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
Blackcat			https://screenconnect.connectwise.com/download

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BlackBasta Ransomware</u>	<p>Black Basta is a ransomware group operating as ransomware-as-a-service (RaaS) that was initially spotted in April 2022. Black Basta uses double extortion as part of its modus operandi, exfiltrating sensitive company data and using the publication of this as a second threat to affected companies</p>	Phishing, Exploiting Vulnerabilities	CVE-2024-1708 CVE-2024-1709
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data, System Compromise	ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
-			https://screenconnect.connectwise.com/download

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>Bl00dy Ransomware</u>	Bl00dy malicious program is part of the Babuk ransomware family. It encrypts files and appended their names with a ".bl00dy" extension.	Exploiting Vulnerabilities	CVE-2024-1708 CVE-2024-1709	
		IMPACT	AFFECTED PRODUCTS	
TYPE Ransomware		ASSOCIATED ACTOR -	Encrypt data, System Compromise	ConnectWise ScreenConnect
				PATCH LINK
				https://screenconnect.connectwise.com/download

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>XWORM</u>	XWorm malware presents a significant threat to systems running Windows operating systems. This malicious software exhibits a range of capabilities, including the ability to remotely control desktops, steal sensitive information, and execute ransomware attacks.	Exploiting Vulnerabilities	CVE-2024-1708 CVE-2024-1709	
		IMPACT	AFFECTED PRODUCTS	
TYPE RAT		ASSOCIATED ACTOR -	Data Theft	ConnectWise ScreenConnect
				PATCH LINK
				https://screenconnect.connectwise.com/download


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>WINELOADER</u>	New modular backdoor WINELOADER has a modular design, with encrypted modules downloaded from the C2 server. The backdoor employs techniques, including re-encryption and zeroing out memory buffers, to guard sensitive data in memory and evade memory forensics solutions.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
Encrypt data		-	
		PATCH LINK	
		-	
TYPE			
Backdoor			
ASSOCIATED ACTOR			
SPIKEDWINE			


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
 <u>UNC4990</u>	Unknown	Health, Transportation, Construction, and logistics	Italy
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	EMPTYSPACE, QUIETBOARD	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1071: Application Layer Protocol; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1566: Phishing; T1113: Screen Capture; T1082: System Information Discovery; T1016: System Network Configuration Discovery; T1614: System Location Discovery			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>UAC-0027</u>	-	-	Ukraine
	MOTIVE		
	Financial gain, Information Theft and Espionage	-	
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DIRTYMOE (also known as PURPLEFOX)	Windows
TTPs			
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1569.002: Service Execution; T1569: System Services; T1218.007: Msiexec; T1218: System Binary Proxy Execution; T1014: Rootkit; T1027: Obfuscated Files or Information; T1055: Process Injection; T1071.004: DNS; T1071: Application Layer Protocol; T1059: Command and Scripting Interpreter			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Volt Typhoon (aka Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, Insidious Taurus)</u></p>	China	Communications, Energy, Transportation Systems, and Water and Wastewater Systems	United States, Canada, Australia, and New Zealand
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	TARGETED CVEs		
-	-	-	


TTPs


TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; T1592: Gather Victim Host Information; T1589: Gather Victim Identity Information; T1589.002: Email Addresses; T1590: Gather Victim Network Information; T1591: Gather Victim Org Information; T1593: Search Open Websites/Domains; T1594: Search Victim-Owned Websites; T1583.003: Botnet; T1584.005: Botnet; T1584.004: Server; T1587.004: Exploits; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.004: Unix Shell; T1047: Windows Management Instrumentation; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1006: Direct Volume Access; T1070.009: Clear Persistence; T1070.001: Clear Windows Event Logs; T1070.004: File Deletion; T1036.005: Match Legitimate Name or Location; T1112: Modify Registry; T1027.002: Software Packing; T1218: System Binary Proxy Execution; T1110.002: Password Cracking; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1003.001: LSASS Memory; T1003.003: NTDS; T1552: Unsecured Credentials; T1552.004: Private Keys; T1087.001: Local Account; T1010: Application Window Discovery; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1654: Log Enumeration; T1046: Network Service Discovery; T1120: Peripheral Device Discovery; T1069: Permission Groups Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1082: System Information Discovery; T1614: System Location Discovery; T1016.001: Internet Connection Discovery; T1033: System Owner/User Discovery; T1007: System Service Discovery; T1124: System Time Discovery; T1563: Remote Service Session Hijacking; T1021.007: Cloud Services; T1021.001: Remote Desktop Protocol; T1550: Use Alternate Authentication Material; T1078.004: Cloud Accounts; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1074: Data Staged; T1113: Screen Capture; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1090: Proxy; T1090.001: Internal Proxy; T1090.003: Multi-hop Proxy; T1048: Exfiltration Over Alternative Protocol

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Water Hydra (aka DarkCasino)</u></p>	-	Finance, Cryptocurrency, Forex and Stock trading, Banking, Gambling sites and Casinos	Worldwide
	MOTIVE Financial gain and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DarkMe RAT	Windows
	TTPs		
TA0001: Initial Access ; TA0010: Exfiltration ; TA0004: Privilege Escalation ; TA0042: Resource Development ; T1566.002: Spearphishing Link ; T1566: Phishing ; T1204: User Execution ; T1204.001: Malicious Link; T1105: Ingress Tool Transfer ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow ; T1588.006: Vulnerabilities; T1588: Obtain Capabilities ; T1588.005: Exploits ; T1559: Inter-Process Communication ; T1559.001: Component Object Model; T1218: System Binary Proxy Execution; T1218.011: Rundll32 ; T1547.001:Registry Run Keys /Startup Folder; T1547: Boot or Logon Autostart Execution ; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell ; T1585: Establish Accounts ; T1585.001: Social Media Accounts; T1586: Compromise Accounts ; T1586.001: Social Media Accounts ; T1584: Compromise Infrastructure ; T1584.004: Server; T1211: Exploitation for Defense Evasion ; T1218.007 : Msiexec; T1140: Deobfuscate/Decode Files or Information ; T1027: Obfuscated Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa)</u></p>	Russia	Finance, Cryptocurrency, Forex and Stock trading, Banking, Gambling sites and Casinos	Poland
	MOTIVE		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	TinyTurla-NG (TTNG) and TurlaPower-NG	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1070: Indicator Removal; T1566: Phishing; T1102: Web Service; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1083: File and Directory Discovery; T1056: Input Capture; T1560: Archive Collected: Data; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1552: Unsecured Credentials; T1552.004: Private Keys; T1555: Credentials from Password Stores; T1555.005: Password Managers			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress)</u></p>	Iran	Defense, Energy, Financial, Government, Healthcare, IT, Manufacturing, Oil and gas, Technology, Telecommunications, Politics, Think Tanks, NGOs, Journalists	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, Afghanistan, Brazil, Canada, Morocco, Pakistan, Spain, UK, USA, Venezuela
	MOTIVE		
	Information theft and espionage	TARGETED CVEs	AFFECTED PRODUCTS
		POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLASS	
TTPs			
TA0043: Reconnaissance; 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; T1595: Active Scanning; T1587.001: Malware; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1059.003: Windows Command Shell; T1569.002: Service Execution; T1555.003: Credentials from Web Browsers; T1018: Remote System Discovery; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1001: Data Obfuscation; T1566.002: Spearphishing Link; T1059.001: PowerShell; T1036: Masquerading; T1055: Process Injection; T1123: Audio Capture; T1105: Ingress Tool Transfer; T1070.004: File Deletion; T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES			
 <p><u>Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Who is Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</u></p>	North Korea	Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchanges	Worldwide			
	MOTIVE					
	Information theft and espionage, Sabotage and destruction, Financial crime	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS			
	-	-	-	TTPs		
<p>TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1078: Valid Accounts; T1070: Indicator Removal; T1140: Deobfuscate/Decode Files or Information; T1040: Network Sniffing; T1046: Network Service Discovery; T1021: Remote Services; T1213: Data from Information Repositories; T1001: Data Obfuscation; T1071: Application Layer Protocol; T1572: Protocol Tunneling; T1041: Exfiltration Over C2 Channel; T1566: Phishing; T1566.001: Spearphishing Attachment</p>						

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)</u></p>	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Construction	Japan, South Korea, Thailand, USA and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	TrollAgent	-	


TTPs

TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0005: Defense Evasion; TA0011: Command and Control; TA0009: Collection; TA0006: Credential Access; T1217: Browser Bookmark Discovery; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1204: User Execution; T1204.002: Malicious File; T1036: Masquerading; T1584: Compromise Infrastructure; T1608.001: Upload Malware; T1608: Stage Capabilities; T1027.002: Software Packing; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1005: Data from Local System; T1480: Execution Guardrails; T1027: Obfuscated Files or Information

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>RansomHouse group</u></p>	-	Construction, Engineering, Healthcare, Electric Utilities, Financial Services	USA, Indonesia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	MrAgent, Mario Ransomware	-	


TTPs

TA0001: Initial Access; TA0002: Execution; TA0042: Resource Development; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1016: System Network Configuration Discovery; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1059.004: Unix Shell; T1071: Application Layer Protocol; T1078.002: Domain Accounts; T1190: Exploit Public-Facing Application; T1486: Data Encrypted for Impact; T1560: Archive Collected Data; T1567.002: Exfiltration to Cloud Storage; T1583.004: Server; T1588.001: Malware

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Earth Preta (aka Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, Stately Taurus)</u></p>	China	Aviation, Education, Government, NGOs, Think Tanks, Telecommunications	Australia, Bangladesh, Belgium, Bulgaria, China, Cyprus, Czech, Ethiopia, France, Germany, Greece, Hong Kong, Hungary, India, Indonesia, Japan, Mongolia, Myanmar, Malaysia, Nepal, Pakistan, Philippines, Russia, Singapore, Slovakia, South Africa, South Korea, South Sudan, Sweden, Taiwan, Thailand, UK, USA, Vietnam and UN
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	DOPLUGS	-	


TTPs

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; T1583.004: Server; T1587.001: Malware; T1585.002: Email Accounts; T1588.002: Tool; T1608.001: Upload Malware; T1608.005: Link Target; T1566.002: Spearphishing Link; T1090: Proxy; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1574.002: DLL Side-Loading; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1036.005: Match Legitimate Name or Location; T1070.009: Clear Persistence; T1564.001: Hidden Files and Directories; T1056.001: Keylogging; T1083: File and Directory Discovery; T1016.001: Internet Connection Discovery; T1049: System Network Connections Discovery; T1082: System Information Discovery; T1012: Query Registry; T1091: Replication Through Removable Media; T1005: Data from Local System; T1025: Data from Removable Media; T1071.001: Web Protocols; T1573: Encrypted Channel


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>LockBit Gang</u>	Unknown	Government, Food and Agriculture, Education, Technology, Manufacturing, Aviation, Defense, Energy, Financial, Healthcare, Transportation	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LockBit Ransomware	Windows, Linux, MacOS and VMware Exsi

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1219: Remote Access Software; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1482: Domain Trust Discovery; T1072: Software Deployment Tools; T1003: OS Credential Dumping; T1095: Non-Application Layer Protocol; T1003.001: LSASS Memory; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1572: Protocol Tunneling; T1082: System Information Discovery; T1219: Remote Access Software; T1046: Network Service Discovery; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1219: Remote Access Software; T1071.001: Web Protocols; T1048: Exfiltration Over Alternative Protocol; T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1566: Phishing; T1078: Valid Accounts; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1072: Software Deployment Tools; T1569.002: Service Execution; T1569: System Services; T1547: Boot or Logon Autostart Execution; T1548: Abuse Elevation Control Mechanism; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1480.001: Environmental Keying; T1480: Execution Guardrails; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1562: Impair Defenses; T1046: Network Service Discovery; T1486: Data Encrypted for Impact; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.006: Vulnerabilities

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Doppelgänger</u>	Russia-aligned	Government, Media	Germany, the United States, Israel, and France
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0003: Persistence; TA0002: Execution; TA0040: Impact; TA0005: Defense Evasion; TA0011: Command and Control; TA0043: Reconnaissance; TA0042: Resource Development; T1140: Deobfuscate/Decode Files or Information; T1593: Search Open Websites/Domains; T1491.002: External Defacement; T1491: Defacement; T1104: Multi-Stage Channels; T1583.001: Domains; T1583: Acquire Infrastructure; T1585: Establish Accounts; T1593.001: Social Media; T1059.007: JavaScript; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1585.001: Social Media Accounts			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES	
 <p><u>Blackcat (aka ALPHV, ALPHVM, UNC4466)</u></p>	Unknown	Healthcare, Oil and gas, Education, Petroleum, Chemical, Energy, Logistics, Finance, Manufacturing, Legal services, Technology, Transport, Engineering, Professional services, Construction and Retail	Worldwide	
	MOTIVE			
	Financial gain	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS	Blackcat Ransomware
	TARGETED CVEs	-	CVE-2016-0099 CVE-2019-7481 CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 CVE-2024-1709	
TTPs				
<p>TA0003: Persistence; TA0002: Execution; TA0008: Lateral Movement; TA0004: Privilege Escalation; TA0011: Command and Control; TA0042: Resource Development; TA0005: Defense Evasion; TA0040: Impact; TA0001: Initial Access; TA0006: Credential Access; T1569: System Services; T1027: Obfuscated Files or Information; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1110: Brute Force; T1562: Impair Defenses; T1588: Obtain Capabilities; T1564: Hide Artifacts; T1486: Data Encrypted for Impact; T1210: Exploitation of Remote Services; T1078: Valid Accounts; T1505: Server Software Component; T1021: Remote Services; T1068: Exploitation for Privilege Escalation; T1040: Network Sniffing; T1041: Exfiltration Over C2 Channel; T1046: Network Service Scanning; T1047: Windows Management Instrumentation; T1106: Native API; T1119: Automated Collection; T1553: Subvert Trust Controls; T1105: Ingress Tool Transfer; T1598: Phishing for Information; T1555: Credentials from Password Stores; T1558: Steal or Forge Kerberos Tickets; T1557: Adversary-in-the-Middle; T1562.001: Disable or Modify Tools; T1562.009: Safe Mode Boot; T1489: Service Stop; T1057: Process Discovery; T1649: Steal or Forge Authentication Certificates; T1588.003: Code Signing Certificates; T1529: System Shutdown/Reboot; T1566: Phishing</p>				

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SPIKEDWINE	Unknown	Diplomats	Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	WINELOADER	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1204.002: Malicious File; T1656: Impersonation; T1204.001: Malicious Link; T1574.002: DLL Side-Loading; T1055.001: Dynamic-link Library Injection; T1573.001: Symmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1584: Compromise Infrastructure; T1053.005: Scheduled Task; T1547.001: Registry Run Keys / Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1036.001: Invalid Code Signature; T1036.004: Masquerade Task or Service; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1218.005: Mshta; T1033: System Owner/User Discovery; T1071.001: Web Protocols; T1001.001: Junk Data; T1598.002: Spearphishing Attachment			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1591: Gather Victim Org Information	
	T1593: Search Open Websites/Domains	T1593.001: Social Media
	T1594: Search Victim-Owned Websites	
	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
	T1595: Active Scanning	
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
	T1596: Search Open Technical Databases	
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
		T1588.002: Tool
		T1588.001: Malware
	T1585: Establish Accounts	T1588.003: Code Signing Certificates
		T1585.001: Social Media Accounts
	T1584: Compromise Infrastructure	T1585.002: Email Accounts
		T1584.004: Server
	T1587: Develop Capabilities	T1584.005: Botnet
		T1587.004: Exploits
	T1583: Acquire Infrastructure	T1587.001: Malware
		T1583.003: Virtual Private Server
		T1583.004: Server
	T1586: Compromise Accounts	T1583.001: Domains
	T1608: Stage Capabilities	T1586.001: Social Media Accounts
		T1608.001: Upload Malware
	T1608.005: Link Target	

Tactic	Technique	Sub-technique	
TA0001: Initial Access	T1566: Phishing	T1566.002: Spearphishing Link T1566.001: Spearphishing Attachment	
	T1190: Exploit Public-Facing Application		
	T1078: Valid Accounts	T1078.004: Cloud Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts	T1078.001: Default Accounts
		T1659: Content Injection	
		T1189: Drive-by Compromise	
	T1133: External Remote Services		
	T1091: Replication Through Removable Media		
	T1199: Trusted Relationship		
	TA0002: Execution	T1204: User Execution	T1204.002: Malicious File
T1204.001: Malicious Link			
T1059: Command and Scripting Interpreter		T1059.001: PowerShell	
		T1059.005: Visual Basic	
		T1059.003: Windows Command Shell	
		T1059.004: Unix Shell	
		T1059.007: JavaScript	
		T1059.002: AppleScript	
		T1059.006: Python	
T1569: System Services		T1569.002: Service Execution	
T1047: Windows Management Instrumentation			
T1203: Exploitation for Client Execution			
T1053: Scheduled Task/Job		T1053.003: Cron	
		T1053.005: Scheduled Task	
T1559: Inter-Process Communication	T1559.001: Component Object Model		
T1072: Software Deployment Tools			
T1106: Native API			
TA0003: Persistence	T1098: Account Manipulation		
	T1078: Valid Accounts	T1078.004: Cloud Accounts	
		T1078.002: Domain Accounts	
		T1078.003: Local Accounts	
		T1078.001: Default Accounts	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder	
	T1133: External Remote Services		
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading	
		T1574.006: Dynamic Linker Hijacking	
	T1037: Boot or Logon Initialization Scripts	T1037.001: Logon Script (Windows)	
	T1543: Create or Modify System Process	T1543.001: Launch Agent	
		T1543.002: Systemd Service	
		T1053.003: Cron	
T1053: Scheduled Task/Job	T1053.005: Scheduled Task		
T1136: Create Account			
T1505: Server Software Component			

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1098: Account Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.004:]Cloud Accounts
		T1078.002: Domain Accounts
		T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.012:]Process Hollowing
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.006: Dynamic Linker Hijacking
	T1037: Boot or Logon Initialization Scripts	T1037.001: Logon Script (Windows)
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.002: Systemd Service
		T1053.005: Scheduled Task
T1053: Scheduled Task/Job	T1053.003: Cron	
T1134: Access Token Manipulation		
T1548: Abuse Elevation Control Mechanism		
T1484: Domain Policy Modification	T1484.001: Group Policy Modification	
TA0005: Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
		T1036.004: Masquerade Task or Service
		T1036.001: Invalid Code Signature
	T1211: Exploitation for Defense Evasion	
	T1078: Valid Accounts	T1078.004: Cloud Accounts
		T1078.002: Domain Accounts
		T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1070: Indicator Removal	T1070.009: Clear Persistence
		T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
		T1218.011: Rundll32
T1014: Rootkit		
T1027: Obfuscated Files or Information	T1027.002: Software Packing	
	T1027.009: Embedded Payloads	
	T1027.007: Dynamic API Resolution	
	T1027.001: Binary Padding	
T1140: Deobfuscate/Decode Files or Information		
T1006: Direct Volume Access		
T1112: Modify Registry		

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1550: Use Alternate Authentication Material	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading T1574.006: Dynamic Linker Hijacking
	T1647: Plist File Modification	
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1562: Impair Defenses	T1562.004: Disable or Modify System Firewall
		T1562.001: Disable or Modify Tools
		T1562.009: Safe Mode Boot
	T1480: Execution Guardrails	T1480.001: Environmental Keying
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
		T1497.001: System Checks
	T1134: Access Token Manipulation	
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1548: Abuse Elevation Control Mechanism	
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1622: Debugger Evasion	
T1656: Impersonation		
TA0006: Credential Access	T1212: Exploitation for Credential Access	
	T1040: Network Sniffing	
	T1110: Brute Force	T1110.002: JPassword Cracking
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.003: NTDS
	T1552: Unsecured Credentials	T1552.004: Private Keys
	T1056: Input Capture	T1056.001: Keylogging
	T1558: Steal or Forge Kerberos Tickets	
	T1649: Steal or Forge Authentication Certificates	
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1614: System Location Discovery	
	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1040: Network Sniffing	
	T1083: File and Directory Discovery	
	T1018: Remote System Discovery	
	T1010: Application Window Discovery	

Tactic	Technique	Sub-technique	
TA0007: Discovery	T1217: Browser Information Discovery		
	T1654: Log Enumeration		
	T1046: Network Service Discovery		
	T1120: Peripheral Device Discovery		
	T1069: Permission Groups Discovery		
	T1057: Process Discovery		
	T1012: Query Registry		
	T1518: Software Discovery		
	T1016.001: System Network Configuration Discovery: Internet Connection Discovery		
	T1482: Domain Trust Discovery		
	T1033: System Owner/User Discovery		
	T1007: System Service Discovery		
	T1124: System Time Discovery		
	T1049: System Network Connections Discovery		
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion	
		T1497.001: System Checks	
T1087: Account Discovery	T1087.001: Local Account		
	T1087.002: Domain Account		
	T1087.003: Email Account		
T1622: Debugger Evasion			
TA0008: Lateral Movement	T1210: Exploitation of Remote Services		
	T1563: Remote Service Session Hijacking		
	T1550: Use Alternate Authentication Material		
	T1021: Remote Services	T1021.001: Remote Desktop Protocol	
		T1021.002: SMB/Windows Admin Shares	
	T1091: Replication Through Removable Media		
T1072: Software Deployment Tools			
TA0009: Collection	T1113: Screen Capture		
	T1115: Clipboard Data		
	T1560: Archive Collected Data	T1560.001: Archive via Utility	
	T1074: Data Staged		
	T1056: Input Capture		
	T1005: Data from Local System		
	T1123: Audio Capture		
	T1213: Data from Information Repositories		
	T1185: Browser Session Hijacking		
	T1056.001: Input Capture: Keylogging		
	T1025: Data from Removable Media		
	T1125: Video Capture		
	T1119: Automated Collection		
	T1557: Adversary-in-the-Middle		

Tactic	Technique	Sub-technique
TA00010: Command and Control	T1071: Application Layer Protocol	T1071.004: DNS
		T1071.001: Web Protocols
	T1659: Content Injection	
	T1105: Ingress Tool Transfer	
	T1102: Web Service	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
		T1573.001: Symmetric Cryptography
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1001: Data Obfuscation	T1001.001: Junk Data
	T1572: Protocol Tunneling	
	T1219: Remote Access Software	
	T1095: Non-Application Layer Protocol	
	T1104: Multi-Stage Channels	
TA00011: Exfiltration	T1048: Exfiltration Over Alternative Protocol	
	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0040: Impact	T1657: Financial Theft	
	T1486: Data Encrypted for Impact	
	T1529: System Shutdown/Reboot	
	T1498: Network Denial of Service	
	T1491: Defacement	T1491.002: External Defacement
	T1490: Inhibit System Recovery	
	T1489: Service Stop	

Top 5 Takeaways

#1

In February, we identified twenty-two critical vulnerabilities, including eight zero-day vulnerabilities. Zero-day vulnerabilities in Ivanti, ConnectWise, and Microsoft are currently under widespread exploitation.

#2

Throughout the month, ransomware strains including **Blackcat**, **Abyss Locker**, **LockBit** and **Akira** actively targeted victims.

#3

Numerous malware families have been observed targeting victims in the wild. These include **EMPTYSPACE**, **DIRTYMOE**, **DarkMe RAT**, **BASICSTAR**, **Xeno RAT**, and **WINELOADER**.

#4

There were a total of **14** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: Financial, Technology, Engineering, Construction, and Energy.

#5

Finally, February witnessed the persistent nature of threats, as Lockbit and Blackcat revived following federal takedowns.

Recommendations

Security Teams


































This digest can be used as a guide to help security teams prioritize the **22 significant vulnerabilities** and block the indicators related to the **14 active threat actors**, **38 active malware**, and **219 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 **22 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 (JANUARY 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							
														

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 threat 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>EMPTYSPACE</u>	SHA256	a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40, 8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d, 060882f97ace7cb6238e714fd48b3448939699e9f085418af351c42b401a1227, 8c25b73245ada24d2002936ea0f3bcc296fdcc9071770d81800a2e76bfca3617, b9ffba378d4165f003f41a619692a8898aed2e819347b25994f7a5e771045217, 84674ae8db63036d1178bb42fa5d1b506c96b3b22ce22a261054ef4d021d2c69
<u>QUIETBOARD</u>	SHA256	15d977dae1726c2944b0b4965980a92d8e8616da20e4d47d74120073cbc701b3, 26d93501cb9d85b34f2e14d7d2f3c94501f0aaa518fed97ce2e8d9347990decf, 26e943db620c024b5e87462c147514c990f380a4861d3025cf8fc1d80a74059a, 71c9ce52da89c32ee018722683c3ffbc90e4a44c5fba2bd674d28b573fba1fdc, 539a79f716cf359dceaa290398bc629010b6e02e47eaed2356074bffa072052f
<u>DIRTYMOE</u>	SHA256	6d817e8cd54c3a21f6d4aa437b16663a2a40b726014a8de1cbf9343101a0ab62, 43eef76fa966395bde56b4e3812831ca75ad010e3b8216103358deb09bdc14d1, 937e0068356e42654c9ab76cc34cf74dfa4c17b29e9439ebaa15d587757b14b0
<u>FritzFrog</u>	SHA256	f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d, fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291

Attack Name	TYPE	VALUE
<u>Mispadu</u>	SHA256	8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea, bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743edd fc53cf68789, fb3995289bac897e881141e281c18c606a772a53356cc81caf38e 5c6296641d4, 46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0 da467eaf52, 03bdae4d40d3eb2db3c12d27b76ee170c4813f616fec5257cf25a 068c46ba15f, 1b7dc569508387401f1c5d40eb448dc20d6fb794e97ae3d1da43b 571ed0486a0, e136717630164116c2b68de31a439231dc468ddcbee9f74cca511 df1036a22ea
<u>Xphase</u>	SHA256	3bd57de116ae8a4f7dc69ac6fa73358e2063ea2b9c90fcb5886c3ccd35f5c524
<u>Albabat</u>	SHA256	e1c399c29b9379f9d1d3f17822d4496fce8a5123f57b33f00150f28774049e9, ce5c3ec17ce277b50771d0604f562fd491582a5a8b05bb35089fe466c67eef54, 483e0e32d3be3d2e585463aa7475c8b8ce254900bacfb9a546a5318fff024b74, 614a7f4e0044ed93208cbd4a5ab6916695e92ace392bc352415b24fe5b2d535c, bfb8247e97f5fd8f9d3ee33832fe29f934a09f91266f01a5fed27a3cc96f8fbb
	File Path	%USERPROFILE%\Albabat\Albabat.ekey, %USERPROFILE%\Albabat\Albabat_Logs.log, %USERPROFILE%\Albabat\personal_id.txt, %USERPROFILE%\Albabat\readme\README.html, %USERPROFILE%\Albabat\readme\assets\banner.jpg, %USERPROFILE%\Albabat\readme\assets\script.js, %USERPROFILE%\Albabat\readme\assets\style.css, %USERPROFILE%\Albabat\readme\pages\faq.html, %USERPROFILE%\Albabat\wallpaper_albabat.jpg
<u>Coyote</u>	MD5	03eaccb664d517772a33255dff96020, 071b6efd6d3ace1ad23ee0d6d3eead76, 276f14d432601003b6bf0caa8cd82fec, 5134e6925ff1397dda0f3b48afec87b, Bf9c9cc94056bcdae6e579e724e8dbbd

Attack Name	TYPE	VALUE
<u>Zardoor backdoor</u>	SHA256	f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a60ef585bd2ac2, c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a218e7735561ef74, 73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c5d8cd73083095, a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e3407bc01f661d, 0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b73c208ab723bf, d267e2a6311fe4e2dfd0237652223add300b9a5233b555e131325a2612e1d7ef
	Mutexes	3e603a07-7b2d-4a15-afef-7e9a0841e4d5, 6c2711b5-e736-4397-a883-0d181a3f85ae, ThreadMutex12453
	IPv4:Port	70[.]34[.]208[.]197:10086, 140[.]82[.]33[.]130:14443, 70[.]34[.]194[.]185:14443, 139[.]84[.]232[.]245:37135, 208[.]85[.]20[.]130:37135, 139[.]84[.]229[.]192:443, 70[.]34[.]195[.]221:443, 217[.]69[.]1[.]128:14443, 108[.]181[.]20[.]36:443, 108[.]61[.]189[.]125:443
<u>RustDoor</u>	MD5	97cd4fc94c59121f903f2081df1c9981, 28bdd46d8609512f95f1f1b93c79d277, 3e23308d074d8bd4ffdb5e21e3aa8f22, 088779125434ad77f846731af2ed6781, b67f6e534d5cca654813bd9e94a125b9, cf54cba05efee9e389e090b3fd63f89b, 44fcf7253bcf0102811e50a4810c4e41, 690a097b0eea384b02e013c1c0410189, 186be45570f13f94b8de82c98eaa8f4f, 3c780bcfb37a1dfae5b29a9e7784cbf5, 925239817d59672f61b8332f690c6dd6, 9c6b7f388abec945120d95d892314ea7, 85cd1afbc026ffdfc4cd3eec038c3185, 6aaba581bcef3ac97ea98ece724b9092, bcbbf7a5f7ccff1932922ae73f6c65b7, bde0e001229884404529773b68bb3da0, 795f0c68528519ea292f3eb1bd8c632e, bc394c859fc379900f5648441b33e5fd, 0fe0212fc5dc82bd7b9a8b5d5b338d22, 835ebf367e769eeaaef78ac5743a47ca, bdd4972e570e069471a4721d76bb5efb

Attack Name	TYPE	VALUE
<u>Rhysida Ransomware</u>	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 0bb0e1fcff8ccf54c6f9ecfd4bbb6757f6a25cb0e7a173d12cf0f402a3ae706f, f6f74e05e24dd2e4e60e5fb50f73fc720ee826a43f2f0056e5b88724fa06fbab, 1a9c27e5be8c58da1c02fc4245a07831d5d431cdd1a91cd35d2dd0ad62da71cd, 2c5d3fea7ad3c9c49e9c1a154370229c86c48fbaf7044213fd85d31efcebf7f6, 3d2013c2ba0aa1c0475cab186ddf3d9005133fe5f88b5d8604b46673b96a40d8, 67a78b39e760e3460a135a7e4fa096ab6ce6b013658103890c866d9401928ba5, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 258ddd78655ac0587f64d7146e52549115b67465302c0cbd15a0cba746f05595, 3518195c256aa940c607f8534c91b5a9cd453c7417810de3cd4d262e2906d24f, d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee
<u>DarkMe RAT</u>	SHA256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c, 252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146, 594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978, 6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49, 71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc, b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb, bf9c3218f5929dfecbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c, dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54
<u>TinyTurla-NG</u>	SHA256	267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b, d6ac21a409f35a80ba9ccfe58ae1ae32883e44ecc724e4ae8289e7465ab2cf40
	Domains	anagram[.].jp, thefinetreats[.]com, caduff-sa[.]ch, jeepcarlease[.]com, buy-new-car[.]com

Attack Name	TYPE	VALUE
<u>Bumblebee</u>	SHA256	c34e5d36bd3a9a6fca92e900ab015aa50bb20d2cd6c0b6e03d070efe09ee689a, 3083ac4480bac3d3b900177ca92afd5ed279279640ac4296cf152e7d30c80d6f, afb75762094c2149d4d5f2312a4b094b34e524747d8d8a8d9e9f132601378a45, e72084687a0e6b9d22bdc51c80870d403645a7e13a1caa2d176acd7a1b10a962, 7140becbc882cab84038ad87e977cd3cb0dc864d2437eb1e2aebab78cc3eb193, 7f312a38cf00246fafd23684e7c80600f95c191bab7470e54836ce0e73fa86dd, ecc93d6cab4d59db2a75ba3ce5bbcaac048d44153973df4d13216c5df74f8d33, a5b39fc06464b347af81f13c5994c2bcef15001b35b4e78e4f4677eab858cb1d, 8695f4936f2942d322e2936106f78144f91602c7acace080e48c97e97b888377, f5eb4c8c087cc070b23ebbd5b58c781e843436932a10fae1966c642a0ef83820
	URL	hxxp[://213[.]139.205.131/w_ver.dat
	Domain	q905hr35[.]life
	IPv4:Port	49.13.76[.]144:443
<u>SNS Sender</u>	MD5	8fd501d7af71afee3e692a6880284616522d709e
<u>Akira Ransomware</u>	SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddcccd5bb37857e7bde6d2eb7, 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f, f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92, ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af, aca0f5e76dacc4b9145c17a25a639aeb2e4cf76b7859bcb27224c42e404013a2,

Attack Name	TYPE	VALUE
<u>Akira Ransomware</u>	SHA256	08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba, ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab, 030db5fb2a639b0c1a63bbd209bd1f043dbc4dbb306102f1726cdd4a6500fb83, b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2, 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3, 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db, 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4, 5009343ce7e6e22a777b22440480fe2eb26098d4a2ecc62e6df4498819e26b5c
<u>POWERSTAR</u>	SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80, 991620817274d4031889134d40294cc6e086cf56e738a8ea78c49860c6dcccde
	SHA1	2581e9bf9fa219cb1bce393f7492212612228221, e588837d652d2cd96c5cb44f8f98fd7d82cc5d30, 214bf21a567b678ec4250c1aca4cf71275e2860e, 0161ba63e65a2b39b754b9d16cf2bc62de98e99a, 5671ff66d0ea0cd93b04ca0ab35ff4e33e33833a
	MD5	f5eddfaeb353ceca4b8713f88f030604, 99dc6ab3f88629069b5109f5ed530e25, 5398e9063ee0d6189cf59c8d4403a40d, e4e8864f88724b736ec3568fd8916796, a2b407eac00422b2bc7ac59a74fc47e0
<u>POWERLESS</u>	SHA256	37bb42720bfc1cf5d0e9d7b66be134b6431055ed8bdfdf384f61ab7ac061d26eb, f1ee5dd179f66f597edfeb4b2c73c6adb4b7b6d4dcfb0bef33ee5c285148d085, a8622dccb40a9fe9c2123f661e32e0a6bc40e95c88c9c2b764e603ce5eccb311, 9ef84d6a709adbd6f29813ee145dbf542a69150e5ab4261e0d58de7ee371a8ef
	SHA1	195e939e0ae70453c0817ebca8049e51bbd4a825, 27b38cf6667936c74ed758434196d2ac9d14deae, 5bdec05bdca8176ae67054a3a7dc8c5ef0ac8deb, c3fd8ed68c0ad2a97d76fc4430447581414e7a7e

Attack Name	TYPE	VALUE
<u>POWERLESS</u>	MD5	c79d85d0b9175cb86ce032543fe6b0d5, 9b6c308f106e72394a89fac083de9934, 859a9e523c3308c120e82068829fab84, 5fc8668f9c516c2b08f34675380e2a57
<u>NOKNOK</u>	SHA256	7ce3140d5db6d716deefeaba6c5472684eddfa792a0697dbdba5f5 1a1efa682, dcb99f07abbe6b6a442e276856f1945f891628882964940d2f72b6ff 9734707d, f9437370b013c76da8cba7c07af72d816c9bc245a3d91f540fae6348 1ab0fa0d
<u>BASICSTAR</u>	SHA256	c6f91e5585c2cbbb8d06b7f239e30b271f04393df4fb81815f6556fa 4c793bb0, f6f0f682668f78dbecfc30a0e0c76b6a3d86298869fb44b39adf19fdc dca5762, 1ffc0bb577e4605059143a5cca213fbe0762c320c74174fe3c2a8f48 78c85fc0, 13b659e009577ab7890157ce00cc5c3641049f46135d5be2b1c17ca 88a1490f9, fdc5d6caaaa4fb14e62bd42544e8bb8e9b02220e687d5936a6838a7 115334c51, 07384ab4488ea795affc923851e00ebc2ead3f01b57be6bf8358d76 59e9ee407
	SHA1	cdce8a3e723c376fc87be4d769d37092e6591972, 1f974d7634103536e524a41a79046785ca7ae3d6, 729346dfdd2203a9943119bac03419d63554c4b8, 09b527ddb848d7697f34ab34c2bce30da6f24238, 2a2610344bf8db66b1e13302e54e4ef77712aada, 25005352eff725afc93214cac14f0aa8e58ca409
	MD5	2edea0927601ef443fc31f9e9f8e7a77, 78e4975dc56e62226f4c56850efb452b, 3fbf3ce1a9b452421970810bd6b6b37a, a517bcb4d8c24dfe750110a91252c26c, e851147f1d5dc5236ed2085cd5e513e7, 853687659483d215309941dae391a68f
<u>EYEGLOSS</u>	SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72 c5811d5f
<u>TrollAgent</u>	MD5	013c4ee2b32511b11ee9540bb0fdb9d1, 035cf750c67de0ab2e6228409ac85ea3, 19c2decfa7271fa30e48d4750c1d18c1, 27ef6917fe32685fdf9b755eb8e97565, 2aaa3f1859102aab35519f0d4c1585dd, 2b678c0f59924ca90a753daa881e9fd3, 4168ff8b0a3e2f7e9c96afb653d42a01, 4222492e069ac78a55d3451f4b9b9fca, 42ea65fda0f92bbe5f4535155125c7, 6097d030fe6f05ec0249e4d87b6be4a6, 62fba369711087ea37ef0b0ab62f3372,

Attack Name	TYPE	VALUE
TrollAgent	MD5	7457dc037c4a5f3713d9243a0dfb1a2c, 7b6d02a459fdaa4caa1a5bf741c4bd42, 87429e9223d45e0359cd1c41c0301836, 88f183304b99c897aacfa321d58e1840, c8e7b0d3b6afa22e801cacaf16b37355, d67abe980a397a94e1715df6e64eedc8, dc636da03e807258d2a10825780b4639, E4a6d47e9e60e4c858c1314d263aa317, 9e75705b4930f50502bcb740fc3ece1, a67cf9add2905c11f5c466bc01d554b0, b532f3dcc788896c4844f36eb6cee3d1, B97abf7b17aeb4fa661594a4a1e5c77f, 8d4af59eebdcca10f3c88049bb097a3a, 9360a895837177d8a23b2e3f79508059
	SHA1	120891212a78114fe114217012c2a000727e034b, 3d1731fa03f2bb8b3ca74ab49c83923428e58362, 4a705f58918c00431de453d5b5f621fa42ff7169, 4c8b7d968806f8108ccde6ac07a37b8174ac44bf, 4eea45c22881a092ac7a8b0a5379076d5803e83e, 6d531b021b20feb1dafa730582944eb82d9c6f3, e6be97ca9e79b45c671c6531908f70b353d47994
	URLS	hxxp://ai[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://ai[.]bananat[.]p-e[.]kr/index[.]php, hxxp://ai[.]daysol[.]p-e[.]kr/index[.]php, hxxp://ai[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://ai[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ai[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://ai[.]negapa[.]p-e[.]kr/index[.]php, hxxp://ai[.]selecto[.]p-e[.]kr/index[.]php, hxxp://ai[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ar[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ca[.]bananat[.]p-e[.]kr/index[.]php, hxxp://pi[.]selecto[.]p-e[.]kr/index[.]php, hxxp://qa[.]jaychoi[.]p-e[.]kr/index[.]php, hxxp://qi[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://sa[.]netup[.]p-e[.]kr/index[.]php, hxxp://ve[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://viewer[.]appofficer[.]kro[.]kr/index[.]php, hxxp://ce[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://coolsystem[.]co[.]kr/admin/mail/index[.]php, hxxp://dl[.]netup[.]p-e[.]kr/index[.]php, hxxp://li[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ol[.]negapa[.]p-e[.]kr/index[.]php, hxxp://pe[.]daysol[.]p-e[.]kr/index[.]php
	SHA256	2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6 d6569a55e, 61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf 832ac92,

Attack Name	TYPE	VALUE
<u>TrollAgent</u>	SHA256	6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9, 955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b, a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9, f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3, ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca
<u>MrAgent</u>	SHA256	8189c708706eb7302d7598ae8cd6bdb048bf1a6dbe29c59e50f0a39fd53973, bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c
<u>Mario Ransomware</u>	SHA256	3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e, afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501, 2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d, 2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e, 0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038, d36afcf1e1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d
<u>VietCredCare</u>	SHA256	bd9eb106e265c5d0ae7a9e9d2d5925d558128599b1ba4a4cbc29b6fc7b3f48f0, 71c4d0fc03bc4e083f64b2f80b2242618fb725efd64f362446f98c6d2051834f, b5621b540d1ca1dd802397822145ae4f80e96e59b81fdc8d0a7b18919ceadd12, 17598536cf0bac6cb0d589410682e2cd9f813ea52bc931fe85292b149dbeb659, 20ac10ea3a964c25f09b0008406388cf4195828eed6daaeda139c55ce84986f4, 8c6e6faa28f67ac56587a4dcea49c820b466113604900c3f829185a096c6df47, aababe351df7fc27a8d9a227f75850adc1fc3fe86248e59953def5b3fa9b8822, 67b095896e09acff1b2140c933d5efff0dd2a10c920b5db6518531f2304a8838, 1d92dd2e8b04e715954d2bf99e053f9b05eb89986e2b13651d17498f51d2de5d, e2b4e099b70a213f27a84b8534964a7dfd870004ebee3c5eb6601f239c5fd3a1, b3eaa35baecf562a018df53066e8ec438cac854b0bb30eba7aa34a9d8230aacb, 74ab0c6b96cfa75b474ba1fbf69b9cd8502981f85a89642c0b3aa35399a4bda,

Attack Name	TYPE	VALUE
<u>VietCredCare</u>	SHA256	e0b00681a57457af72fc53866316fc2ba1b0c99d79685ca3a4e8973d023b6426, 071001dcdcf87312fece26c4f9bec92f0e0c651eb88786d6ac4ea7ee128fe0aba, 83d3c0e4b813020aa8c2e917be86bbf8b48336960a7ac65f973e88fc05575263, 596f86cf3d2911f2817289be25621d9a1f93bd0d861b66f0fec2a9092b9eff3c, f1b430bed2b7c1c10f66d8551713c3bcc06c689f0c55a57129703feeab58927f, c4616a07ab285f8a124079e6d2afd30ea1c552804c4ac689510e5a0e85e6dd3b, 3a56c8b9269a6dd225bc150dfd6bcf058aeadd2d5196ed02cec5bf00521238d9, f791d75904f434461c0bcccc0ff3d39ab4eb04eb208e9b7eed3e71376b6820b8, 5c1ef4b5e5a8cd2a80fd5e5aee0d29eb44fedcb9dd5e73e6b5c74f17e83a19cb, 1f28712c2fabfd21aa286fa70e6191f4265d808b3880b897f4c8df5778c1b785, d305ec61046d4470559480cf724b16584e65752a37c7817b8a06b208247b2ac5, aa2ce3666ff4ede662c071d07b16d4e2fadcc6c2dd9fe76eb9fb4dc82817a5ec8, a2ac7a96a14f855caa520ce2862dbdb83d1cb278d0f9171e116926c5a40196aa, 27f377560d2ada287cb134b1d350eaa2fc15799a3845fe35c06e6d208e63bb71, d26634062b44a009eaf0cc024fd24e7d32d4117664904b86b925b2d5639e527b, 2eeb5b0e3d6e3e1f1422b6d8115a48c0fb6953e42e974a2754e079ea0de0819f, dafdfdf54ec92cf126f676947fb708f6354326ebf5f6e3fbd84022df179a1c85, ffc70cddcfdbdda5a941d53a2307567da14853442e00282c7e0bd57bc9f963a1, c1fb24f868d17673b41da5aaa8738730963f4a8e3d208420a0cd21a8f2a5470f, 257146b44136f54e976273759e3f3f671d1622797259091a37312d58933a4ea8, 987863291c7025bef2e2a7d8b5081f4bde9d1ca38172a99567004c1c44599010, 22b462e4e852a4f5b668c941780e4d01af7f9e645b6cf50a6f9154ce9d96ebe4, 14b8e34338e445d15d901f3b39fea324ef66eab686877d520a4b3a5cc86632ef
<u>DOPLUGS</u>	SHA256	651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859, f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5, 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6, b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb, 88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b, 12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd, 71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787, 3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b, a0c94205ca2ed1bcd065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916, 17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82, d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc, d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4, c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692, 39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a, 42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5, 9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58
<u>LockBit Ransomware</u>	SHA256	d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2, a35c3274a726b27cbcef5abe3f28d8f9675a30883490d37f23b4d730d72eca42, 56ff8149e3694e8cc919bec6739d599881d3bd9cb503eca7f6cc31e71f4f1df9, af4cddd01266e97f5b3ea0ccb6e3f8c21c313b2dca7cee581023ef23dbfee9ee, d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46,

Attack Name	TYPE	VALUE
<u>LockBit Ransomw are</u>	SHA256	92813f3c2973a00dc738f72acdf3014e914128a4b427dde5c19e73a87b5f38d1, f01909eee3dec5474a5a845deea3f8fb5502ac006f65060a7e945f91c966e266, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, c1b449af312de6828850d4b6810dca9982a6ee0ba91b8d1f5cb6573349d2744a, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 12b6fead37cca9d8ca4c00c2a9d56c0a402e760ab309356f078587acb7f33396, d4f150a8b26e9edccea4987433fb5b8a105970db143ba196f13652730c635668, 54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2, a35c3274a726b27cbcef5abe3f28d8f9675a30883490d37f23b4d730d72eca42, 56ff8149e3694e8cc919bec6739d599881d3bd9cb503eca7f6cc31e71f4f1df9, af4cddd01266e97f5b3ea0ccb6e3f8c21c313b2dca7cee581023ef23dbfee9ee, d4f150a8b26e9edccea4987433fb5b8a105970db143ba196f13652730c635668, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 92813f3c2973a00dc738f72acdf3014e914128a4b427dde5c19e73a87b5f38d1, f01909eee3dec5474a5a845deea3f8fb5502ac006f65060a7e945f91c966e266, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, c1b449af312de6828850d4b6810dca9982a6ee0ba91b8d1f5cb6573349d2744a, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 12b6fead37cca9d8ca4c00c2a9d56c0a402e760ab309356f078587acb7f33396
<u>AsyncRAT</u>	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99
<u>Migo</u>	SHA256	8cce669c8f9c5304b43d6e91e6332b1cf1113c81f355877dabd25198c3c3f208, c5dc12dbb9bb51ea8acf93d6349d5bc7fe5ee11b68d6371c1bbb098e21d0f685, 2b03943244871ca75e44513e4d20470b8f3e0f209d185395de82b447022437ec, 364a7f8e3701a340400d77795512c18f680ee67e178880e1bb1fcda36ddbc12c
<u>Abyss Locker</u>	SHA256	72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462, 3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69522a0a3c34c96b6d, 9243bdcb30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc, 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64, dee2af08e1f5bb89e7bad79fae5c39c71ff089083d65da1c03c7a4c051fabae0, e6537d30d66727c5a306dc291f02ceb9d2b48bffe89dd5eff7aa2d22e28b6d7c, 1d04d9a8eeed0e1371afed06dcc7300c7b8ca341fe2d4d777191a26dabac3596,

Attack Name	TYPE	VALUE
<u>Abyss Locker</u>	SHA256	1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eachefe4120, 25ce2fec4cd164a93dee5d00ab547ebe47a4b713cced567ab9aca4a7080afcb7, b524773160f3cb3bfb96e7704ef31a986a179395d40a578edce8257862cafe5f, 362a16c5e86f13700bdf2d58f6c0ab26e289b6a5c10ad2769f3412ec0b2da711, e5417c7a24aa6f952170e9dfcfd044c2a7259a03a7683c3ddb72512ad0cd5c7, 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da, 877c8a1c391e21727b2cdb2f87c7b0b37fb7be1d8dd2d941f5c20b30eb65ee97, 2e42b9ded573e97c095e45dad0bdd2a2d6a0a99e4f7242695054217e2bba6829
<u>Xeno RAT</u>	MD5	13b1d354ac2649b309b0d9229def8091, 6f9e84087cabbb9aaa7d8aba43a84dcf, 7704241dd8770b11b50b1448647197a5, 0aa5930aa736636fd95907328d47ea45
	SHA256	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c, 4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0, 1762536a663879d5fb8a94c1d145331e1d001fb27f787d79691f9f8208fc68f2, 96b091ce5d06afd11ee5ad911566645dbe32bfe1da2269a3d3ef8d3fa0014689
<u>Blackcat Ransomw are</u>	MD5	944153fb9692634d6c70899b83676575, efc80697aa58ab03a10d02a8b00ee740, c90abb4bbbfe7289de6ab1f374d0bcbe, 341d43d4d5c2e526cadd88ae8da70c1c, 34aac5719824e5f13b80d6fe23cbfa07, eea9ab1f36394769d65909f6ae81834b, 379bf8c60b091974f856f08475a03b04, ebca4398e949286cb7f7f6c68c28e838, c04c386b945ccc04627d1a885b500edf, 824d0e31fd08220a25c06baee1044818
	SHA256	1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5, 3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71, af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021, bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1, 5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905, bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e, 732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0
	SHA1	3dd0f674526f30729bcd4271e6b7eb0bb890c52, d6d442e8b3b0aef856ac86391e4a57bcb93c19ad, 6b52543e4097f7c39cc913d55c0044fcf673f6fc, 004ba0454feb2c4033ff0bdb2ff67388af0c41b6, 430bd437162d4c60227288fa6a82cde8a5f87100, 1376ac8b5a126bb163423948bd1c7f861b4bfe32, 380f941f8047904607210add4c6da2da8f8cd398
	IP	5.199.168[.]24, 91.92.254[.]193
	Domain	resources.docusong[.]com, Fisa99.screenconnect[.]com

Attack Name	TYPE	VALUE
<u>Bl00dy Ransomwar</u> <u>e</u>	SHA256	3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623, 8e51de4774d27ad31a83d5df060ba008148665ab9caf6bc889a5e3fba4d7e600
	URLs	hxxp://23[.]26[.]137[.]225:8091/chromeset.exe, hxxp://23[.]26[.]137[.]225:8084/msappdata.msi
<u>XWORM</u>	Domains	input-beats[.]gl[.]at[.]ply[.]gg scamkiller.duckdns[.]org
	SHA256	444338339260d884070de53554543785acc3c9772e92c5af1dff96e60e67c195, 47d83461ee57031fd2814382fb526937a4cfa9a3eea7a47e4e7ee185c0602b27, f1c7045badec0b9771da4a0f067eac99587d235d1ede35190080cd051d923da
<u>WINELOADER</u>	SHA256	72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, b014cdf3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083
	URLs	hxxps://castechtools[.]com/api.php, hxxps://seeceafcleaners[.]co[.]uk/cert.php, hxxps://seeceafcleaners[.]co[.]uk/wine.php, hxxps://passatempobasico[.]com[.]br/wine.php

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 1, 2024 • 7:10 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com