Date of Publication
June 2, 2023

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

MAY 2023

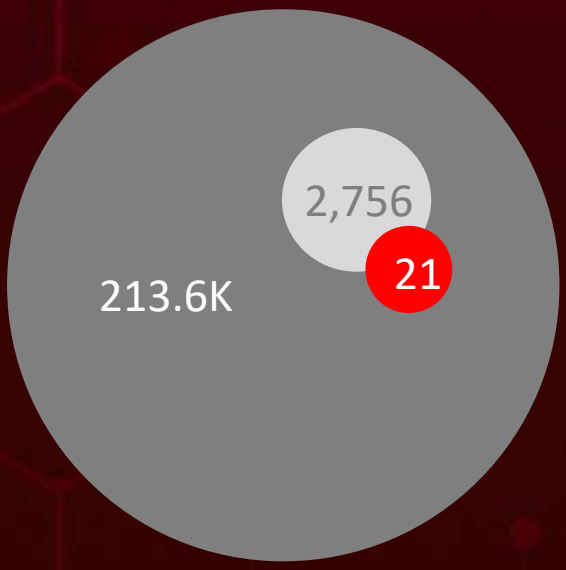
Table Of Contents

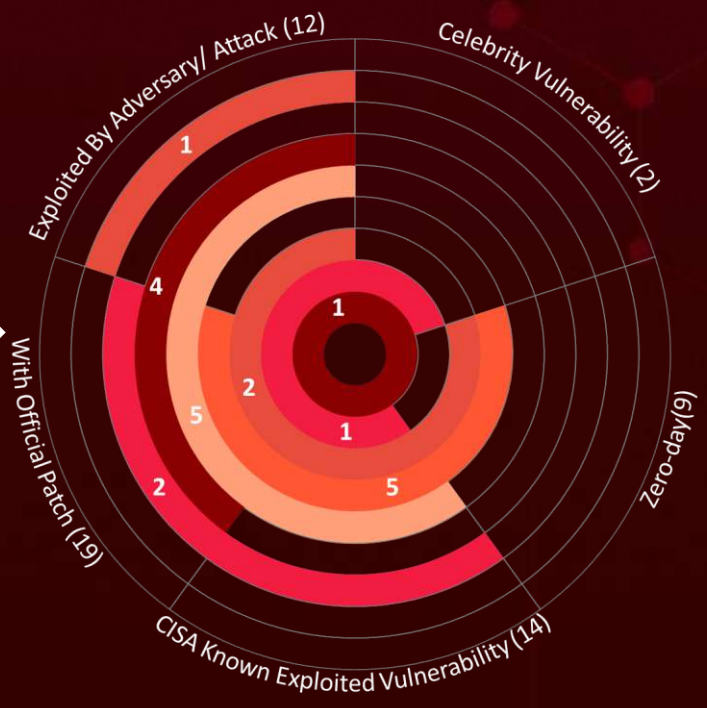
Summary

In **May**, the cybersecurity community witnessed significant attention drawn to the discovery of **nine zero-day** vulnerabilities. Among them was the **Celebrity Vulnerability**, exploited by **GoldenJackal APT** and **MEME#4CHAN phishing campaign** deploy **Xworm**, which heightened the sense of urgency among security teams to patch their systems.

The month of May saw a rise in **ransomware** attacks, with various strains such as **CACTUS**, **Rancoz**, **CryptNet**, **MichaelKors**, **Buhti**, **BianLian**, and **Bl00dy** actively targeting victims. As ransomware continues to evolve and grow in sophistication, organizations must take steps to protect themselves by implementing comprehensive backup and disaster recovery strategies and training employees on how to recognize and avoid phishing attacks.

Finally, the **unpatched** vulnerabilities, **CVE-2023-29552**, which can lead to a Denial-of-Service Attack and result in potential losses of up to **$120,000**, and **CVE-2018-5713**, exploited by **Earth Longzhi APT**, have been actively utilized in attacks





Total Vulnerabilities Published

Vulnerabilities Published in the Month

Exploited Vulnerabilities

Insights

1877 Team
Primarily targeting the Middle East, organizations in Africa, and Asia.

$200,000 to $1,000,000
Akira Ransomware Strikes, Demanding High Stakes!

8220 Gang
Exploits Oracle WebLogic Server vulnerability to deploy cryptominers

9 Zero-Days Exposed
and exploited by Adversaries in this month

Top 5 Prime Targeted Verticals of the Month: **Government**, **Manufacturing**, **Education**, **Finance**, and **Healthcare**

29 staggering new malware strains wreaked havoc as they were deployed in a multitude of attacks.

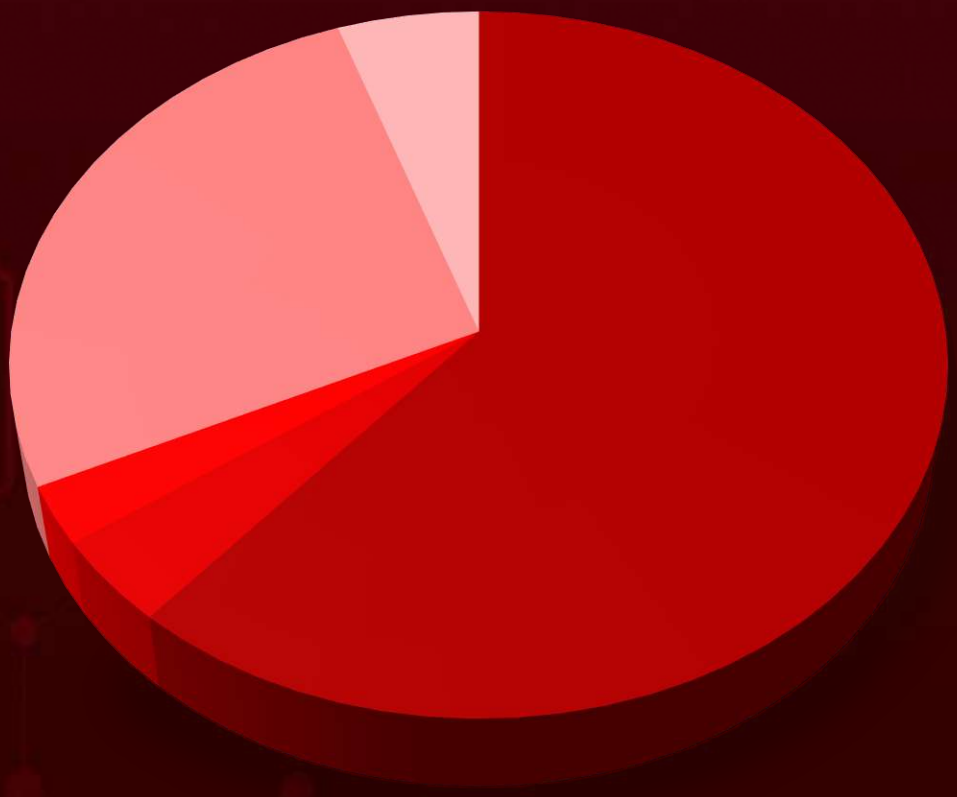
Mirai Botnet
Exploited TP-Link router vulnerability allows attackers to execute commands and infect devices

APT28
Targeting the Ukrainian civic community with the help of the Russian GRU

The **Philippines**, **Turkey**, **India**, **UAE**, and **Afghanistan** were the most targeted countries

SideWinder exploited **CVE-2017-0199** to invade antivirus (AV) detection

Threat Landscape



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

Celebrity Vulnerabilities

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Windows Server: 2008 - 2022 & Windows: 7 - 11 21H2	GoldenJackal APT
	ZERO-DAY	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	✓	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	Xworm, JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	**CWE ID**	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059:Command and Scripting Interpreter, T1133:External Remote Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	✓	Windows Server: 2008 R2 - 2019 2004	BianLian
	ZERO-DAY	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	✗	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*	BianLian ransomware
NetLogon Privilege Escalation Vulnerability (ZEROLOGON)	**CWE ID**	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-330	T1068:Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-24055	KeePass Injection Vulnerability	KeePass 2.5x of before	✗	✗	✓
CVE-2023-29552	SLP Reflective Denial-of-Service (DoS) Amplification Vulnerability	Service Location Protocol	✗	✗	✗
CVE-2023-27532	Veeam Missing Authentication for Critical Function	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition	✗	✗	✓
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability	TP-Link Archer AX21	✗	✓	✓
CVE-2018-5713	Improper Input Validation in Malwarefox Anti-malware	Malwarefox Anti-malware 2.72.169	✗	✗	✗
CVE-2023-25717	Ruckus Remote Code Execution Vulnerability	All Ruckus Wireless Admin panels version 10.4 and older	✗	✓	✓
CVE-2023-29336	Win32k Elevation of Privilege Vulnerability	Windows & Windows Server	✓	✓	✓
CVE-2023-24932	Secure Boot Security Feature Bypass Vulnerability	Windows & Windows Server	✓	✗	✓
CVE-2017-0199	Microsoft Office/ WordPad Remote Code Execution Vulnerability with Windows API	Microsoft Windows, Windows Server, Office	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2017-3506	Denial of service Vulnerability in Oracle WebLogic Server	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	✗	✗	✓
CVE-2023-32409	Apple Sandbox Escape Vulnerability	macOS Ventura	✓	✓	✓
CVE-2023-28204	Apple Out-of-bounds read Vulnerability	macOS Ventura	✓	✓	✓
CVE-2023-32373	Apple use-after-free Vulnerability	macOS Ventura	✓	✓	✓
CVE-2023-23397	Microsoft Office Outlook Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2021-22205	GitLab Remote Code Execution Vulnerability	Community and Enterprise Editions From 11.9	✗	✓	✓
CVE-2023-2868	Barracuda ESG Remote Command Injection Vulnerability	Barracuda Email Security Gateway	✓	✓	✓
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF and NG	✗	✓	✓
CVE-2022-47986	IBM Aspera Faspex Code Execution Vulnerability	IBM Aspera Faspex	✗	✓	✓
CVE-2023-27351	PaperCut MF/NG Improper Authentication Vulnerability	PaperCut MF and NG	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
ViperSoftX	Info stealer	CVE-2023-24055	KeePass 2.5x of before	✓	Unknown
POWERTRASH Loader	Loader	CVE-2023-27532	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition	✓	Through reflective PE injection
DICELOADER (also known as Lizar)	Loader	CVE-2023-27532 CVE-2023-27350 CVE-2023-27351	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition & PaperCut MF and NG	✓	Through reflective PE injection & Exploiting unpatched PaperCut servers
Mirai Botnet	Botnet	CVE-2023-1389	TP-Link Archer AX21	✓	Exploiting vulnerabilities in IoT devices
LOBSHOT	Infostealer	-	Windows	-	Via Google Ads
Croxloader	Banking Trojan	CVE-2018-5713	Malwarefox Anti-malware 2.72.169	✗	Social engineering tactics

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Atomic Stealer	InfoStealer	-	MacOS	-	Legitimate AnyDesk remote desktop Software
BlackBit	Ransomware	-	-	-	Via Phishing emails, malicious ads
SILENTTRINITY	Rootkit	-	Windows, Mac, and Linux	-	Phishing emails
Akira ransomware	Ransomware	-	Windows	-	Unknown
ReconShark	Reconnaissance Tool	-	Microsoft OneDrive	-	spear-phishing emails & OneDrive Links
AndoryuBot	Botnet	CVE-2023-25717	All Ruckus Wireless Admin panels version 10.4 and older	✓	Ruckus vulnerability
Snake (aka Uroburos, Urouros)	Cyber Espionage Tool	-	Windows, MacOS, and Linux	-	Unknown
DarkWatchMan RAT	RAT	-	-	-	Phishing
DownEx	Fileless	-	Windows	-	Spear-phishing emails
CACTUS Ransomware	Ransomware	-	-	-	Exploiting known vulnerabilities in VPN appliances
BPFDoor	Backdoor	-	Linux	-	Unknown

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Greatness	Phishing-as-a-service	-	Microsoft 365	-	Phishing pages
Babuk Ransomware	Ransomware	-	-	-	Unknown
CopperStealth	Rootkit	-	-	-	via pay-per-install (PPI) networks
CopperPhish	Phishing kit	-	-	-	Via a Private Loader
Rancoz ransomware	Ransomware	-	-	-	Unknown
Tsunami	Backdoor	CVE-2017-3506	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	✓	Exploiting known vulnerabilities
XMRIG cryptominer	cryptominer				
Xworm	Worm	CVE-2022-30190	Microsoft Windows	✓	Phishing email
Minas	Miner	-	-	-	Unknown
CryptNet	Ransomware	-	-	-	Unknown
MichaelKors	Ransomware	-	Windows, Linux and VMware ESXi	-	Unknown
BlackCat	Ransomware	-	Windows, Linux, and VMware ESXi	-	Phishing Emails
Donut	Loader	-	-	-	Unknown
JackalControl	Trojan	CVE-2022-30190	Microsoft Windows	✓	Unknown
JackalSteal	InfoStealer				Unknown
JackalPerInfo	InfoStealer				Unknown
JackalScreenWatcher	Spyware				USB drives
JackalWorm	Worm				USB drives
Pikabot	Backdoor	-	-	-	Unknown

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PowerExchange	Backdoor	-	Windows	-	Phishing emails
Buhti Ransomware	Ransomware	CVE-2023-27350 CVE-2022-47986	PaperCut MF &NG and IBM Aspera Faspex	✓	Exploiting known vulnerabilities
GobRAT	RAT	-	Linux	-	Exploiting known vulnerabilities In WEBUI accessible routers
BianLian ransomware	Ransomware	CVE-2020-1472	Microsoft Netlogon Remote Protocol (MS-NRPC)	✓	valid RDP credentials
Bl00dy Ransomware	Ransomware	CVE-2023-27350 CVE-2023-27351	PaperCut MF and NG	✓	Exploiting unpatched PaperCut servers
Clop Ransomware					
LockBit Ransomware					
TrueBot	Botnet				
Cobalt Strike Beacons	Rootkit				
Merdoor backdoor	Backdoor	-	-	-	Unknown
ZXShell rootkit	Rootkit				

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
FIN7 (aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)	Financial crime	Russia	CVE-2023-27532	POWERTRASH Loader & DICELOADER (also known as Lizar)	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition
TA505 (Graceful Spider, Gold Evergreen, Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo, Spandex Tempest)	Financial crime, Financial gain	Russia	-	LOBSHOT	Windows
1877 Team	Hacktivist	Kurdistan	-	-	-
Earth Longzhi (Subgroup of APT41)	Information theft and Espionage, financial crime	China	CVE-2018-5713	Croxloader and SPHijacker	Malwarefox Anti-malware 2.72.169
SideCopy	Information theft and espionage	Pakistan	-	SILENTTRINITY	Windows, Mac, and Linux
Dragon Breath APT (aka Golden Eye Dog & APT-Q-27)	Financial gain	Unknown	-	-	Telegram, LetsVPN, and WhatsApp for Windows

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)	Information theft and espionage	North Korea	-	ReconShark	Microsoft OneDrive
Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)	Information theft and espionage	Russia	-	Snake (aka Uroburos, Urouros)	Windows, MacOS, and Linux
SideWinder (aka Rattlesnake, T-APT-04, APT-C-17, Razor Tiger, Baby Elephant, Operation Origami)	Information theft and espionage	India	CVE-2017-0199	-	Microsoft Windows, Windows Server, Office
Red Menshen (AKA Red Dev 18)	Information theft and espionage	China	-	BPFDoor	Linux
Lancefly	Information theft and espionage	China	-	Merdoor backdoor, ZXShell rootkit	-
RA Group	Information theft and espionage; Financial gain	Unknown	-	Babuk Ransomware	-
Water Orthrus	Information theft and espionage	Unknown	-	CopperStealth and CopperPhish	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
8220 Gang (8220 Mining Group)	Financial gain	China	CVE-2017-3506	Tsunami malware and XMRIG cryptominer	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2
Camaro Dragon	Information theft and Espionage; Sabotage	China	-	-	-
APT28 (aka FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)	Information theft and espionage	Russia	CVE-2023-23397	-	Microsoft Windows
GoldenJackal APT	Information theft and espionage	Unknown	CVE-2022-30190	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher	Microsoft Windows
GUI-vil (aka p0-LUCR-1)	Information theft and espionage	Indonesia	CVE-2021-22205	-	GitLab Community and Enterprise Editions From 11.9

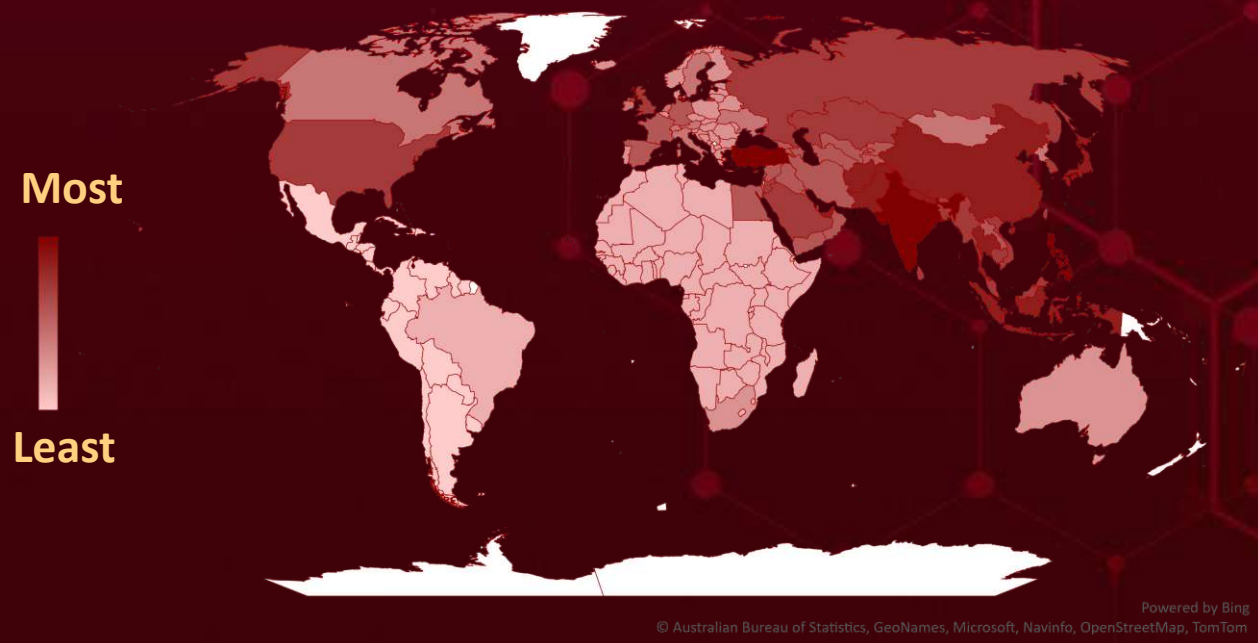
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Blacktail	Financial gain	Unknown	CVE-2023-27350 CVE-2022-47986	Buhti Ransomware	PaperCut MF and NG & IBM Aspera Faspex
BianLian	Financial gain	Unknown	CVE-2020-1472	BianLian ransomware	Microsoft Netlogon Remote Protocol (MS-NRPC)

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Password manager software	KeePass 2.5x of before
	Backup & Replication Application	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition - 11.0.1.1261 & 12.0.0.1420
	TP-Link router	TP-Link Archer AX21
	Anti-malware Application	Malwarefox Anti-malware 2.72.169
	Operating System and Application	Fortiadc version: 7.2.0 Fortiproxy version: 1.0.0-2.0.0
	Ruckus Wireless router	All Ruckus Wireless Admin panels version 10.4 and older
	Operating System	Windows: 11 - 11 22H2, 10- 10 S Windows Server: 2012 - 2022 20H2 Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016 Windows Server: 2008 - 2022 Windows: 7 - 11 21H2 Microsoft Outlook: 2013 - 2021 Microsoft Office: 365 – 2021 Windows Server: 2008 R2 - 2019 2004
	Application	WordPress Plugins Advanced Custom Fields: 5.9.5 - 6.1.4 & Advanced Custom Fields Pro: before 6.1.5

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
ORACLE	Application	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2
PaperCut	Print management software application	PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9
	Operating System	macOS Ventura before 13.4
GitLab	Application	GitLab Community and Enterprise Editions From 11.9
Barracuda	Email Security Gateway appliance	Barracuda Email Security Gateway (ESG): 5.1.3 - 9.2
IBM	Application	IBM Aspera Faspex for Windows: 4.4.1 - 4.4.2 PL1 IBM Aspera Faspex for Linux: 4.4.1 - 4.4.2 PL1

Targeted Countries



Color	Countries
	Philippines
	Turkey
	India
	United Arab Emirates
	Afghanistan
	Cyprus
	Nepal
	China
	Pakistan
	Indonesia
	Singapore
	Japan
	Thailand
	Sri Lanka
	Russia
	Jordan
	Taiwan
	Kazakhstan
	East Timor
	Bangladesh
	Brunei
	Qatar
	Malaysia

Color	Countries
	Saudi Arabia
	Maldives
	South Korea
	Myanmar
	Bhutan
	Cambodia
	United States
	Vietnam
	United Kingdom
	Israel
	Syria
	Spain
	Armenia
	Tajikistan
	Palestine
	Oman
	Egypt
	Bahrain
	France
	Iran
	Georgia
	Iraq
	Germany

Color	Countries
	Turkmenistan
	Hong Kong
	Azerbaijan
	Kuwait
	Uzbekistan
	Kyrgyzstan
	Yemen
	Laos
	Lebanon
	Sweden
	Netherlands
	Ukraine
	Ireland
	North Korea
	Italy
	Switzerland
	Macau
	Austria
	Mongolia
	Canada
	Greece
	Slovakia
	Portugal
	Hungary
	Australia

Color	Countries
	Iceland
	Norway
	Belarus
	San Marino
	Belgium
	South Africa
	Bosnia and Herzegovina
	Czechia
	Bulgaria
	Vatican City
	Latvia
	Poland
	Liechtenstein
	Romania
	Lithuania
	Serbia
	Luxembourg
	Slovenia
	Finland
	Croatia
	Malta
	Andorra
	Moldova
	Denmark

Color	Countries
	Monaco
	Albania
	Montenegro
	Estonia
	North Macedonia
	Madagascar
	Tunisia
	Kenya
	Morocco
	Zambia
	Mozambique
	South Sudan
	Cameroon
	Mauritius
	Namibia
	Eswatini
	Zimbabwe
	Sierra Leone
	Gambia
	Malawi
	Burkina Faso
	Nigeria
	Mauritania

Targeted Industries

Most

Government

Manufacturing

Education

Financial

Healthcare

Real Estate

Consumers

Defence

Technology

Media

Engineering

NGOs

Tele-communications

Food products

Construction

Transportation

Hotels

Gaming

Tele-communications

Research Organizations

Automotive

Aviation

Energy

Insurance

Retail

Think-Tanks

Legal

Embassies

Chemical

Oil & Gas

Pharmaceutical

Professional Services

Utilities

Least

TOP 25 MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1083
File and Directory Discovery

T1566
Phishing

T1204
User Execution

T1140
Deobfuscate/ Decode Files or Information

T1036
Masquerading

T1574
Hijack Execution Flow

T1021
Remote Services

T1082
System Information Discovery

T1562
Impair Defenses

T1057
Process Discovery

T1055
Process Injection

T1059.001
PowerShell

T1204.002
Malicious File

T1071
Application Layer Protocol

T1056
Input Capture

T1486
Data Encrypted for Impact

T1090
Proxy

T1047
Windows Management Instrumentati on

T1070
Indicator Removal

T1190
Exploit Public-Facing Application

T1053
Scheduled Task/Job

T1588
Obtain Capabilities

T1041
Exfiltration Over C2 Channel

Top Indicators of Compromise (IOCs)

Attack	TYPE	VALUE
JackalControl	MD5	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c 8c1070f188ae87fba1148a3d791f2523
	URLs	hxxp://abert-online[.]de/meeting/plugins[.]php hxxp://acehigh[.]host/robotx[.]php hxxp://assistance[.]uz/admin/plugins[.]php hxxp://cnom[.]sante[.]gov[.]ml/components/com_avreloaded/views/popup/tmpl/header[.]php hxxp://info[.]merysof[.]am/plugins/search/content/plugins[.]php
JackalSteal	URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php
	MD5	c05999b9390a3d8f4086f6074a592bc2
JackalPerInfo	MD5	a491aefb659d2952002ef20ae98d7465
JackalScreenWatcher	MD5	1072bfeee89e369a9355819ffa39ad20
JackalWorm	MD5	5de309466b2163958c2e12c7b02d8384
BianLian ransomware	SHA256	076e59781d0759de35022291c3d63bbf4227bd79561d80f52c9073a6278c5077 0772fb1102685def711ffe647080e1a9b6597fe60e8f1afe7b457ac97c6ac25e 16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf 183b28fb93db1c907b32aa9fa2f83c7b0ebcc6724de85707a89e5d03c5be5d12 1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9
	IPV4	5.230.73[.]234 5.230.73[.]37 51.222.96[.]1 52.87.206[.]242

Attack	TYPE	VALUE
Croxloader	IPV4	194.31.53[.]128 198.13.47[.]158 172.67.139[.]61 207.148.115[.]125 64.227.164[.]34 194.31.53[.]128 198.13.47[.]158
	Domains	evnpowerspeedtest[.]com www.updateforhours[.]com dns.eudnslog[.]com asis.downloadwindowsupdate[.]co
	SHA256	7910478d53ab5721208647709ef81f503ce123375914cd504b9524577057f0ec ebf461be88903ffc19363434944ad31e36ef900b644efa31cde84ff99f3d6aed 21ffa168a60f0edcbc5190d46a096f0d9708512848b88a50449b7a8eb19a91ed 942b93529c45f27cdbd9bbcc884a362438624b8ca6b721d51036ddaebc750d8e 75a51d1f1dd26501e02907117f0f4dd91469c7dd30d73a715f52785ea3ae93c8 4399c5d9745fa2f83bd1223237bdabbfc84c9c77bacc500beb25f8ba9Df30379 8327cd200cf963ada4d2cde942a82bbed158c008e689857853262fcda91d14a4 9eceba551baafe79b45d412c5347a3d2a07de00cc23923b7dee1616dee087905 630bb985d2df8e539e35f2da696096e431b3274428f80bb6601bbf4b1d45f71e ef8e658cd71c3af7c77ab21d2347c7d41764a68141551938b885da41971dd733 e654ecc10ce3df9f33d1e7c86c704cfdc9cf6c6f49aa11af2826cbc4b659e97c 16887b36f87a08a12fe3b72d0bf6594c3ad5e6914d26bff5e32c9b44acfec040 39de0389d3186234e544b449e20e48bd9043995ebf54f8c6b33ef3a4791b6537
Buhti Ransomware	IPV4	91.215.85[.]183 81.161.229[.]120
	SHA256	9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf 9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd

Attack	TYPE	VALUE
Buhti Ransomware	SHA256	063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6 d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986babba5e9a51ed4a65 8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441 898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a 515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855 4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880 22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe 18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef 01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4 7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c 287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52 32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c 5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72 d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72 65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b 8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334 8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2 97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24055	✗	KeePass 2.5x of before	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:keepass:keepass:*:*:*:*:*:*:*:*	ViperSoftX
KeePass Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-312	T1055: Process Injection	https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29552	✗	Service Location Protocol	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:service_location_protocol:service_location_protocol:*:*:*:*:*:*:*:*	-
SLP Reflective Denial-of-Service (DoS) Amplification Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-345	T1498:Network Denial of Service T1498.002: Reflection Amplification	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27532	✗	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition	FIN7
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:backup_\&_replication:11.0.1.1261:*:*:*:*:*:*:*	POWERTRASH Loader & DICELOADER
Veeam Missing Authentication for Critical Function	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1555: Credentials from Password Stores	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-1389	✗	TP-Link Archer AX21	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tplink:archer_ax21_firmware:*:*:*:*:*:*:*:*;	Mirai Botnet
TP-Link Archer AX-21 Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1055: Process Injection	https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-5713	✗	Malwarefox Anti-malware 2.72.169	Earth Longzhi
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:malwarefox:antimalware:2.72.169:*:*:*:*:*:*:*	Croxloader
Improper Input Validation in Malwarefox Anti-malware	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1499: Endpoint Denial of Service	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-25717	✗	All Ruckus Wireless Admin panels version 10.4 and older	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ruckuswireless:ruckus_wireless_admin:*:*:*:*:*:*:*:*	AndoryuBot
Ruckus Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059:Command and Scripting Interpreter	https://support.ruckuswireless.com/security_bulletins/315

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29336	✗	Windows: 10 - 10 S; Windows Server: 2008 - 2016	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Win32k Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068:Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24932	✗	Windows: 10 - 10 S, 11 – 11 22H2; Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Secure Boot 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/en-US/vulnerability/CVE-2023-24932

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0199	✗	Microsoft Office: 2007 - 2016	SideWinder
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_office:2016:*:*:*:*:*:*:*	-
Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0199

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-3506	✗	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	8220 Gang
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:oracle_weblogic_server:*:*:*:*:*:*:*:*	-
Denial of service Vulnerability in Oracle WebLogic Server	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1498: Network Denial of Service	https://www.oracle.com/security-alerts/cpuapr2017.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32409	✗	macOS Ventura before 13.4	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*	-
Apple Sandbox Escape Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1497: Virtualization/Sandbox Evasion	https://support.apple.com/en-us/HT213758

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28204	✗	macOS Ventura before 13.4	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*	-
Apple Out-of-bounds Read Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1005: Data from Local System	https://support.apple.com/en-us/HT213758

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32373	✗	macOS Ventura before 13.4	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*	-
Apple use-after-free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1574: Hijack Execution Flow	https://support.apple.com/en-us/HT213758

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23397	✗	Microsoft Windows	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps::*:*:*:enterprise:*:*:*	-
Microsoft Office Outlook Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-294	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22205	✗	Community and Enterprise Editions From 11.9	GUI-vil
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*	-
GitLab Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1203: Exploitation for Client Execution	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2868	✗	Barracuda Networks Email Security Gateway (ESG): 5.1.3 - 9.2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:barracuda_networks:esg:9.2:*:*:*:*:*:*:*	-
Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://status.barracuda.com/incidents/34kx82j5n4q9

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350	✗	PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*	Bl00dy Ransomware, Clop Ransomware, LockBitRansomware, DiceLoader, TrueBot, and Cobalt Strike Beacons
PaperCut MF/NG Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47986	✗	IBM Aspera Faspex for Windows: 4.4.1 - 4.4.2 PL1 & IBM Aspera Faspex for Linux: 4.4.1 - 4.4.2 PL1	Blacktail
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ibm:aspera_faspex:*:*:*:*:*:*:*:*	Buhti Ransomware
IBM Aspera Faspex Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://www.ibm.com/support/pages/node/6952319

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27351	✗	PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*	Bl00dy Ransomware, Clop Ransomware, LockBit Ransomware, DiceLoader, TrueBot, and Cobalt Strike Beacons
PaperCut MF/NG Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ViperSoftX	ViperSoftX info stealer malware primarily targeting cryptocurrencies, using sophisticated encryption techniques and monthly changes in command-and-control servers to evade detection.	Unknown	CVE-2023-24055
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Info stealer		Data Theft	KeePass 2.5x of before
ASSOCIATED ACTOR			**PATCH LINK**
-			https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/

IOC TYPE	VALUE
URLs	http://ahoravideo-schnellvpn[.]xyz http://chatgigi2[.]com
SHA256	d5799651ab7bb5939136addde222255f81e090c3c127d05727b71b3b2cbc9860 F1e6821caa29aade550171d640ed5605556e7d074542eea5d5370168f2c09880 f310e01a9ed40b6563b88de23d560cf839079b503260eb86a7bc32160129170b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DownEx	The DownEx malware was discovered in a cyberattack on government institutions in Kazakhstan and Afghanistan in 2022, likely with state sponsorship.	Spear-phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Fileless		Data Theft and espionage	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
Domain	net-certificate[.]services
IPV4	139.99.126[.]38 84.32.188[.]123 206.166.251[.]216
MD5	1e46ef362b39663ce8d1e14c49899f0e bb7cf346c7db1c518b1a63c83e30c602

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
POWERTRASH Loader	POWERTRASH Loader is a type of malware that uses an obfuscated PowerShell script to load and execute a malicious payload, leaving little forensic evidence. It is highly dangerous and difficult to detect or remove.	Through reflective PE injection	CVE-2023-27532
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data theft, installing malware, remote access to infected system	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition
ASSOCIATED ACTOR			**PATCH LINK**
FIN7 (aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)			https://www.veeam.com/kb4424

IOC TYPE	VALUE
IPV4	217[.]12.206.176 162[.]248.225.115
SHA1	8687b6b1508a93556d6e30d14e5c4ee9971f2d0 e5480a47172e3f75dbf0384f4ca82c7b47910e0f

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
DICELOADER (also known as Lizar)	The infiltrators used DICELOADER as a foothold to gain access to the compromised machines and carry out post-exploitation procedures. It is highly dangerous and difficult to detect or remove.	Through reflective PE injection & Exploiting unpatched PaperCut servers	CVE-2023-27532 CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data theft, installing malware, remote access to infected system	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition & PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
FIN7 (aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)			https://www.veeam.com/kb4424

IOC TYPE	VALUE
IPV4	217[.]12.206.176 162[.]248.225.115 45[.]136.199.128 91[.]149.243.181 91[.]199.147.152 95[.]217.49.123 77[.]75.230.112 194[.]87.148.41 195[.]123.244.162
SHA1	b621f8c5e9033718b4e9d47a2f0eccb9783f612a

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
Mirai	The Mirai botnet is a type of malware that infects Internet of Things (IoT) devices and turns them into a network of bots that can be used for DDoS attacks. It was responsible for several high-profile attacks in 2016 and continues to be a threat today.	Exploiting vulnerabilities in IoT devices	CVE-2023-1389
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Disruptive	TP-Link Archer AX21
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware
IOC TYPE	**VALUE**		
SHA256	888f4a852642ce70197f77e213456ea2b3cfca4a592b94647827ca45adf2a5b8 b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LOBSHOT	LOBSHOT is a new malware that is being distributed through Google Ads. It is a remote access trojan that can allow threat actors to take control of an infected Windows devices.	Via Google Ads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Hidden desktops, execute commands, steal data, and deploy further malware payloads.	Windows
ASSOCIATED ACTOR			**PATCH LINK**
TA505			-
IOC TYPE	**VALUE**		
IPV4	95.217.125[.]200		
SHA256	e4ea88887753a936eaf3361dcc00380b88b0c210dcbde24f8f7ce27991856bf6		

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
Croxloader	Croxloader is a variant of the Ursnif banking Trojan used to steal sensitive data from infected systems. It was launched using a legitimate Windows Defender binary as part of a larger attack that disabled security products using the "SPHijacker" tool.	Social engineering tactics	CVE-2018-5713
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Data Theft	Malwarefox Anti-malware 2.72.169
ASSOCIATED ACTOR			**PATCH LINK**
APT41			✕

IOC TYPE	VALUE
IPV4	194.31.53[.]128 198.13.47[.]158
SHA256	7910478d53ab5721208647709ef81f503ce123375914cd504b9524577057f0ec ebf461be88903ffc19363434944ad31e36ef900b644efa31cde84ff99f3d6aed 21ffa168a60f0edcbc5190d46a096f0d9708512848b88a50449b7a8eb19a91ed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atomic Stealer	Atomic Stealer malware is a full-featured infostealer designed to steal sensitive data from macOS users. The malware can grab account passwords, browser data, session cookies, and crypto-wallets.	Legitimate AnyDesk remote desktop software	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data theft	MacOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
MD5	5e0226adbe5d85852a6d0b1ce90b2308
SHA256	15f39e53a2b4fa01f2c39ad29c7fe4c2fef6f24eff6fa46b8e77add58e7ac709
URLs	hxxp[:]//amos-malware[.]ru/sendlog
IPV4	37[.]220.87[.]16
Domains	amos-malware[.]ru

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
BlackBit	The BlackBit ransomware, a variant of LokiLocker with cosmetic changes, checks keyboard layout, establishes persistence, removes backups, disables defenses, and presents payment information through various methods, making it a sophisticated Strain.	Via Phishing emails, malicious ads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f18db2f b8ffd72534056ea89bfd48cbe6efb0b4d627a6284a7b763fdb7dfd070c1049ba		
SHA1	b04ccaa781be7521d50faa36db269f71ac56af58 2f052cc3e64870b8ac28efb2d79bc2b16dff3e8e e9b35995bf772cd11be13bc5c9ac93c846f00405		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SILENTTRINITY	SILENTTRINITY is a newer and more comprehensive tool, functioning as a post-exploitation framework with the same capabilities as those of Empire or CobaltStrike.	Via Phishing emails, malicious ads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
SideCopy			-
IOC TYPE	**VALUE**		
SHA256	9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce bf34077c8b22759b28dcc458dc1b7bba3810c1c30b050b26a26e8d9f64e7791 c7753ffb7f66b0dfb05a24955324182cb92bbf41dd8fccb308c3f04d497a16da		

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
Akira ransomware	Akira ransomware is a new threat targeting corporate networks and has already attacked several companies in various industries, stealing their data and demanding ransom amounts ranging from $200,000 to $1,000,000.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488,3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c,67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ReconShark	Kimsuky, a North Korean APT group, is using a new malware tool called ReconShark to conduct global cyberattacks.	spear-phishing emails & OneDrive Links	-
TYPE		IMPACT	AFFECTED PRODUCTS
Reconnaissance Tool		Data Theft andCompromise of Sensitive Information	Microsoft OneDrive
ASSOCIATED ACTOR			PATCH LINK
Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)			-
IOC TYPE	VALUE		
SHA1	86a025e282495584eabece67e4e2a43dca28e505c8f54cb73c240a1904030eb36bb2baa7db6aeb01		
Domain	yonsei[.]lol		

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
AndoryuBot	AndoryuBot targets critical Ruckus Wireless Admin panel vulnerability to infect Wi-Fi access points for use in DDoS attacks, malware supports 12 DDoS attack modes and is marketed through YouTube videos.	Ruckus vulnerability	CVE-2023-25717
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnets		Data Theft, Denial of Service and Potential Financial Losses	All Ruckus Wireless Admin panels version 10.4 and older
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.ruckuswireless.com/security_bulletins/315
IOC TYPE	**VALUE**		
IPV4	163[.]123[.]142[.]146 45[.]153[.]243[.]39		
SHA256	ea064dd91d8d9e6036e99f5348e078c43f99fdf98500614bffb736c4b0fff408,f42c6cea4c47bf0cbef666a8052633ab85ab6ac5b99b7e31faa1e198c4dd1ee1,3441e88c80e82b933bb09e660d229d74f7b753a188700fe018e74c2db7b2aaa0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkWatchMan RAT	DarkWatchMan RAT allows attackers to gain remote control over compromised systems and extract sensitive data such as keystrokes, clipboard data, and system information.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and remote access to infected system.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	2edf05f2130d4e12599dc44ff8bfc8921706c64156d873ebbd0c6ecac95fec399afc15393e8bae03ad306ae1c50645e3ca820517f8fd74d21944d846df6b7c20		

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
Snake (aka Uroburos, Urouros)	Snake is a powerful cyber-espionage malware developed by FSB & linked to Turla hackers. Boasts high stealth, rigorous engineering & global reach.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Cyber Espionage Tool		Data Theft	Windows, MacOS, and Linux
ASSOCIATED ACTOR			**PATCH LINK**
Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)			-
IOC TYPE	**VALUE**		
SHA256	6a4836cd5847c3d42b846d1616cc94429ec27446555b66f9abf061e7747bdca0,3c3511a9b6d98f49943cbec9355ebb8a006706f42304f608b6d9eb6f2da79718,735808b3dfad2472c5785399b6e34bf5cccef1153ad15bd1167420ff05b1a9d8,ff51c7ab066f425f73ba2005dbf3d2be4bc5344b152f18818c0ea5da81368ef0,1c05f794c40193734a68e145ca1aaf7268b37f6fe3ea2bea5f12aa2ceB24ee60		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BPFDoor	A new variant of the BPFDoor is featuring more robust encryption and reverse shell communication. It uses the BPF to bypass firewall restrictions, allowing threat actors to maintain persistence and remain undetected.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Red Menshen (AKA Red Dev 18)			-
IOC TYPE	**VALUE**		
SHA256	afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7		
Mutex	/var/run/initd[.]lock		

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
CACTUS Ransomware	CACTUS is a new strain of ransomware that targets large commercial entities, gains initial access to networks through VPN vulnerabilities, and communicates with victims through Tox, using a variety of tools and tactics.	Exploiting known vulnerabilities in VPN appliances	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Exfiltrates sensitive data and and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IPV4	163[.]123[.]142[.]213		
MD5	d9f15227fefb98ba69d98542fbe7e568 3adc612b769a2b1d08b50b1fb5783bcf be7b13aee7b510b052d023dd936dc32f 26f3a62d205004fbc9c76330c1c71536		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Greatness	The Phishing-as-a-Service (PaaS) platform named 'Greatness' has experienced a the surge in its operations, which target organizations utilizing Microsoft 365 in the USA	Phishing pages	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Phishing-as-a-service		Compromise critical infrastructure and sensitive data	Microsoft 365
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
URLs	hxxps[:]//bluecheckcommunication[.]com/finale/host8/admin/js/mj[.]php hxxps[:]//thesslcgroup[.]org/host10/admin/js/mj[.]php		
SHA256	c5b29072d28e35c3992015fcbedc29540dd5ffc2931257a71866affae9de31f4d07a2aa49f7b41eac954cd917aeedad3309d2856f63d51410da10dd5ff5847ce		

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

NAME	OVERVIEW	DELERY METHOD	TARGETED CVEs
Babuk Ransomware	The emergence of the RA ransomware group highlights the utilization of the recently leaked Babuk ransomware source code as they employ it to develop their variant of the malware.	Phishing pages	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Compromise critical infrastructure and sensitive data	Microsoft 365
ASSOCIATED ACTOR			**PATCH LINK**
RA Group			-
IOC TYPE	**VALUE**		
URLs	hxxp[://]hkpomcx622gnqp2qhenv4ceyrhwvld3zwogr4mnkdeudq2txf55keoad[.]onion		
SHA256	3ab167a82c817cbcc4707a18fcb86610090b8a76fe184ee1e8073db152ecd45e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CopperStealth	CopperStealth deploys a rootkit to inject payloads into system processes, enabling the execution of additional tasks while blocking access to blacklisted registry keys and certain executables and drivers.	via pay-per-install (PPI) networks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Stealthy system infiltration, payload injection, and access restrictions	-
ASSOCIATED ACTOR			**PATCH LINK**
Water Orthrus			-
IOC TYPE	**VALUE**		
SHA256	293a2adf60a94437cc0f92545b7caabdaed0a63007b51e2b3d449cdb1e00f5a86c3995155e0e5cbb17e6f71b8d8b89d4dfc77849e869da7901a79053e8e8232b5558eaebeeeb4c5c731b531305e7c97c9cf1b1449b0466f46430aa0549c256e9ad5f59c497f423a07cfb4affc82aac408eafeeefef22f8ba25cabff2ff991754636772857bd9b88d5b530586c7008f48e61ec429fb50a82019d0505dcf994930		

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
CopperPhish	CopperPhish is a phishing kit that employs multiple persistence methods and utilizes downloaders such as PrivateLoader to distribute various types of malware.	Via a PrivateLoader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Phishing kit		Phishing risk, credential theft, malware distribution	-
ASSOCIATED ACTOR			**PATCH LINK**
Water Orthrus			-
IOC TYPE	**VALUE**		
SHA256	8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e39c9f743528eb317340cdd53a65630785b1168f6f0a6b253ae2518fb450f0b8128d1d1c6fb23ef5f92b16e2701c49bb34b4a81af11f95ff5674d291c5ffb3b2807cccf04854a58e43a5043e240b662f84ac512b2d2432b1b7e4cd5465d1dde33bff741d972e1dac7fa1197ac9365106b49bd07cea868d69c660aa569fe75f005		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rancoz	Rancoz ransomware is a newly discovered variant that exhibits similarities to Vice Society ransomware. It employs advanced techniques to encrypt victims' files and extract ransom payments.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	8d9f3e223f8d5e350b87dc0908fee0a5		
SHA1	9fe3060e5cbe3a9ab6c3fb3dee40bd6cd385a6f6		
SHA256	b95a4443bb8bff80d927ac551a9a5a5cfac3e3e03a5b5737c0e05c75f33ad61e		

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
Tsunami	To carry out their attacks, the gang uses various tools including Tsunami malware. This assists them in identifying and exploiting weaknesses in the targeted applications.	Exploiting known vulnerabilities	CVE-2017-3506
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data loss, unauthorized access, and infrastructure damage	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2
ASSOCIATED ACTOR			**PATCH LINK**
8220 Gang (8220 Mining Group)			http://www.oracle.com/technetwork/security-advisory/cpuapr2017-
IOC TYPE	**VALUE**		
URLs	http[:]//79[.]137[.]203[.]156/Ebvjmba.dat http[:]//185[.]17[.]0[.]19/bypass.ps1 http[:]//185[.]17[.]0[.]19/Nmfwg.png		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Xworm	XWORM is a notorious worm malware known for its advanced evasion capabilities and the availability of cracked versions in the underground criminal marketplace.	Via Follina	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Worm		Widespread infection, evasion, and facilitation of cybercrime	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190
IOC TYPE	**VALUE**		
SHA256	3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16		

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
XMRIG cryptominer	To carry out their attacks, the gang uses various tools including XMRIG cryptominer. This assists them in identifying and exploiting weaknesses in the targeted applications.	Exploiting known vulnerabilities	CVE-2017-3506
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data loss, unauthorized access, and infrastructure damage	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2
ASSOCIATED ACTOR			**PATCH LINK**
8220 Gang (8220 Mining Group)			http://www.oracle.com/technetwork/security-advisory/cpuapr2017-
IOC TYPE	**VALUE**		
URLs	http[:]//79[.]137[.]203[.]156/Ebvjmba.dat http[:]//185[.]17[.]0[.]19/bypass.ps1 http[:]//185[.]17[.]0[.]19/Nmfwg.png		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Minas	Minas is a multi-stage cryptocurrency miner with a concealed presence. It evades detection through encryption, randomization, and persistence techniques, showcasing determined network compromise.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Financial loss, compromised security, performance impact	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	08da41489b4b68565dc77bb9acb1ecb4 06fe9ab0b17f659486e3c3ace43f0e3a f38a1b6b132afa55ab48b4b7a8986181 63e0cd6475214c697c5fc115d40327b4		

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
CryptNet	CryptNet is a new ransomware-as-a-service group that employs data exfiltration and .NET code. Currently, it has two victims listed on its data leak site.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data extraction, file encryption, ransom demands, compromised backups, and financial consequences	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775 1cc7283ee218081f2f056bd2ec70514e86b8dcb921342dc9aed69e7480dec18e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MichaelKors	MichaelKors ransomware, a new RaaS operation, has been targeting Linux and VMware ESXi systems since April 2023, utilizing the tactic of "hypervisor jackpotting" to gain unrestricted access and encrypt files, posing a significant threat to organizations' virtualization infrastructure.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Financial and data losses	Windows, Linux, and VMware ESXi
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5 cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849 a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808 7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6		

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
BlackCat (aka ALPHV, AlphaV, AlphaVM, ALPHV-ng, or Noberus)	BlackCat ransomware is a sophisticated threat targeting corporate environments. It employs advanced encryption, spreading capabilities, and triple extortion tactics. It now uses a signed kernel driver for defense evasion.	Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and data losses	Windows, Linux, and VMware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497		
SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Donut	Donut is a position-independent shellcode that runs .NET Assemblies, PE files, and other Windows payloads from memory with customizable parameters.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		System compromise, data loss, and unauthorized access	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	f6c316e2385f2694d47e936boac4bc9b55e279d530dd5e805f0d963cb47c3c0d 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330 aae9c8bd9db4e0d48e35d9ab3b1a8c7933284dcbeb344809fed18349a9ec7407 27a6c3f5c50c8813ca34ab3b0791c08817c8038776657749548908848429 73ed 1485cOed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1cOOc780419a4e		

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
JackalControl	Jackal Control is a Trojan that enables remote control of a target machine through predefined commands. It uses an HTTPS communication channel to receive instructions, allowing attackers to execute programs, download files, and upload files.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		System compromise, data loss, and unauthorized access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalSteal	JackalSteal is a file exfiltration implant used to locate and extract targeted files from compromised machines, monitoring USB drives, remote shares, and logical drives, while requiring installation by another component as it lacks persistence.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		System compromise, data loss, and unauthorized access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	c05999b9390a3d8f4086f6074a592bc2		
URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php		

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
JackalPerInfo	Jackal Perinfo is a malware that gathers system information and targeted files containing stored credentials and web activities, using predefined directories and files for its operations.	Unknown	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	a491aefb659d2952002ef20ae98d7465		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JackalScreenWatcher	JackalScreenWatcher is a malware tool that captures screenshots of the victim's desktop and sends them to a remote server using encryption and compression techniques, sharing similarities with the JackalSteal component.	USB drives	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Spyware		Data loss	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
MD5	1072bfeee89e369a9355819ffa39ad20		
URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php		

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
JackalWorm	The Jackal Worm is a self-propagating malware that spreads through USB drives, hiding and replacing directories with copies of itself to infect systems with different types of malware.	USB drives	CVE-2022-30190
TYPE		IMPACT	AFFECTED PRODUCTS
Worm		Unauthorized execution of malicious code, data loss, system instability	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190
IOC TYPE	VALUE		
MD5	5de309466b2163958c2e12c7b02d8384		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Pikabot	Pikabot is an advanced backdoor that has been active since 2023, utilizing anti-analysis techniques, including the "sleep" function and language-based execution cessation, while also showing associations with the Qakbot trojan.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Unauthorized access and control over compromised systems.	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	92153e88db63016334625514802d0d1019363989d7b3f6863947ce0e490c1006 a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821 8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365 a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc 347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944		

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
PowerExchange	PowerExchange is a PowerShell-based backdoor malware for Microsoft Exchange servers, enabling credential theft, command execution, and file exfiltration, while evading detection by utilizing the Exchange Web Services API for communication.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	f18575065970ef36e613ffa046f381fe9b01b3e9 2ba23d9115fb1c1d4c5899d34dc4772631d77eda 2b995ce4656db7257451080111705d5b98b45df3 68299DF5D8CE52845A8FC10598F138840094181C d82aad3222664ec9fb112808dfabbb56de9aa770		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Buhti Ransomware	Buhti ransomware, linked to Blacktail threat actors, employs leaked code of LockBit and Babuk variants. By exploiting vulnerabilities like PaperCut NG, they exfiltrate data and distribute ransomware. The addition of a custom Golang exfiltration tool heightens the evolving threat.	Exploiting known vulnerabilities	CVE-2023-27350 CVE-2022-47986
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data theft	PaperCut MF and NG & IBM Aspera Faspex
ASSOCIATED ACTOR			**PATCH LINK**
Blacktail			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219 https://www.ibm.com/support/pages/node/6952319
IOC TYPE	**VALUE**		
IPV4	91.215.85[.]183 81.161.229[.]120		

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
GobRAT	GobRAT, a new RAT, is infecting Linux routers in Japan through vulnerable web interfaces, granting attackers remote control and the ability to execute commands.	Exploiting known vulnerabilities In WEBUI accessible routers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
URLs	https[:]//su.vealcat[.]com http[:]//su.vealcat[.]com:58888 https[:]//ktlvz.dnsfailover[.]net http[:]//ktlvz.dnsfailover[.]net:58888		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BianLian ransomware	BianLian ransomware group is ramping up data-leak extortion to extract payments, using similar tactics & a custom backdoor, and bringing 30 new C2 servers online monthly.	valid RDP credentials	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Unauthorized execution of malicious code, data loss, system instability	Microsoft Netlogon Remote Protocol (MS-NRPC)
ASSOCIATED ACTOR			**PATCH LINK**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
IOC TYPE	**VALUE**		
SHA256	ea5c88fe464562227f483e8fc4eb2cf43e98a897aaaa3e94de4d236d5dc6e7e7 f3a4fb09a0498e7ab3b33338ca6bc03460e43d437d9f3afbfc1a521c1029ff19		

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
Bl00dy Ransomware	The Bl00dy ransomware operation launched in May 2022 and uses an encryptor based on the leaked LockBit source code rather than developing their own software.	Exploiting unpatched PaperCut servers	CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Unauthorized execution of malicious code, data loss, system instability	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
Tox ID	E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F		
IPV4	102.130.112[.]157 172.106.112[.]46 176.97.76[.]163		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clop Ransomware	Clop ransomware exfiltrates data that will be published on a leaked site if the victim refuses to pay the ransom.	Exploiting unpatched PaperCut servers	CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Unauthorized execution of malicious code, data loss, system instability	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c 0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3 c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d		

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
LockBit Ransomware	LockBit attacks typically employ a double extortion tactic to encourage victims to pay, first, to regain access to their encrypted files and then to pay again to prevent their stolen data from being posted publicly.	Exploiting unpatched PaperCut servers	CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Unauthorized execution of malicious code, data loss, system instability	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA1	2d15286d25f0e0938823dcd742bc928e78199b3d 864f56b25a34e9532a1175d469715d2f61c56f7f ef958f3cf201f9323ceae9663d86464021f8e10d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TrueBot	Truebot malware is a downloader malware that spreads through infected systems, collects information on targets, and deploys malicious payloads. The attacker's command and control (C2) receives the collected data.	Exploiting unpatched PaperCut servers	CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Unauthorized execution of malicious code, data loss, system instability	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
Domain	windowservicecemter[.]com		
SHA1	b918f97c7c6ebc9594de3c8f2d9d75ecc292d02b		

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
Cobalt Strike Beacons	Cobalt Strike is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors.	Exploiting unpatched PaperCut servers	CVE-2023-27350 CVE-2023-27351
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Unauthorized execution of malicious code, data loss, system instability	PaperCut MF and NG
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f		
Domain	study.abroad[.]ge		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Merdoor backdoor	A custom-written backdoor called Merdoor, which is a powerful and fully-featured malware that has been in existence since 2018. Merdoor is used selectively, appearing on only a few networks and machines, indicating highly targeted attacks for intelligence gathering purposes.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
Lancefly			-
IOC TYPE	**VALUE**		
SHA256	13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead 8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38		

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
ZXShell rootkit	The ZXShell rootkit includes a loader that drops a malicious Windows Kernel driver and creates a service. It is used to disable antivirus software and provide additional functions.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Financial and data losses	-
ASSOCIATED ACTOR			**PATCH LINK**
Lancefly			-
IOC TYPE	**VALUE**		
SHA256	1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221		

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 REGIONS
FIN7 (aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)	Russia	Casinos and Gambling, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation.	Australia, France, Malta, UK, USA.
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-27532	POWERTRASH Loader & DICELOADER	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition
TTPs			
T1497: Virtualization/Sandbox Evasion; T1059: Command and Scripting Interpreter; T1566: Phishing; T1001: Data Obfuscation; T1047: Windows Management Instrumentation; T1059.001: PowerShell; T1010: Application Window Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA505(Graceful Spider, Gold Evergreen, Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo, Spandex Tempest)	Russia	Education, Financial, Healthcare, Hospitality, Retail.	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	LOBSHOT	-
TTPs			
T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1027: Obfuscated Files orInformation, T1027.007: Dynamic API Resolution, T1140: Deobfuscate/Decode Files or Information, T1568: Dynamic Resolution, T1005: Data from Local System, T1083: File and Directory Discovery, T1033: System Owner/User Discovery, T1021: Remote Services, T1204: User Execution, T1204.002: Malicious File, T1021.005: VNC, T1041: Exfiltration Over C2 Channel, T1218: System Binary Proxy Execution, T1176: Browser Extensions, T1641: Data Manipulation, T1115: Clipboard Data, T1321: Data Encoding			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
1877 Team	Kurdistan	Governments, Universities, Telecommunication, Defense, and IT	Middle East, Africa, Asia
	MOTIVE		
	Hacktivist		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1003: OS Credential Dumping, T1005: Data from Local System, T1010: Application Window Discovery, T1012: Query Registry, T1018: Remote System Discovery, T1027: Obfuscated Files or Information, T1027.002: Software Packing, T1033: System Owner/User Discovery, T1036: Masquerading, T1047: Windows Management Instrumentation, T1055: Process Injection, T1055.012: Process Hollowing, T1056: Input Capture, T1056.001: Keylogging, T1057: Process Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Earth Longzhi (Subgroup of APT41)	China	Government, healthcare, technology, and manufacturing	Philippines, Thailand, Taiwan, and Fiji
	MOTIVE		
	Information theft and Espionage, financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2018-5713	Croxloader and SPHijacker	Malwarefox Anti-malware 2.72.169
TTPs			
T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1569: System Services, T1569.002: Service Execution, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1140: Deobfuscate/Decode Files or Information, T1070: Indicator Removal, T1070.004: File Deletion, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1548: Abuse Elevation Control Mechanism, T1548.002: Bypass User Account Control, T1068: Exploitation for Privilege Escalation, T1546: Event Triggered Execution, T1546.012: Image File Execution Options Injection			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Red Menshen (AKA Red Dev 18)	China	Telecommunications	Middle East and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	BPFDoor	-
TTPs			
T1071:Application Layer Protocol;T1205:Traffic Signaling;T1573:Encrypted Channel;T1562:Impair Defenses;T1059:Command and Scripting Interpreter;T1562.004:Disable or Modify System Firewall;T1040:Network Sniffing;T1572:Protocol Tunneling;T1205.002:Socket Filters;T1106:Native API;T1083:File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
SideCopy	Pakistan	Defense, Embassies, Government	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	SILENTTRINITY	-

TTPs
T1047: Windows Management Instrumentation, T1543: Create or ModifySystem Process, T1543.002: Systemd Service, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1036: Masquerading, T1070: Indicator Removal, T1070.006: Timestomp, T1112: Modify Registry, T1497: Virtualization/Sandbox Evasion, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1564: Hide Artifacts, T1564.001: Hidden Files and Directories, T1056: Input Capture, T1010: Application Window Discovery, T1018: Remote System Discovery, T1057: Process Discovery, T1082: System Information Discovery, T1083: File and Directory Discovery, T1518: Software Discovery, T1518.001: Security Software Discovery, T1114: Email Collection, T1071: Application Layer Protocol, T1095: Non-Application Layer Protocol, T1105: Ingress Tool Transfer, T1571: Non-Standard Port, T1573: Encrypted Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Dragon Breath APT (aka Golden Eye Dog & APT-Q-27)	Unknown	Online Gambling, Gaming	Philippines, Japan, Taiwan, Singapore, Hong Kong, and China
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Telegram, LetsVPN, and WhatsApp for Windows
TTPs			
T1120:Peripheral Device Discovery;T1091:Replication Through Removable Media;T1059:Command and Scripting Interpreter;T1574:Hijack Execution Flow;T1574.002:DLL Side-Loading;T1055:Process Injection;T1027:Obfuscated Files or Information;T1027.002:Software Packing;T1036:Masquerading;T1070:Indicator Removal;T1070.004:File Deletion;T1070.006:Timestomp;T1057:Process Discovery;T1082:System Information Discovery;T1083:File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
RA Group	Unknown	Manufacturing, Wealth Management, Insurance Providers, and Pharmaceuticals	United States and South Korea
	MOTIVE		
	Information theft and espionage; Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1083: File and Directory Discovery; T1490: Inhibit System Recovery; T1496: Resource Hijacking; T1552: Unsecured Credentials; T1560: Archive Collected: Data; T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)	North Korea	Think tanks, Research universities, and government entities.	United States, Europe, and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ReconShark	Microsoft OneDrive
TTPs			
T1053:Scheduled Task/Job;T1059:Command and Scripting Interpreter;T1090:Proxy;T1566:Phishing;T1566.002:Spearphishing Link;T1547:Boot or Logon Autostart Execution;T1547.001:Registry Run Keys/Startup Folder;T1132:Data Encoding;T1012:Query Registry;T1047:Windows Management Instrumentation;T1070:Indicator Removal;T1070.004:File Deletion;T1059.005:Visual Basic;T1204:User Execution;T1204.002:Malicious File;T1104:Multi-Stage Channels			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Lancefly APT	China	Government, aviation, education, and telecoms	South and Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Merdoor backdoor, ZXShell rootkit	-
TTPs			
T1057: Process Discovery; T1014: Rootkit; T1219: Remote Access Software; T1059: Command and Scripting Interpreter; T1112: Modify Registry; T1021: Remote Services; T1003: OS Credential Dumping; T1056: Input Capture; T1574: Hijack Execution Flow; T1055: Process Injection; T1090: Proxy; T1056.001: Keylogging; T1574.001: DLL Search Order Hijacking; T1218: System Binary Proxy Execution; T1027: Obfuscated Files or Information; T1566: Phishing; T1110: Brute Force; T1059.001: PowerShell; T1218.011: Rundll32; T1003.001: LSASS Memory; T1036: Masquerading; T1560.001: Archive via Utility; T1021.002: SMB/Windows Admin Shares			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)	Russia	Research facilities, Education, Small Businesses, Media organizations, Government facilities, Financial Services, Manufacturing, and Communications.	North America, South America, Europe, Africa, Asia, and Australia.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Snake (aka Uroburos, Urouros)	Windows, MacOS, and Linux

TTPs
T1095:Non-Application Layer:Protocol;T1104:Multi-Stage Channels;T1106:Native API;T1001:Data Obfuscation;T1001.003:Protocol Impersonation;T1003:OS Credential Dumping;T1014:Rootkit;T1027:Obfuscated Files or Information;T1027.002:Software Packing;T1036:Masquerading;T1040:Network Sniffing;T1046:Network Service Discovery;T1055:Process Injection;T1055.001:Dynamic-link Library Injection;T1056:Input Capture;T1056.001:Keylogging;T1059:Command and Scripting Interpreter;T1059.001:PowerShell;T1071:Application Layer Protocol;T1071.001:Web Protocols;T1071.003:Mail Protocols;T1071.004:DNS;T1074:Data Staged;T1078:Valid Accounts;T1083:File and Directory Discovery;T1090:Proxy;T1090.003:Multi-hop Proxy;T1112:Modify Registry;T1119:Automated Collection;T1132:Data Encoding;T1132.002:Non-Standard Encoding;T1135:Network Share Discovery;T1140:Deobfuscate/Decode:Files or Information;T1190:Exploit Public-Facing Application;T1482:Domain Trust Discovery;T1546:Event Triggered:Execution;T1546.016:Installer Packages;T1547.006:Kernel Modules and Extensions;T1559:Inter-Process Communication;T1560.003:Archive via Custom Method;T1564:Hide Artifacts;T1569.002:Service Execution;T1570:Lateral Tool Transfer;T1572:Protocol Tunneling;T1573:Encrypted Channel;T1588:Obtain Capabilities;T1610:Deploy Container

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SideWinder (aka Rattlesnake, T-APT-04, APT-C-17, Razor Tiger, Baby Elephant, Operation Origami)	India	Military, Government, and Business Entities	Pakistan, Turkey, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam, Afghanistan, China, and Nepal
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-0199	-	Microsoft Windows, Windows Server, Office
TTPs			
T1518:Software Discovery;T1480:Execution Guardrails;T1574:Hijack Execution Flow;T1559:Inter-Process Communication;T1027:Obfuscated Files or Information;T1047:Windows Management Instrumentation;T1059:Command and Scripting Interpreter;T1071:Application Layer Protocol;T1105:Ingress Tool Transfer;T1140:Deobfuscate/Decode Files or Information;T1203:Exploitation for Client Execution;T1204:User Execution;T1221:Template Injection;T1204.002:Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Blacktail	Unknown	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-27350 CVE-2022-47986	Buhti Ransomware	PaperCut MF and NG & IBM Aspera Faspex
TTPs			
T1047:Windows Management Instrumentation;T1059:Command and Scripting Interpreter;T1129:Shared Modules; T1027:Obfuscated Files or Information; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1003:OS Credential Dumping;T1056:Input Capture;T1056.001:Keylogging;T1057:Process Discovery;T1082:System Information Discovery; T1083:File and Directory Discovery;T1518:Software Discovery; T1518.001:Security Software Discovery; T1005:Data from Local System; T1185:Browser Session Hijacking;T1486:Data Encrypted for Impact; T1489:Service Stop			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Water Orthrus	Unknown	-	China
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1566: Phishing; T1195: Supply Chain Compromise; T1218: System Binary Proxy Execution; T1218.002: Control Panel; T1204: User Execution; T1202: Indirect Command Execution; T1070: Indicator Removal; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1542: Pre-OS Boot; T1542.003: Bootkit; T1027: Obfuscated Files or Information; T1020: Automated Exfiltration; T1087: Account Discovery; T1110: Brute Force; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1082: System Information Discovery; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1021: Remote Services; T1056: Input Capture; T1046: Network Service Discovery; T1047: Windows Management Instrumentation			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
8220 Gang (8220 Mining Group)	China	Technology, Cloud Services	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-3506	MgBot	Oracle WebLogic Server
TTPs			
T1140: Deobfuscate/Decode Files or Information; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1071: Application Layer Protocol; T1204.002: Malicious File; T1071.001: Web Protocols; T1566: Phishing; T1204: User Execution; T1190: Exploit Public-Facing Application; T1525: Implant Internal Image; T1132: Data Encoding; T1055: Process Injection; T1132.001: Standard Encoding; T1027: Obfuscated Files or Information; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1027.010: Command Obfuscation; T1055.002: Portable Executable Injection; T1620: Reflective Code Loading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Camaro Dragon	China	Foreign Affairs Entities	Europe
	MOTIVE		
	Information theft and Espionage; Sabotage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1566: Phishing; T1189: Drive-by Compromise; T1542: Pre-OS Boot; T1542.001: System Firmware; T1542.003: Bootkit; T1095: Non-Application Layer Protocol; T1210: Exploitation of Remote Services			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT28 (aka FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and Gas, Think Tanks, and Intelligence organizations	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-23397	-	Microsoft Windows
TTPs			
T1176:Browser Extensions; T1014:Rootkit; T1114:Email Collection; T1566:Phishing; T1056:Input Capture; T1134:Access Token Manipulation; T1204:User Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GUI-vil (aka p0-LUCR-1)	Indonesia	Cloud computing and technology services	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-22205	-	GitLab Community and Enterprise Editions From 11.9
TTPs			
T1596:Search Open Technical Databases; T1098:Account Manipulation; T1078:Valid Accounts; T1068:Exploitation for Privilege Escalation; T1496:Resource Hijacking; T1021:Remote Services; T1021.004:SSH; T1211:Exploitation for Defense Evasion; T1538:Cloud Service Dashboard			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GoldenJackal APT	Unknown	Government and Diplomatic entities	Middle East and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-30190	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher	Microsoft Windows
TTPs			
T1027:Obfuscated Files orInformation; T1219:Remote Access Software; T1059:Command and ScriptingInterpreter; T1112:Modify Registry; T1021:Remote Services; T1003:OS Credential Dumping; T1056:Input Capture; T1574:Hijack Execution Flow; T1055:Process Injection; T1090:Proxy; T1566:Phishing; T1218:System Binary Proxy Execution; T1566.001:Spearphishing Attachment; T1190:Exploit Public-Facing Application; T1021:Remote Services; T1041:Exfiltration Over C2 Channel; T1555:Credentials from Password Stores; T1005:Data from Local System; T1102:Web Service; T1113:Screen Capture; T1204:User Execution; T1204.002:Malicious File; T1036:Masquerading; T1221:Template Injection; T1588:Obtain Capabilities; T1588.005:Exploits; T1092:Communication Through Removable Media; T1053:Scheduled Task/Job			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
BianLian	Unknown	Hospitality, Real Estate, Manufacturing, Food Products, Professional Services, Education, Construction & Engineering, Health Care, Consumer Discretionary, Diversified Telecommunication	Canada, United States, United Kingdom, India, Sweden, France, Germany, Spain, Austria, Switzerland, Turkey, Cyprus, Indonesia, Australia, Northern Ireland
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2020-1472	BianLian ransomware	Microsoft Netlogon Remote Protocol (MS-NRPC)

TTPs
T1552:Unsecured Credentials;T1567.002:Exfiltration to Cloud Storage;T1569:System Services; T1027:Obfuscated Files or Information;T1055:Process Injection;T1140:Deobfuscate/Decode Files or Information;T1587:Develop Capabilities;T1587.001:Malware;T1083:File and Directory Discovery; T1059:Command and Scripting Interpreter;T1059.001:Power Shell;T1069.002:Domain Groups; T1190:Exploit Public-Facing Application;T1053:Scheduled Task/Job;T1053.005:Scheduled Task; T1059.004:Unix Shell;T1078:Valid Accounts;T1574:Hijack Execution Flow;T1562:Impair Defenses; T1562.001:Disable or Modify Tools;T1003:OS Credential Dumping;T1003.001:LSASS Memory; T1003.003:NTDS;T1486:Data Encrypted for Impact; T1133:External Remote Services; T1566:Phishing;T1059.003:Windows Command Shel;T1098:Account Manipulation;T1552.001:Credentials In Files;T1087:Account Discovery;T1087.002:Domain Account;T1482:Domain Trust Discovery;T1083:File and Directory Discovery;T1046:Network Service Discovery;T1135:Network Share Discovery;T1012:Query Registry;T1018:Remote System Discovery;T1033:System Owner User Discovery;T1021:Remote Services; T1021.001:Remote Desktop Protocol;T1115:Clipboard data;T1105:Ingress Tool Transfe;T1219:Remote Access Software:T1537:Transfer Data to Cloud Account;T1048:Exfiltration Over Alternative Protocol;T1567:Exfiltration Over Web Service

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
		T1583.005: Botnet
	T1584: Compromise Infrastructure	T1584.005: Botnet
	T1586: Compromise Accounts	T1586.002: Email Accounts
		T1586.003: Cloud Accounts
	T1587: Develop Capabilities	T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.003: Code Signing Certificates
		T1588.004: Digital Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.003: Install Digital Certificate
		T1608.005: Link Target
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1047: Windows Management Instrumentation	
	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1559: Inter-Process Communication	
	T1569: System Services	T1569.002: Service Execution

Tactic	Technique	Sub-technique
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.004: Winlogon Helper DLL
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification
	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.011: Services Registry Permissions Weakness
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.003: Thread Execution Hijacking
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.002: Systemd Service
		T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.004: Winlogon Helper DLL
		T1547.006: Kernel Modules and Extensions
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.011: Services Registry Permissions Weakness

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.002: Software Packing
		T1027.005: Indicator Removal from Tools
		T1027.009: Embedded Payloads
	T1036: Masquerading	T1036.001: Invalid Code Signature
		T1036.007: Double File Extension
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.003: Thread Execution Hijacking
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.006: Timestomp
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1112: Modify Registry	
	T1127: Trusted Developer Utilities Proxy Execution	T1127.001: MSBuild
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1218: System Binary Proxy Execution	T1218.001: Compiled HTML File
		T1218.005: Mshta
		T1218.007: Msiexec
		T1218.011: Rundll32
	T1221: Template Injection	
	T1222: File and Directory Permissions Modification	
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
TA0006: Credential Access	T1003: OS Credential Dumping	
	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	
	T1212: Exploitation for Credential Access	
	T1552: Unsecured Credentials	T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.002: User Activity Based Checks
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.007: VBA Stomping
		T1564.010: Process Argument Spoofing
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.011: Services Registry Permissions Weakness
	T1601: Modify System Image	T1601.001: Patch System Image
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
	T1135: Network Share Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.002: User Activity Based Checks
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1615: Group Policy Discovery	
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
	T1091: Replication Through Removable Media	
	T1210: Exploitation of Remote Services	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1125: Video Capture	
	T1213: Data from Information Repositories	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1602: Data from Configuration Repository	T1602.002: Network Device Configuration Dump

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1001: Data Obfuscation	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
		T1573.001:Encrypted Channel: Symmetric Cryptography
	T1092:Communication Through Removable Media	
	T1205:Traffic Signaling	T1205.002:Traffic Signaling Socket Filters
	T1572:Protocol Tunneling	
	T1104:Multi-Stage Channels	
	T1132:Data Encoding	
	T1571:Non-Standard Port	
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1496: Resource Hijacking	
	T1499: Endpoint Denial of Service	
	T1529: System Shutdown/Reboot	
	T1531: Account Access Removal	
	T1565: Data Manipulation	T1565.001: Stored Data Manipulation

Top 5 Takeaways

#1 In **May**, there were **nine zero-day** vulnerabilities. **GoldenJackal APT** and **MEME#4CHAN** phishing campaign exploited one of this **Celebrity** vulnerabilities.

#2 Throughout the month, various ransomware strains including **CACTUS**, **Rancoz**, **CryptNet**, **MichaelKors**, **Buhti**, **BianLian**, and **Bl00dy** actively targeted victims

#3 The **Philippines**, **Turkey**, **India**, **UAE**, and **Afghanistan** were the most **targeted** countries throughout the month.

#4 There were a total of **20** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: **Government**, **Manufacturing**, **Education**, **Finance**, and **Healthcare**.

#5 The **two** unpatched vulnerabilities, **CVE-2023-29552**, which can lead to potential losses of up to **$120,000,** and **CVE-2018-5713**, exploited by **Earth Longzhi APT,** have been actively utilized in attacks

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **21 significant vulnerabilities** and block the indicators related to the **20 active threat actors, 47 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 **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 (MAY 2023)

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

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

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

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

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
ViperSoftX	SHA256	09620efdc1324f063aec6aa3d822c194f253d9393c5a7b4f7c8880b8fa260d2c 0d8e99281629352c68e5d1e462db3b003571fdc21149d6834bd2aa2d86ea03b9 2769ff525276045565a15fb959ae54a1ba294eb7903fa80a8656577d7dd5e76c 30a7ff659d267e9e201273087d4ced99f6eefe3078b40f38a1f6c5ff4e6d4fd3 380697610810cdecaa497ad75b031106b486bc6c7da78add23885a963aab6dc0 3d19c605f3d4a84bd76190acd23838e4c9362fef3ec5c80bd049ee25bbafb862 416fad3d260add53a44052b726c1e911632012221c1e28942389ca0dd2902394 4c1021cd1863369e59e9087c34fee936281789e65cbbda464b0948aecb592807 516517135c39aee7b2aeecbfae063deb9b8869ca993f60120d7c5ee90ee90444 51c862efdb6b52c42dfe4f25c471c82c0368c0b9f8b194d07f9dcc4245b46394 5232a2a668c95ee6ab24cba79ed7bf4e9598a750020a2a88a2f352d2f667b7c5 5e9d9016bbb70c1b4b02f13d5a12e112250651a77bf5b89a92d124d0f8576cdb 66c98bb87c3bfc97e137ef3fc22e498ff1fb7368d82c2641db4998d090d31ef4 671756d73f9e8f35f9a71b102d474415aada55f1a846b0c20b73daf554d03173 696978b39b7afc97d4b7d6a3ab56b6b991fab9f9e511e722a2db5b8459679240 6a7ccf87978dad1a2d1a1a52100101fb330d966ff6cd990b1d04eb627ef4530c 6b23b6615b1287bf4ec20eab532921cabeb72e08af089782d5c827e48334ba36 6b8809f6f282778aeaa9634e1108f0776066d32e096526fa4c00cbba3dacc30e 6ca4b83ff71f42e15032e59a47b8275c298d28c2dcc646c4e4325b2243425235 8047b20dc50317fb38f7e805992b65eabad92362acd8ff728903da5a86e4f23d 83b8eca3bc4fe79fa47d918d34917344a2e179b0c4efc5c769b9f3a380a65247

Attack Name	TYPE	VALUE
ViperSoftX	SHA256	85ecdeb135cf384cb82e62dea82baa7c01f56e88bdabb5784ee7401cd5537e69 8a2939ad4ee9cea394aba543b98076504cfdfafce76cecfb8fc88ade77bb6f59 8eff0c96aecd3f144a26699b8f3d6ec8d44b9ae4154417121f604d5297073cd8 96ddf314a4c6f10936622361416ac9b93b5cf4b61b148bfb42592d22a83f0634 a498168cdac52a10a25499a46e0d30db2db86c4dadd737bb6628c61a99810b79 aaf389bbbe02c31bf4605fcba51b1d5228337358cf66efafe979f782251b7fc5 b59dce85b24f078285d73553a05cd157c11d3495f399b753f21b3e7506bbe60f bb681757fc4dac5a64bf1b263e0ddd16db6e055d0efb2089ad04af5bba007d0a c313e51f884672b16adcb0731bc338a554ff351fdbe921d266564c67dc730fcc d07a06783eb4fde909c0f4f09ec6f69a91820010b9327fc7fa318b199f1ca1e4 d5799651ab7bb5939136addde222255f81e090c3c127d05727b71b3b2cbc9860 f1e6821caa29aade550171d640ed5605556e7d074542eea5d5370168f2c09880 f310e01a9ed40b6563b88de23d560cf839079b503260eb86a7bc32160129170b f39386ba9605b7a1ac360a8460c4f5c5fc916d5c159ba3ba226545447cd7e4c7 fa31f03cfbb8ae682deab86660810ca244a718009cf4a24827699d679139067d 083837c37de9fce9e49257bc2b38dec11530b990b023fadc6f82a7cb00685fc0 0ca08b8044c466e286fb5ec2162a23fe35dda700019a1bc9f4528c777abb2a69 1b26d62c80689746de39869dfab8d8f05257bd16e46fe923344988802569be10 204a056399bbb7e1b4fcf2bdd8f463cf2d3ff21d9f7c5b745d74d62eb6184e88 22981d8cd10e0aeede5a2c5c209cf2d1a46b9eb54f85eca9f97d816b202d186b 2f936ccac29c88745093564858c4cb0cd6fed5bba997c3db71d7157f8c530be5 33fb5151edd9f921e0793575b5d1a5a24f75370455b3413405a2e66f02746e47 34ac92dfb29936f8af4e270da0d36b7cb4ffa743b115e2bfed23b0e127b38d0e

Attack Name	TYPE	VALUE
ViperSoftX	SHA256	46a96def15c2dbd0825d008f11de605e912184aa40dbbe9295333a5d80ec45f9 515f32da068c171f1dd03472be04327d55cf6d2c5d40268fc1e61abb75e86616 53744ca02d82f1f966a3f882a17fbd424955991496b486e8dc4022e5a939c286 5b8b64cfba9e3771f586c5aa4f69fe210ecd1f037a6818cacf31cba543f1958d 6614299d5f9c1754a894597bd4fa894415d455df1dd4da6a96b717d2206b511a 6753eadd2cd36978630a31d9c9efbe12d09cf139916feee0d145b09ad18750f6 6c5d40b9484287b3a8eac469e0383b1309689e22d1726e36428e278cd883cc2f 6d18365010a19c4e74056d7a7c64d1046ef10a02ec7938fc936ac61898db5ed7 70c8cf961923f93aab18e771c2eb4a09683223129944cab26f75bff35449be8a 7176b56faa36c2275ff6728864d40eb92fbf956d0b6ae09907816811be94e22e 7516f43db52f494ce788ba514590d39cf26da53728388a26e400df4c944e1d18 7576ce1542ac29c8f5f7585d8c19b6a716242ef21f9b6a87c92718220544d467 7890a7ae77a4ebeca05c344946d8a0a308e263ca88a8ca4530d6566bffa331b8 7a22bc09774dbd2d982596804f6eb767074019ce33cc5ffe8efa9c2e1972de86 80f0eed86e0499bbafbcb956e7f6f81b6a56dba56716082cf9ed280f35b355e8 90497bf6dc0724220a21694303c816cdc1f8c815f25c2cef5f2f53478d84752e 91a2a76932341c1e0df8f7b4058d87e69133cee839559f0146cccb42f1b14fea 95e6d8d692e7c7bc6e78389c4b8719ee05e6f71d6447aa016b5682496aef0385 978d83bcc3361c62d5974c33f56c2ab72618a13f9ccc0c37c6b1e824fe74e03e 983038dc5a3650de4f5ce46763a5c8e7e4441c5960e0c1f20f3ca9ff1561fefe a2f6ce37dd1c14fb789e1531e04fac2716e659fa5232295cd8b80b2994b93819 ad1b21536bf9892d070b72b0609970677ba45b9e53c05936dfb1a4f299930a84 b006d1043f97d47339ba1b6816d6c728207fe280a56d7fc10e5b7e7f0b969836

Attack Name	TYPE	VALUE
ViperSoftX	SHA256	b3600c49c758f86e496d2b5efdbad239a218e74ca014c80f6bb7445f6fe7e4c6 b813b13d41fd4d824bd146ba9e7bead121362039ab79379ff15702c54476a703 bbaa007a1f4e3c62615e5886e4b91dc24545ed60232ec8290ec203f12a78d1d7 bd9b5b3ed93ec879a270a767e1beddc836ab5802fcb49e48cb154eb898389e49 c42a6b316558eed903c3c41b7da6120bf809e918da51119cbeea27f7047ab71d cc6bcb0f72789c7781550d0c184a1b94c5592f31e6459cc9754525232938a331 cf7b4af2c9497c97a2a9cb7f0e5818e76ccf534c3392d6b8d16be415d5a8ffbc d1556221a4bac69453c9bafaf7b7c753e3fd36aac171e3695c88265a22bd7889 d28910954ea84e6f8bad1f844333c3945416f6aeb8cb25e76bfee2319d029847 d7d4c5383a032e8090512f18a0e6387e2de78328c6fac8b6bcefc40a07cde212 d80a423aa16751868dd36d144a4a0e06335593c585187d77e2d00e913bbc95d1 dc0fe945dc3fcab4b4fa4ee9868c75d66719941b33189710dc5bf8b981f55ae8 dc58f7bd854e1537085324068f3a6e675831a5c4c441f9a2059cc7c40a59c61a e022dd5086aa6b1bc91489a3ed81a2143b8b78616d3285c00d6df4bc504f32fe e4c705b6b93315d728d9ee5fd17734f3968620ecdc255955600f06eeefa252d8 e82cf0af68ec6ec4097d7bd0a5573af50aac191484e983bc9b298b30a7185aeb fd60eaf4d48f49ade5641aa928a30ac35721dbee52e69525132a9e3b1981eab7 Ff03b15d57942f671b7c0b9cb978873b2314d13bf4f6603e7b26f3339fbe0c2a 0a0b5f64870c166c1fe246a7ac815f738e15dbc8481b985da862026f61c48282 3529336d0733bd2ee92acc8ed332f6c4eed36a8b0b272371ffdeb80117689b26 42018acd1660989d939814b2bdfaac086540f7a793b0d1b5b82ef72cd7dc2d6a 7c028a7a4eccd48049f0b66ab0211cccf136e56d2af8cd27cfb1c720a43993d0 88c46a74d0b7ba05e4641628f546cf29b322f1e0147b5bcb8439f3716f6da847

Attack Name	TYPE	VALUE
ViperSoftX	SHA256	c73053fafaeff83d1cad7256aaa6ec7ad8e91ee5c2514c8b7b9de0307ae724a0 527982073113924b7e168b8fdd21beee42923510b58ca2ab444a4a6a4619f78a
	Domains	http://ahoravideo-schnellvpn[.]xyz http://chatgigi2[.]com http://arrowlchat[.]com http://static-cdn-349[.]net
POWERTRASH Loader	IPV4	217[.]12.206.176 162[.]248.225.115 45[.]136.199.128 91[.]149.243.181 91[.]199.147.152 95[.]217.49.123 77[.]75.230.112 194[.]87.148.41 195[.]123.244.162
	SHA1	8687b6b1508a93556d6e30d14e5c4ee9971f2d80 E5480a47172e3f75dbf0384f4ca82c7b47910e0f
DICELOADER (also known as Lizar)	SHA1	b621f8c5e9033718b4e9d47a2f0eccb9783f612a
	IPV4	217[.]12.206.176 162[.]248.225.115 45[.]136.199.128 91[.]149.243.181 91[.]199.147.152 95[.]217.49.123 77[.]75.230.112 194[.]87.148.41 195[.]123.244.162
Mirai Botnet	SHA256	b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2 2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599 4cb8c90d1e1b2d725c2c1366700f11584f5697c9ef50d79e00f7dd2008e989a0 461f59a84ccb4805c4bbd37093df6e8791cdf1151b2746c46678dfe9f89ac79d

Attack Name	TYPE	VALUE
Mirai Botnet	SHA256	aed078d3e65b5ff4dd4067ae30da5f3a96c87ec23ec5be44fc85b543c179b777 0d404a27c2f511ea7f4adb8aa150f787b2b1ff36c1b67923d6d1c90179033915 eca42235a41dbd60615d91d564c91933b9903af2ef3f8356ec4cfff2880a2f19 3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3ceeec51018ef4d aaf446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b
	IPV4	185[.]225[.]74[.]251
	URLs	http[://]185[.]225[.]74[.]251/armv4l http[://]185[.]225[.]74[.]251/armv5l http[://]185[.]225[.]74[.]251/armv6l http[://]185[.]225[.]74[.]251/armv7l http[://]185[.]225[.]74[.]251/mips http[://]185[.]225[.]74[.]251/mipsel http[://]185[.]225[.]74[.]251/sh4 http[://]185[.]225[.]74[.]251/x86_64 http[://]185[.]225[.]74[.]251/i686 http[://]185[.]225[.]74[.]251/i586 http[://]185[.]225[.]74[.]251/arc http[://]185[.]225[.]74[.]251/m68k http[://]185[.]225[.]74[.]251/sparc
	Domains	zvub[.]us
LOBSHOT	IPV4	95.217.125[.]200
	SHA256	e4ea88887753a936eaf3361dcc00380b88b0c210dcbde24f8f7ce27991856bf6
Croxloader	IPV4	194.31.53[.]128 198.13.47[.]158 172.67.139[.]61 207.148.115[.]125 64.227.164[.]34 194.31.53[.]128 198.13.47[.]158
	Domains	evnpowerspeedtest[.]com www.updateforhours[.]com dns.eudnslog[.]com asis.downloadwindowsupdate[.]co

Attack Name	TYPE	VALUE
Croxloader	SHA256	7910478d53ab5721208647709ef81f503ce123375914cd504b9524577057f0ec ebf461be88903ffc19363434944ad31e36ef900b644efa31cde84ff99f3d6aed 21ffa168a60f0edcbc5190d46a096f0d9708512848b88a50449b7a8eb19a91ed 942b93529c45f27cdbd9bbcc884a362438624b8ca6b721d51036ddaebc750d8e 75a51d1f1dd26501e02907117f0f4dd91469c7dd30d73a715f52785ea3ae93c8 4399c5d9745fa2f83bd1223237bdabbfc84c9c77bacc500beb25f8ba9Df30379 8327cd200cf963ada4d2cde942a82bbed158c008e689857853262fcda91d14a4 9eceba551baafe79b45d412c5347a3d2a07de00cc23923b7dee1616dee087905 630bb985d2df8e539e35f2da696096e431b3274428f80bb6601bbf4b1d45f71e ef8e658cd71c3af7c77ab21d2347c7d41764a68141551938b885da41971dd733 e654ecc10ce3df9f33d1e7c86c704cfdc9cf6c6f49aa11af2826cbc4b659e97c 16887b36f87a08a12fe3b72d0bf6594c3ad5e6914d26bff5e32c9b44acfec040 39de0389d3186234e544b449e20e48bd9043995ebf54f8c6b33ef3a4791b6537
Atomic Stealer	MD5	5e0226adbe5d85852a6d0b1ce90b2308
	URLs	hxxp[:]//amos-malware[.]ru/sendlog
	SHA256	15f39e53a2b4fa01f2c39ad29c7fe4c2fef6f24eff6fa46b8e77add58e7ac709
	Domains	amos-malware[.]ru amos-malware[.]ru/sendlogillegal
	IPV4	37[.]220.87[.]16
	SHA1	0a87b12b2d12526c8ba287f0fb0b2f7b7e23ab4a 24c9f5c90ad325dae02aa52e2b1bac2857ae2faf 36997111b5e7aa81b430a72df9f54bac2a9695ba 7534b4ef7727d14b4fdd32d18651d32572c7747b 0db22608be1172844c0ebf08d573ea4e7ef37308 2681a24f0ec0b1c153cc12d5d861c0c19c8383ea 385b9cc7d3147f049e7b42e97f242c5060fc9e97 46426409b9e65043b15ce2fcddd61213ff4e5156 48a0a7d4f0ae4b79b4f762857af3bbb02e8ab584

Attack Name	TYPE	VALUE
Atomic Stealer	SHA1	4f25d1a1aa18c8d85d555cd7a8f1cf2cf202af8c 58a3bddbc7c45193ecbefa22ad0496b60a29dff2 5d2e995fa5dce271ac5e364d7198842391402728 79007aabf9970e0aff7df52fd1c658b69f950c6f 793195d48cce96bb9b4fc1ee5bac03b371db75f7 82f4647e6783b012fc9a1f86108c644fcf491cf6 849cde22d1d188cc290bb527bbd7252ad07099af 9058ab6e05cb1f9ce77e4f8c18324a6827fb270d 97b19a82a32890d5ddaecac5a294cc3384309ea9 98f98a737a26c9dd1b27c474715976356ea4e18b aab3a2897950e85a2b957f77d2f100e61e29061c b42243d72765f142953bb26794b148858bff10a8 ca05f80fe44174d1089077f4b2303c436653226f d5db5a11b9605d54cf66a153b0112b91c950d88f d9d46ecfc1100d2b671ad97dc870e879d2634473 de465aad6cde9f0ce30fce0157bc18abf5a60d40 e114f643805394caece2326fb53e5d3a604a1aa9 f28025717f9db8a651f40c8326f477bf9d51a10f 1f29b00c18bc0b7e1dfee5e79f8111da09f8fab8 a02730f734032ed0f3b3705926b657aa4b88d720 c70fdf4362eb56032793ab08e6aeb892f1bd4a9b e951b889aabca7ee5b0ff9d06a057884ed788b70
BlackBit	MD5	90bae9356dc021172d0ff06603e7a4cf bf528ecf7601043fe7931ed1fdd1d081 9d898e39591f9a8b49fa27841acb7392 d37b49b0a53fd07895ca4dc956cbc459 8ead445620033ecee6c426cfbeac214b
	SHA1	b04ccaa781be7521d50faa36db269f71ac56af58 2f052cc3e64870b8ac28efb2d79bc2b16dff3e8e e9b35995bf772cd11be13bc5c9ac93c846f00405 3cac81473dd91e7adf4516f1805bc5bdfeb562e4 7fd07c934ce9b7c4ad902408ed528acf4ce32ddb
	SHA256	1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e6 03161e3f18db2f b8ffd72534056ea89bfd48cbe6efb0b4d627a6284a7b763fdb7 dfd070c1049ba 43c6aef23a90c742274d6db2148a5cb5027c82e94ba2db4ae4 b4184956e370b5 cd29a952a51204f2e8744271b822c277b63ad8a54e3a6422e3 42eb9c53df0bda b3324b629febeefb17201abb52bc66094b4ffb292f8aa3a549f3 9e7e11c63694

Attack Name	TYPE	VALUE
SILENTTRINITY	SHA256	9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce bf34077c8b22759b28dcc458dc1b7bba3810c1c30b050b26a26e8d9f64e77971 c7753ffb7f66b0dfb05a24955324182cb92bbf41dd8fccb308c3f04d497a16da a2e55cbd385971904abf619404be7ee8078ce9e3e46226d4d86d96ff31f6bb9a e88835e21c431d00a9b465d2e8bed746b6369892e33be10bc7ebbda6e8185819 68ec4461653ae682eeace1bff583307ec521a3ee23873a991c031cc49dc8132f b9514ed1566c8ce46ab5bfd665f8b997f2d5624740f298699df43bb108e08c4d 85faf414ed0ba9c58b9e7d4dc7388ba5597598c93b701d367d8382717fb485ec 1c2399674713d2a3fc19b841e979eed61d73d1b7ca8fd6f29ba95a41f5a7684d f0cc9b18ba32f95085d5f9a3539dc08832c19e7d3124a5febbdc3bae47deab24 17eabfb88a164aa95731f198bd69a7285cc7f64acd7c289062cd3979a4a2f5bf 865e041b41b9c370a4eed91a9a407bd44a94e16e236e07be05e87de319a4486c
	URLs	hXXp://cornerstonebeverly[.]org hXXp://cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime[.]hta hXXps://cornerstonebeverly[.]org/js/files/ntfonts/avena/ hXXp://cornerstonebeverly[.]org/js/files/ntfonts/jquery[.]txt hXXp://144.91.72[.]17:8080/user_details hXXp://144.91.72[.]17:8080/streamcmd?AV=Unknown&OS=6.1.7601.17932&Vesrion=1&detail=Wfstzepn_Admin
Akira ransomware	SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
ReconShark	Domain	yonsei[.]lol
	URLs	https[:]//rfa[.]ink/bio/r.php https[:]//mitmail.tech/gorgon/r.php https[:]//rfa[.]ink/bio/t1.hta https[:]//mitmail[.]tech/gorgon/t1.hta https[:]//rfa[.]ink/bio/ca.php?na=reg.gif

Attack Name	TYPE	VALUE
ReconShark	URLs	https[:]//mitmail.tech/gorgon/ca.php?na=reg.gif https[:]//rfa[.]ink/bio/ca.php?na=secur32.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=secur32.gif https[:]//newshare[.]online/lee/ca.php?na=secur32.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_eset.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_eset.gif https[:]//rfa[.]ink/bio/ca.php?na=video.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=video.gif https[:]//rfa[.]ink/bio/ca.php?na=start2.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start2.gif https[:]//rfa[.]ink/bio/ca.php?na=start4.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start4.gif https[:]//rfa[.]ink/bio/ca.php?na=start3.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start3.gif https[:]//rfa[.]ink/bio/ca.php?na=videop.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=videop.gif https[:]//rfa[.]ink/bio/ca.php?na=start1.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start1.gif https[:]//rfa[.]ink/bio/ca.php?na=vbs_esen.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs_esen.gif https[:]//rfa[.]ink/bio/ca.php?na=start0.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start0.gif https[:]//rfa[.]ink /bio/d.php?na=vbtmp https[:]//rfa[.]ink/bio/ca.php?na=vbs.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs.gif https[:]//rfa[.]ink/bio/d.php?na=battmp https[:]//rfa[.]ink/bio/ca.php?na=dot_v3.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_v3.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_esen.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_esen.gif http[:]//rfa[.]ink/bio/ca.php?na=dot_avg.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_avg.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_kasp.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_kasp.gif
	SHA1	86a025e282495584eabece67e4e2a43dca28e505 c8f54cb73c240a1904030eb36bb2baa7db6aeb01
AndoryuBot	IPV4	163[.]123[.]142[.]146 45[.]153[.]243[.]39
	SHA256	ea064dd91d8d9e6036e99f5348e078c43f99fdf98500614bffb736c4b0fff408 f42c6cea4c47bf0cbef666a8052633ab85ab6ac5b99b7e31faa1e198c4dd1ee1 3441e88c80e82b933bb09e660d229d74f7b753a188700fe018e74c2db7b2aaa0

Attack Name	TYPE	VALUE
AndoryuBot	SHA256	3c9998b8451022beee346f1afe18cab84e867b43c14ba9c7f04e5c559bfc4c3a b71b4f478479505f1bfb43663b4a4666ec98cd324acb16892ecb876ade5ca6f9 e740a0d2e42c09e912c43ecdc4dcbd8e92896ac3f725830d16aaa3eddf07fd5c 4fe4cff875ef7f8c29c95efe71b92ed31ed9f61eb8dfad448259295bd1080aca 2e7136f760f04b1ed7033251a14fef1be1e82ddcbff44dae30db12fe52e0a78a 1298da097b1c5bdce63f580e14e2c1b372c409476747356a8e9cfaf62b94513d 55e921a196c92c659305aa9de3edf6297803b60012f83967562a57547875fec1
Snake (aka Uroburos, Urouros)	SAH256	6a4836cd5847c3d42b846d1616cc94429ec27446555b66f9abf061e7747bdca0 3c3511a9b6d98f49943cbec9355ebb8a006706f42304f608b6d9eb6f2da79718 735808b3dfad2472c5785399b6e34bf5cccef1153ad15bd1167420ff05b1a9d8 ff51c7ab066f425f73ba2005dbf3d2be4bc5344b152f18818c0ea5da81368ef0 1c05f794c40193734a68e145ca1aaf7268b37f6fe3ea2bea5f12aa2ceb24ee60 a693fe103b7177f431889a2116a5b48cd3f59a1663667bdc6bd62920be14357e 7b9c6745870b51dbf676ddc45b91ab5b241768a614c74689e96af73a4836f136 b4a93ba9ec9dad5f5a8eb01d58ddcbb3ebc60182ed040272ae295a1ce0a53b50 088ec7b0c8c7b697a2236dbb3966bd9f03c47f63a608e2455862f30bf712635f 41eeced2b87d5e4a4b46326c14e0890a24fc17e99d82f16fd5b5976c3ab66598 10b854d66240d9ee1ce4296d2f7857d2b1c6f062ca836d13d777930d678b3ca6 55047d88678f22d87a5fcec2a27d043d028102f49362c2ca6598b2fc056d8c80
DarkWatchMan RAT	MD5	2edf05f2130d4e12599dc44ff8bfc892 1706c64156d873ebbd0c6ecac95fec39 9afc15393e8bae03ad306ae1c50645e3 ca820517f8fd74d21944d846df6b7c20
	SHA1	1f87eeb37156d64de97d042b9bcfbaf185f8737d 149ce68540a068cdd204df796f6bff7d70f16473 be450cd1fab1b708ac1de209224e0d7f7adc0fae

Attack Name	TYPE	VALUE
DarkWatchMan RAT	SHA1	bb91d5234f37905f4830061331beab99e51206e7
	SHA256	4e38b7519bf7b482f10e36fb3e000cc2fcbf058730f6b9598a6a7ba5543766d4 d439a3ce7353ef96cf3556abba1e5da77eac21fdba09d6a4aad42d1fc88c1e3c 706eebdf4de19d17f9a753984f7b4cff7f5487c74d7862d21684e754967d8dd4 1b5eb6d4680f7d4da7e2a1a1060b9f13565e082346e375a92244bb55672d49d7
DownEx	Domain	net-certificate[.]services
	IPV4	139.99.126[.]38 84.32.188[.]123 206.166.251[.]216
	MD5	1e46ef362b39663ce8d1e14c49899f0e bb7cf346c7db1c518b1a63c83e30c602 a45106470f946ea6798f7d42878cff51 3ac42f25df0b600d6fc9eac73f011261 14a8aad94b915831fc1d3a8e7e00a5df 457eca2f6d11dd04ccce7308c1c327b7 d310a9f28893857a0dc1f7c9b624d353 d20e4fffbac3f46340b61ab8f7d578b1 5602da1f5b034c9d2d6105cdc471852b 89f15568bc19cc38caa8fd7efca977af ae5d4b9c1038f6840b563c868692f2aa c273cdfcfd808efa49ec0ed4f1c976e0 d11fcd39a30a23176337847e54d7268c 70e4305af8b00d04d95fba1f9ade222d 1492b0079b04eb850279114b4361f10c
CACTUS Ransomware	IPV4	163[.]123[.]142[.]213
	MD5	d9f15227fefb98ba69d98542fbe7e568 3adc612b769a2b1d08b50b1fb5783bcf be7b13aee7b510b052d023dd936dc32f 26f3a62d205004fbc9c76330c1c71536 d5e5980feb1906d85fbd2a5f2165baf7 78aea93137be5f10e9281dd578a3ba73
BPFDoor	SHA256	afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7
	Mutex	/var/run/initd[.]lock
Greatness	URLs	hxxps[:]//bluecheckcommunication[.]com/finale/host8/admin/js/mj[.]php

Attack Name	TYPE	VALUE
Greatness	URLs	hxxps[:]//thesslcgroup[.]org/host10/admin/js/mj[.]php hxxps[:]//cliffordandblu[.]com/wp-includes/SimplePie/Parse/pate/procs/admin/js/mj[.]php hxxps[:]//avenzzi[.]com/ayoo/host7/admin/js/mj[.]php hxxps[:]//at[.]benconcept[.]com/wp-content/plugins/TOPXOH/offe/host6/admin/js/mj[.]php hxxps[:]//cp3955[.]com/host8/admin/js/mj[.]php hxxps[:]//schneidera[.]ga/[.]well-known/off/host8/admin/js/mj[.]php hxxp[:]//bbqpro[.]za[.]com/fb/host7/admin/js/mj[.]php hxxps[:]//www[.]c2tec[.]com[.]br/today/host16/admin/js/mj[.]php hxxps[:]//cedarcreeklabradoodles[.]com/host6/admin/js/mj[.]php hxxps[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//hihin[.]net/wp-content/plugins/backwpup/k/host7/admin/js/mj[.]php hxxps[:]//hansarobotics[.]com/host7/admin/js/mj[.]php hxxp[:]//cloudnewsdaily[.]sa[.]com/img/host8/admin/js/mj[.]php hxxps[:]//pog[.]flylineaeru[.]com/html/admin/js/mj[.]php hxxp[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//manimot[.]ca/wp-includes/dump/host8/admin/js/mj[.]php hxxps[:]//ochrelandscapes[.]com[.]au/host9/admin/js/mj[.]php hxxps[:]//fanningcpaz[.]com/jumpjumping/host15/admin/js/mj[.]php hxxp[:]//mail[.]sorderatoluca[.]com/wp-content/host7/admin/js/mj[.]php
	SHA256	c5b29072d28e35c3992015fcbedc29540dd5ffc2931257a71866affae9de31f4 d07a2aa49f7b41eac954cd917aeedad3309d2856f63d51410da10dd5ff5847ce bbf7f77c3aca82b1531ba295cb5edb700777325dec9533d0c0341b66ddd073e3 d587c80ba12878146cfcb62262608c4a09f8b4d8647f9819ee3a5a94874b0205 492a45dd47acb19c6995acdbfce22a0cbcc135bc0263fd3efab165b1b75c9f68 61c094210d25d2e501234cc45b399b556d9bc95bc18f81c9ef4f433cc96b431a 9937f4ab00c4d41c8986a4d4e5a2a4193412e031c5a33d5f88913cc8dd0b5d4f

Attack Name	TYPE	VALUE
Greatness	SHA256	c9375f405c6409087cfabb34bdc8e9d1333f8b1f6448395a3889856a07ba3573 8619111ae4e427ce31eea0dd4e3b1ec5fa728438b64fdbff3351256cc52d5831 ca130ace64ce6277b612c0e507a5b8e37e54b4f635b18d896992a844ca99de72 2b4ca60d215bd7eaf13891878ef4ddeac36354343cdc59f9f2882f8eb61b7234 3216d8ad022b72512c65756c4272e897d8669faa8f3fbf8c4788fd41d67477f1 Ed4cd5308bf283928dfe5e3a0985e90c82014136a87fdac13670e0748482b5ed 02212ba142819acd27377cf8fa627e230ad44f0ff9f4a31a9a1fc7d17b74c88b 11d980af0e1f9576b2b2fa319ee58a49ee72f4722e96141ce5990b37248cad42 8567f25398c14ca530a110909e08a383df0ff94c4562f3105b59c1b84fdbf808 cccfdf7ba2c5f740a0ddfee6d273cf286d48765334e8e66ca1d8834fb4426af7 f20aea297c4c00e78e8059572c535b4c879b5c331f552c881ff7929d6df0f6a6 fcee0c8773ecc95b846e4b45dd1364d42796387d831f7203e50e116d1ed5a750 b34b9aa0b8a36deec3157f262c5be11fa705da4c4902dc50ce6f0df2b838471c cae49fe3b224160c790fec72309f1bdb8f0e1d7c8a82a49262b12707b1789ce0
Babuk Ransomware	URL	hxxp[://]hkpomcx622gnqp2qhenv4ceyrhwvld3zwogr4mnkdudq2txf55keoad[.]onion
	SHA256	3ab167a82c817cbcc4707a18fcb86610090b8a76fe184ee1e8073db152ecd45e
CopperStealth	SHA256	8a21eae144a23fffd35f8714964ff316caaa37fe464e8bbc143f4485119b5575 293a2adf60a94437cc0f92545b7caabdaed0a63007b51e2b3d449cdb1e00f5a8 ad5f59c497f423a07cfb4affc82aac408eafeeefef22f8ba25cabff2ff991754 636772857bd9b88d5b530586c7008f48e61ec429fb50a82019d0505dcf994930 7246dbf235f66034bd7042408f01b8670c3f45d39082fcbf5b893d7952614833 73fd83a9eb267fed5a3178b75a9bff0bac9e0864daed830fddf6a8686c286cbb

Attack Name	TYPE	VALUE
CopperStealth	SHA256	7fd6cb3e1648dd9d1994c65762826772ae32dc58fbc7ac51179a0b3526f1395f e3f31eabaa0b3bebe0c5152fc6097a8fbf1c6fd9e57d06fe8e9bd8860e8f07a6 033ba1740ba105bf4a5081f438f46f1d7ad17a175aab132bd844edcf8e30949f ed88b019b3a8346c89aaf6ba7ce6c6be0b9a88c121312f3db9b6ebd776a9af5a ecdd5adb40297ec29c0e8a8f50223069db3d32c2a1d223adfb52c3a695d41fa2 f916f4d1d8c1df0d31b8d18b7c94109b4303412880538f64ec3eb2e257732ead 53f4306d30b4f7b731c0cd7be6df39f02613fb4c0e9b5aa85f754e145dca080c 139f8412a7c6fdc43dcfbbcdba256ee55654eb36a40f338249d5162a1f69b988 5b932eab6c67f62f097a3249477ac46d80ddccdc52654f867406 0b4ddf638e5d 6994b32e3f3357f4a1d0abe81e8b62dd54e36b17816f2f1a80018584200a1b77 32882949ea084434a376451ff8364243a50485a3b4af2f2240bb5f20c164543d 50819a1add4c81c0d53203592d6803f022443440935ff8260ff3b6d5253c0c76 770f33259d6fb10f4a32d8a57d0d12953e8455c72bb7b60cb39ce505c507013a 86047bb1969d1db455493955fd450d18c62a3f36294d0a6c3732c88dfbcc4f62 bb2422e96ea993007f25c71d55b2eddfa1e940c89e895abb50dd07d7c17ca1df 06c5ebd0371342d18bc81a96f5e5ce28de64101e3c2fd0161d0b54d8368d2f1f 6661320f779337b95bbbe1943ee64afb2101c92f92f3d1571c1bf4201c38c724 f9f2091fccb289bcf6a945f6b38676ec71dedb32f3674262928ccaf840ca131a E6f764c3b5580cd1675cbf184938ad5a201a8c096607857869bd7c3399df0d12 e1cb86386757b947b39086cc8639da988f6e8018ca9995dd669bdc03c8d39d7d 4734a0a5d88f44a4939b8d812364cab6ca5f611b9b8ceebe27df6c1ed3a6d8a4 ea50f22daade04d3ca06dedb497b905215cba31aae7b4cab4b533fda0c5be620 fa9abb3e7e06f857be191a1e049dd37642ec41fb2520c105df2227fcac3de5d5

Attack Name	TYPE	VALUE
CopperStealth	SHA256	f936ec4c8164cbd31add659b61c16cb3a717eac90e74d89c47afb96b60120280 a292fd3792ef81f3a3afd73c5b19878677e0293528e646e244ef50a36c4a0fb2 8b141803aeaa4f696fb19711d45a2628c73476c893ac1ba7967eb8d84862ea9a ac4bcb31d35428d8147d413d3354b9fdf70d9e9f3463ead04783805fdd306d86 04d2cb7d5f0e28797c1fde9036f06535040c223ecd66828e21c55971241adbbf bf5ae3846ada31fdf91f7d9c03c54dd10598571a5a24ed96c582a6a6fe20006f e257b8efdb3719bf21ed15d5abb30b0cbdbf9027a3db17ad0baca319eec13889 49337a65b01dd6e634456bca17ca28118a8126e4706d92b4673afe1c9cfea638 4934e4990928dbec77463f383b693f4f4a9fc40256e72a36e98c292722b84cf1 5558eaebeeeb4c5c731b531305e7c97c9cf1b1449b0466f46430aa0549c256e9 6c3995155e0e5cbb17e6f71b8d8b89d4dfc77849e869da7901a79053e8e8232b
	URLs	hxxp[:]//cnzz.fnxitong.com[:]99/gg.html hxxp[:]//chromei.org/tj/ hxxp[:]//so.fnxitong.com[:]99/tongji.php?u=e002 hxxp[:]//so.fnxitong.com[:]99/tongji.php?u=001 hxxp[:]//cnzz.fnxitong.com[:]99/gg.txt hxxp[:]//chromei.org/encode.txt hxxp[:]//up.chromei.org/e002.txt hxxp[:]//www.chromel.cn/encode.txt
CopperPhish	URLs	hxxps[:]//0zpt4.za.com/ hxxps[:]//3hdr0.za.com/
	SHA256	48211c6f957c2ad024441be3fc32aecd7c317dfc92523b0a675c0cfec86ffdd9 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 28d1d1c6fb23ef5f92b16e2701c49bb34b4a81af11f95ff5674d291c5ffb3b28 07cccf04854a58e43a5043e240b662f84ac512b2d2432b1b7e4cd5465d1dde33 bff741d972e1dac7fa1197ac9365106b49bd07cea868d69c660aa569fe75f005 036a689038dfaa195c899d57a4d3fdcf5f99b91bdbf9739a4d05f9bd1dcfe15e

Attack Name	TYPE	VALUE
CopperPhish	SHA256	65a632de69bcb62c8f344a9cc0951d3c599301ca6d8aed66bbdab9f1b977799a 971259ae3eb7dc843c6872b22154e5cf74e48ca35fb895145df63fa50e8e8792 58eb8b6fd34406316438e2e17ed3c44b6c26695b28c71db7b062a63a116ee33b 0a596289cb9c6dcb065d96fb33c1e9509f62ff42b00a0d679bb8b9e64dce8ea5 fcf49a50a3b86adeea6b1cfbb0d86dfed774673a5900570878197f822f6f2126 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 6f52f36d84ea04d00f307d5aafedcda98118d140c1ac1af0525ecb374c0f5cf2 688de5bbd2cb1e5556304002c1b7f5fdfe147251217f93b8733017161a834fa5 1a1a70fd2c5a012c4e8547713a3abf1dc2dbd05a81ab1fcca4ab1ad71ad36979 15430150c081728440618aac046cc1d50a4391b55fa7f8fa66325d9b462e57c3 acac571f03810d6e8408d4df25fda741cf492c7d842113155034da1f871c10ea f340e0ef5f90024b9626a83c2c1eed2011417372073088169d7c2c7ec842f228 699873a949ca1e3a15f8428d1e28e3bdf7b95ec1606e10785f3f51b118e2669e dda6bc4618cd6f723d6ad5f45f171a075c208b5b2693a35f24dd6607a3f167f0 7e3f5a8f6fc490736ba7e04389cf83d9ea47a5079e63901300e2dec79c1f77ab 1fd3c8d5ec7043fb01ea9d9985075d0b014f7153e88cd56d267fb10f1f979a1c 50fae4fe4a258854c629a3dd24262e1a35a09d317f2d1b7bb31d5a81a237c258 a5f00b52c99b951009334c6c52524c4e494c8ee77da1340a623a35a35e96b935 00ff5f2af303cee7ede802b8a013f415bc69caa023330143df746b9b23aa60fd Dd3ffec50a0ef7434b85f85330cebb9a2afa2123bed19ac39179806bacf48775
Rancoz	MD5	8d9f3e223f8d5e350b87dc0908fee0a5
	SHA1	9fe3060e5cbe3a9ab6c3fb3dee40bd6cd385a6f6
	SHA256	b95a4443bb8bff80d927ac551a9a5a5cfac3e3e03a5b5737c0e05c75f33ad61e

Attack Name	TYPE	VALUE
Tsunami & XMRIG cryptominer	URLs	http[:]//79[.]137[.]203[.]156/Ebvjmba.dat http[:]//185[.]17[.]0[.]19/bypass.ps1 http[:]//185[.]17[.]0[.]19/Nmfwg.png
	IPV4	185[.]17[.]0[.]19 194[.]38[.]23[.]170 201[.]71[.]165[.]153 179[.]43[.]155[.]202
	Domains	Work[.]letmaker[.]top su-94[.]letmaker[.]top
Xworm	SHA256	3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16
Minas	MD5	08da41489b4b68565dc77bb9acb1ecb4 06fe9ab0b17f659486e3c3ace43f0e3a f38a1b6b132afa55ab48b4b7a8986181 63e0cd6475214c697c5fc115d40327b4
CryptNet	SHA256	2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775 1cc7283ee218081f2f056bd2ec70514e86b8dcb921342dc9aed69e7480dec18e
MichaelKors Ransomware	SHA256	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5 cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849 a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808 7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6 3339ba53e1f05f91dbe907d187489dbaba6c801f7af6fd06521f3ba8c484ec6c
	SHA1	c7fcbaedf6b077b3d9bfc4720c3860a5d848bcb4 c7b28fe059e944f883058450d5c77b03076b0ea1 b033a146de147d97db6f8dadbe2141df2f0192be 91ad089f5259845141dfb10145271553aa711a2b 228239d1bf7020ecdc4021f3c20a14041b210d78 0f5457b123e60636623f585cc2bf2729f13a95d6
	MD5	c159afb7d2111690326cad610776db34 b0fd45162c2219e14bdccab76f33946e aa1ddf0c8312349be614ff43e80a262f 99549bcea63af5f81b01decf427519af 546af2069c28f794dc918958a80ac17b 40c9dc2897b6b348da88b23deb0d3952

Attack Name	TYPE	VALUE
BlackCat	SHA256	52d5c35325ce701516f8b04380c9fbdb78ec6bcc13b444f758fdb03d545b0677 c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497
	MD5	909f3fc221acbe999483c87d9ead024a a837302307dace2a00d07202b661bce2
	SHA1	17bd8fda268cbb009508c014b7c0ff9d8284f850 78cd4dfb251b21b53592322570cc32c6678aa468 c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91 91568d7a82cc7677f6b13f11bea5c40cf12d281b 0bec69c1b22603e9a385495fbe94700ac36b28e5 5ed22c0033aed380aa154e672e8db3a2d4c195c4 cb25a5125fb353496b59b910263209f273f3552d 994e3f5dd082f5d82f9cc84108a60d359910ba79 f6793243ad20359d8be40d3accac168a15a327fb b2f955b3e6107f831ebe67997f8586d4fe9f3e98
Donut	SHA256	f6c316e2385f2694d47e936boac4bc9b55e279d530dd5e805f0d963cb47c3c0d 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330 aae9c8bd9db4e0d48e35d9ab3b1a8c7933284dcbeb344809fed18349a9ec7407 27a6c3f5c50c8813ca34ab3b0791c08817c803877665774954890884842973ed 1485cOed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1cOOc780419a4e
JackalControl	MD5	5ed498f9ad6e74442b9b6fe289d9feb3 a5ad15a9115a60f15b7796bc717a471d c6e5c8bd7c066008178bc1fb19437763 4f041937da7748ebf6d0bbc44f1373c9 eab4f3a69b2d30b16df3d780d689794c 8c1070f188ae87fba1148a3d791f2523
	URLs	hxxp://abert-online[.]de/meeting/plugins[.]php hxxp://acehigh[.]host/robotx[.]php hxxp://assistance[.]uz/admin/plugins[.]php hxxp://cnom[.]sante[.]gov[.]ml/components/com_avreloaded/views/popup/tmpl/header[.]php hxxp://info[.]merysof[.]am/plugins/search/content/plugins[.]php

Attack Name	TYPE	VALUE
JackalControl	URLs	hxxp://invest[.]zyrardow[.]pl/admin/model/setting/plugins[.]php hxxp://weblines[.]gr/gallery/gallery_input[.]php hxxp://www[.]wetter-bild[.]de/plugins[.]php hxxps://ajapnyakmc[.]com/wp-content/cache/index[.]php hxxps://asusiran[.]com/wp-content/plugins/persian-woocommerce/include/class-cache[.]php hxxps://asusiran[.]com/wp-content/themes/woodmart/inc/modules/cache[.]php hxxps://croma[.]vn/wp-content/themes/croma/template-parts/footer[.]php hxxps://den-photomaster[.]kz/wp-track[.]php hxxps://eyetelligence[.]ai/wp-content/themes/cms/inc/template-parts/footer[.]php hxxps://finasteridehair[.]com/wp-includes/class-wp-network-statistics[.]php hxxps://gradaran[.]be/wp-content/themes/tb-sound/inc/footer[.]php hxxps://mehrganhospital[.]com/wp-includes/class-wp-tax-system[.]php hxxps://meukowcognac[.]com/wp-content/themes/astra/page-flags[.]php hxxps://nassiraq[.]iq/wp-includes/class-wp-header-styles[.]php hxxps://new[.]jmcashback[.]com/wp-track[.]php hxxps://news[.]lmond[.]com/wp-content/themes/newsbook/inc/footer[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/cache/functions[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/themes/dt-the7/inc/cache[.]php hxxps://pabalochistan[.]gov[.]pk/new/wp-content/themes/twentyfifteen/content-manager[.]php hxxps://sbj-i[.]com/wp-content/plugins/wp-persian/includes/class-wp-cache[.]php hxxps://sbj-i[.]com/wp-content/themes/hamyarwp-spacious/cache[.]php hxxps://sokerpower[.]com/wp-includes/class-wp-header-styles[.]php hxxps://technocometsolutions[.]com/wp-content/themes/seofy/templates-sample[.]php hxxps://www[.]djstuff[.]fr/wp-content/themes/twentyfourteen/inc/footer[.]php hxxps://www[.]perlesoie[.]com/wp-content/plugins/contact-form-7/includes/cache[.]php hxxps://www[.]perlesoie[.]com/wp-content/themes/flatsome/inc/classes/class-flatsome-cache[.]php

Attack Name	TYPE	VALUE
JackalSteal	URLs	hxxps://tahaherbal[.]ir/wp-includes/class-wp-http-iwr-client.php hxxps://winoptimum[.]com/wp-includes/customize/class-wp-customize-sidebar-refresh.php
	MD5	c05999b9390a3d8f4086f6074a592bc2
JackalPerInfo	MD5	a491aefb659d2952002ef20ae98d7465
JackalScreenWatcher	MD5	1072bfeee89e369a9355819ffa39ad20
JackalWorm	MD5	5de309466b2163958c2e12c7b02d8384
Pikabot	SHA256	92153e88db63016334625514802d0d1019363989d7b3f6863947ce0e490c1006 a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821 8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365 a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc 347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944
	URLs	hxxps://129.153[.]135.83:2078 hxxps://132.148.79[.]222:2222 hxxps://45.154.24[.]57:2078 hxxps://45.85.235[.]39:2078 hxxps://94.199.173[.]6:2222
PowerExchange	MD5	f18575065970ef36e613ffa046f381fe9b01b3e9 2ba23d9115fb1c1d4c5899d34dc4772631d77eda 2b995ce4656db7257451080111705d5b98b45df3 68299DF5D8CE52845A8FC10598F138840094181C d82aad3222664ec9fb112808dfabbb56de9aa770 70aaa46784a2abd8af5628cb94f876d57fe8d154 fd3750d809f6ff9cf2b49d7a63f8f3fa0a457f61
	URL	hxxps://enmckkb0t0v3[.]x[.]pipedream[.]net?n=my
	File Names	Brochure[.]zip Brochure[.]exe MicrosoftEdgeUpdateService
	File Paths	C:\Users\Public\MicrosoftEdge\autosave[.]exe C:\Users\Public\MicrosoftEdge\wsdl[.]ps1 C:\Users\Public\MicrosoftEdge\Microsoft[.]Exchange[.]WebServices[.]dll C:\Users\Public\MicrosoftEdge\config[.]conf

Attack Name	TYPE	VALUE
PowerExchange	File Paths	C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Handler\v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]Handler[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Roles\v4[.]0_1[.]0[.]0[.]0_9cbc39238c01012f\System[.]Web[.]Roles[.]dll C:\Users\Public\System[.]Web[.]Handler[.]dll C:\Windows\temp\temp[.]ps1 C:\Users\Public\temp[.]ps1 C:\Windows\System32\System[.]Web[.]TransportClient[.]dll C:\Windows\System32\inetsrv\System[.]Web[.]TransportClient[.]dll C:\Windows\Mirosoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]TransportClient\v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]TransportClient[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]ServiceAuthentication\v4[.]0_1[.]0[.]0[.]0__ff08ceb7abd6adf3\System[.]Web[.]ServiceAuthentication[.]dll
Buhti Ransomware	IPV4	91.215.85[.]183 81.161.229[.]120
	SHA256	063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6 d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65 8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441 898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a 515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855 4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880 22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe 18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef

Attack Name	TYPE	VALUE
Buhti Ransomware	SHA256	01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4 7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c 287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52 32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c 5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72 d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72 65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b 8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334 8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2 97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351 9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf 9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937 Bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24
GobRAT	URLs	https[:]//su.vealcat[.]com http[:]//su.vealcat[.]com:58888 https[:]//ktlvz.dnsfailover[.]net http[:]//ktlvz.dnsfailover[.]net:58888
	Domains	su.vealcat[.]com ktlvz.dnsfailover[.]net wpksi.mefound[.]com
	SHA256	060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a

Attack Name	TYPE	VALUE
GobRAT	SHA256	3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1 60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3 a8b914df166fd0c94106f004e8ca0ca80a36c6f2623f87a4e9afe7d86b5b2e3a aeed77896de38802b85a19bfcb8f2a1d567538ddc1b045bcdb29cb9e05919b60 6748c22d76b8803e2deb3dad1e1fa7a8d8ff1e968eb340311fd82ea5d7277019 e133e05d6941ef1c2e3281f1abb837c3e152fdeaffefde84ffe25338fe02c56d 43dc911a2e396791dc5a0f8996ae77ac527add02118adf66ac5c56291269527e af0292e4de92032ede613dc69373de7f5a182d9cbba1ed49f589ef484ad1ee3e 2c1566a2e03c63b67fbdd80b4a67535e9ed969ea3e3013f0ba503cfa58e287e3 98c05ae70e69e3585fc026e67b356421f0b3d6ab45b45e8cc5eb35f16fef130c 300a92a67940cfafeed1cf1c0af25f4869598ae58e615ecc559434111ab717cd a363dea1efda1991d6c10cc637e3ab7d8e4af4bd2d3938036f03633a2cb20e88 0c280f0b7c16c0d299e306d2c97b0bff3015352d2b3299cf485de189782a4e25 f962b594a847f47473488a2b860094da45190738f2825d82afc308b2a250b5fb 4ceb27da700807be6aa3221022ef59ce6e9f1cda52838ae716746c1bbdee7c3d 3e1a03f1dd10c3e050b5f455f37e946c214762ed9516996418d34a246daed521 3bee59d74c24ef33351dc31ba697b99d41c8898685d143cd48bccdff707547c0 c71ff7514c8b7c448a8c1982308aaffed94f435a65c9fdc8f0249a13095f665e
BianLian ransomware	SHA256	076e59781d0759de35022291c3d63bbf4227bd79561d80f52c9073a6278c5077 0772fb1102685def711ffe647080e1a9b6597fe60e8f1afe7b457ac97c6ac25e 16cbfd155fb44c6fd0f9375376f62a90ac09f8b7689c1afb5b9b4d3e76e28bdf 183b28fb93db1c907b32aa9fa2f83c7b0ebcc6724de85707a89e5d03c5be5d12 1cba58f73221b5bb7930bfeab0106ae5415e70f49a595727022dcf6fda1126e9

Attack Name	TYPE	VALUE
BianLian ransomware	SHA256	207078c70be916bb7d2ad4d206d2dca37406f84313f88699fa57fa9745a055bb 228ef7e0a080de70652e3e0d1eab44f92f6280494c6ba98455111053701d3759 38d6ec5f93f6722c3573989f1463fb1cba1c01c3a1a0579f329e0d625c57070b 42b0606aa2c765c0b0789b47ebd3a3f43144dc0c20b2ff6db648ac5feb0a37a3 45f76c5c5126501018f907f886dd23a56dd882ee7d4f41c41d732612b2e4da88 46fa9a69989b79b56495a1ece8a45d6d5ae43c600b8a13ef88f3eb9d84efda02 487f0d748a13570a46b20b6687eb7b7fc70a1a55e676fb5ff2599096a1ca888c 4ca84be5b6ab91694a0f81350cefe8379efcad692872a383671ce4209295edc7 53095e2ad802072e97dbb8a7ccea03a36d1536fce921c80a7a2f160c83366999 55016f61b9880be414cc4e1280d6bb620cfbe5e1e8e12e305a304d3dff7e209c 597c492a5af56d935d360fcfd2c1e89928dde492c86975f2c5cc33ec90b042ce 60b1394f3afee27701e2008f46d766ef466caa7711c45ddfd443a71efc39a407 61dfe2ccdc7cee55cf0530064499a52bf93bc6c3d8996ed013fcc5692e94c73a 667821f5996855bf83507fb1009f5d8d36c1258aa3c776106d453200f3bb0ed3 77617775dc6fa8b893607d52c3282ece1912bcdd0b583b418399af2eade249b8 7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893 93953eef3fe8405d563560dc332135bfe5874ddeb373d714862f72ee62bef518 93fb7f0c2cf10fb5885e03c737ee8508816c1102e9e3d358160b78e91fa1ebdb 96e02ea8b1c508f1ee3c1535547f9b89396f557011e61478644ae5876cdaaca5 a8e999a7a77d3b9846250a34ebda7d80ea83a79b3714b1f7ac8f92bc52a895fd a92dd4885af317d36cd62dac31d0d5c93febd367e8f4412e7593fb48c9f34256 ac1d42360c45e0e908d07e784ceb15faf8987e4ba1744d56313de6524d2687f7 adefaad2a9c449d0e9fabb5035422a6ce31d0f26b0109a7c2911f570a6c74144

Attack Name	TYPE	VALUE
BianLian ransomware	SHA256	afb7f11da27439a2e223e6b651f96eb16a7e35b34918e501886d25439015bf78 b4249f2effb8dd651458c831d38155346c1e2d30b191bf37197ffa5164d25f7c ba3c4bc99b67038b42b75a206d7ef04f6d8abaf87a76c373d4dec85e73859ce2 c62371f129d19707870c0f9a89b0f8a65970aed02537e358e532e4416bc8678e dcc7115496faa0797c32bb6d5d823821f19f5177e09e05dbe0151a6b9e1edfb7 dd03ea7ba369fc9df641c09f29e4abcb8378b5a8dadd3d7c14d47449525f1716 E136d635de39d23cef600cc53efd671f1e8aba7d982bde152b21ea1f7c04703e 1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43 ea5c88fe464562227f483e8fc4eb2cf43e98a897aaaa3e94de4d236d5dc6e7e7 f3a4fb09a0498e7ab3b33338ca6bc03460e43d437d9f3afbfc1a521c1029ff19 f3f3c692f728b9c8fd2e1c090b60223ac6c6e88bf186c98ed9842408b78b9f3c f6669de3baa1bca649afa55a14e30279026e59a033522877b70b74bfc000e276 f84edc07b23423f2c2cad47c0600133cab3cf2bd6072ad45649d6faf3b70ec30 117a057829cd9abb5fba20d3ab479fc92ed64c647fdc1b7cd4e0f44609d770ea 3a2f6e614ff030804aa18cb03fcc3bc357f6226786efb4a734cbe2a3a1984b6f 46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b 7f91e10c39e0a77c83af3ef48061cbb73194c793f9c3c8bc7fa1aa0fc75eb385 F77433e517f493ca54e6a4603e51739053ebfac03d2764ad9d1f7e00cfadefa0 e7e097723d00f58eab785baf30365c1495e99aa6ead6fe1b86109558838d294e 0c1eb11de3a533689267ba075e49d93d55308525c04d6aff0d2c54d1f52f5500 40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce
	IPV4	5.230.73[.]234 5.230.73[.]37 51.222.96[.]1 52.87.206[.]242

Attack Name	TYPE	VALUE
BianLian ransomware	IPV4	54.227.224[.]229 66.85.147[.]22 72.11.134[.]215 81.17.28[.]71 85.239.52[.]96 85.239.53[.]168 96.44.135[.]76 96.44.156[.]206 96.44.157[.]203 104.223.0[.]85 104.234.118[.]129 104.238.35[.]26 155.94.160[.]243 173.232.2[.]41 185.99.133[.]112 192.161.48[.]51 204.152.203[.]94 208.123.119[.]100 35.157.43[.]44 45.86.163[.]228 52.53.186[.]224 54.144.145[.]126 66.85.156[.]83 102.129.214[.]35 103.199.17[.]27 103.20.235[.]122 103.20.235[.]188 104.200.67[.]156 104.200.67[.]244 104.200.67[.]31
Bl00dy Ransomware	Tox ID	E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F
	URL	hxxp[://]192.184.35[.]216:443/4591187629[.]exe
	IPV4	102.130.112[.]157 172.106.112[.]46 176.97.76[.]163 192.160.102[.]164 194.87.82[.]7 195.123.246[.]20 198.50.191[.]95 206.197.244[.]75 216.122.175[.]114 46.4.20[.]30 5.188.206[.]14

Attack Name	TYPE	VALUE
Bl00dy Ransomware	IPV4	5.8.18[.]233 5.8.18[.]240 80.94.95[.]103 89.105.216[.]106 92.118.36[.]199
Clop Ransomware	SHA256	c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c 0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3 c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d
LockBit Ransomware	SHA1	2d15286d25f0e0938823dcd742bc928e78199b3d 864f56b25a34e9532a1175d469715d2f61c56f7f ef958f3cf201f9323ceae9663d86464021f8e10d
TrueBot	SHA1	b918f97c7c6ebc9594de3c8f2d9d75ecc292d02b
	Email addresses	decrypt.support@privyonline[.]com fimaribahundqf@gmx[.]com main-office@data-highstream[.]com prepalkeinuc0u@gmx[.]com tpyrcne@onionmail[.]org
	Domain	windowservicecemter[.]com
	SHA256	c0f8aeeb2d11c6e751ee87c40ee609aceb1c1036706a5af0d3d78738b6cc4125
Cobalt Strike Beacons	SHA256	0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f
	Domain	study.abroad[.]ge
	IPV4	5.8.18[.]233 5.8.18[.]240
Merdoor backdoor	SHA256	13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead 8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38 89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744 5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075

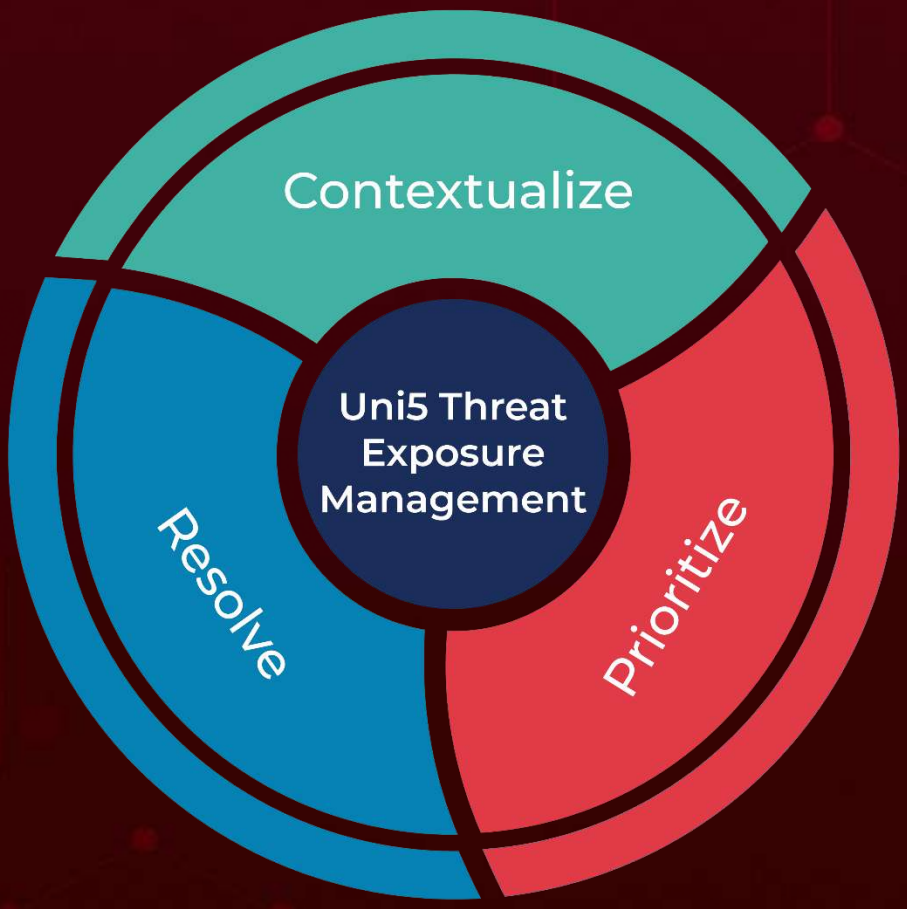
Attack Name	TYPE	VALUE
Merdoor backdoor	SHA256	ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740 14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3 db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03 e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2 dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6 fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949 fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104 341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200 f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4 750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3 9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774 a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0 d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7 f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57 139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4 11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5 0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75 eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b 1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fc1a109b9ae092a5d7492b7dd fae713e25b667f1c42ebbea239f7b1e13ba5dc99b225251a82e65608b3710be7
ZXShell rootkit	SHA256	1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e

Attack Name	TYPE	VALUE
ZXShell rootkit	SHA256	a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221 592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae 929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798 009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4 ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8 ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28 32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849

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

June 02, 2023 . 05:37 AM

More at www.hivepro.com