Date of Publication
May 3, 2023

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

APRIL 2023

Table Of Contents

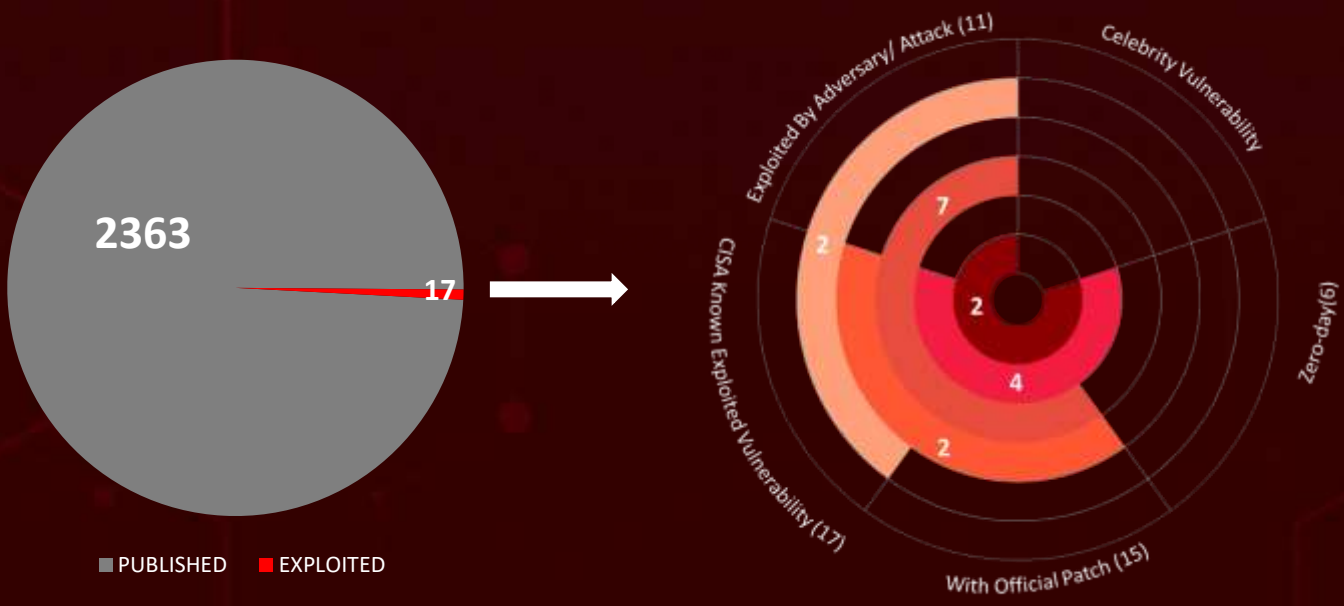
Summary

In **April**, the discovery of **six zero-day** vulnerabilities drew significant attention from the cybersecurity community. **One** of these vulnerabilities was exploited by **Rorschach Ransomware group**, leading to a heightened sense of urgency among security teams to patch their systems.

The month of April saw a rise in **ransomware** attacks, with various strains such as **Rorschach**, **Money message**, **Blackcat**, **Trigona**, **Cylance**, **Nokoyawa**, and **LockBit** 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.

Attackers are leveraging two vulnerabilities (**CVE-2023-27350** and **CVE-2023-27351**)in PaperCut MF/NG software to install Atera remote management software. In addition to ransomware attacks, several malware families were observed targeting victims worldwide. These include **Jaguar Tooth**, **BellaCiao**, **QBot**, **MgBot**, **Domino Backdoor**, **and** **Carbanak Backdoor**. These malware families are designed to steal sensitive data, disrupt systems, and evade detection by security tools.

Finally, the **CVE-2023-2033** vulnerability is a high-severity zero-day vulnerability that was exploited in attacks, making it the first zero-day chrome vulnerability to be exploited since the start of the year 2023.



Insights

QBot

A new wave identified utilizing malicious PDF attachments in emails written in various languages.

APT 36

Targeting educational institutions in India using Crimson RAT

Zaraza bot

New credential-stealing malware uses Telegram as its C&C

0-Day

Google Chrome fixes the first 2023 zero-day

Government, Energy, Financial, Tele Communication, Healthcare, and **Education** were the most targeted sectors

97

number of vulnerabilities were patched during Microsoft Patch Tuesday

Rorschach

aka BabLock Ransomware is the most active ransomware strain of the month

Bitter Group

Distributes CHM malware to Chinese institutions

Netherlands, United States, Norway, Ukraine, and **Belgium** were the most targeted countries

CrossLock Ransomware

New Go-based Ransomware Threat with Cross-Platform Capabilities and Double Extortion Techniques

Threat Landscape

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-20121	Cisco EPNM, Cisco ISE, and Cisco Prime Infrastructure Command Injection Vulnerability	Cisco EPNM, Cisco ISE, and Cisco Prime Infrastructure	✗	✗	✓
CVE-2023-20122	Cisco ISE Command Injection Vulnerability	Cisco Identity Services Engine (ISE)	✗	✗	✓
CVE-2021-35394	Realtek Jungle SDK Remote Code Execution Vulnerability	Realtek Jungle SDK	✗	✓	✓
CVE-2022-27926	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	✗	✓	✓
CVE-2022-41352	Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	Zimbra Collaboration (ZCS)	✗	✓	✓
CVE-2022-46169	Cacti Command Injection Vulnerability	Cacti	✗	✗	✓
CVE-2021-27876	Veritas Backup Exec Agent File Access Vulnerability	Veritas	✗	✗	✓
CVE-2021-27877	Veritas Backup Exec Agent Improper Authentication Vulnerability	Veritas	✗	✗	✓
CVE-2021-27878	Veritas Backup Exec Agent Command Execution Vulnerability	Veritas	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-28205	Apple WebKit Use-After-Free Vulnerability	Apple WebKit	✓	✓	✓
CVE-2023-28206	Apple macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability	Apple macOS	✓	✓	✓
CVE-2023-28252	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2013-3900	Microsoft WinVerifyTrust function Remote Code Execution	Microsoft WinVerifyTrust function	✓	✓	✓
CVE-2023-2033	Google Chrome Type Confusion Vulnerability	Google Chrome	✓	✓	✓
CVE-2017-6742	Cisco SNMP Remote Code Execution Vulnerability	Cisco SNMP	✗	✓	✓
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF/NG	✗	✓	✓
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine Multiple Products	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
AlienFox	Modular Toolkit	-	-	-	Compromise email and web hosting services
ShellBot (aka PerlBot, DDoS Perl IrcBot)	Botnets	CVE-2021-35394 CVE-2022-46169	Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2; cacti: before 1.1.19-2.20	✓	Exploiting Cacti and Realtek vulnerabilities
Moobot					
Rorschach/babLock	Ransomware	CVE-2022-41352	Zimbra Collaboration(ZCS)	✓	Malicious email attachment
Money Message	Ransomware	-	-	-	Unknown
BlackCat (aka ALPHV and Noberus) ransomware	Ransomware	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878	Veritas Backup Exec	✓	Internet-exposed Windows server, running Veritas Backup Exec version 21.0
Cylance	Ransomware	-	-	-	Unknown
Micropsia	Backdoor	-	-	-	Unknown
Arid Gopher	Infostealer	-	-	-	Unknown
Nokoyawa	Ransomware	CVE-2023-28252	Windows & Windows Server	✓	Through CVE-2023-28252

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
CHM	Dropper	-	-	-	Via Email attachments
Trigona	Ransomware	-	-	-	Improperly managed MS-SQL servers
Havoc Demon	Backdoor	-	-	-	Via Email attachments
Rilide	Stealer	-	-	-	By mimicking Google Drive extensions
Kadavro Vector Ransomware	Ransomware	-	-	-	Fake Tor Browser Installers
Crimson RAT	RAT	-	-	-	Phishing emails
Zaraza bot	Botnet	-	-	-	Unknown
Dave Loader	Loader	-	-	-	Phishing or Malvertising
Domino Backdoor	Backdoor	-	-	-	Dave Loader
NewWorldOrder Loader	Loader	-	-	-	Unknown
Carbanak Backdoor	Backdoor	-	-	-	NewWorldOrder Loader
Project Nemesis infostealer	Infostealer	-	-	-	Domino Loader
LockBit Ransomware	Ransomware	-	-	-	Ransomware affiliate program
QBot (also known as QakBot, QuackBot, and Pinkslipbot)	Trojan	-	-	-	Malicious PDF attachments in emails

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
CrossLock	Ransomware	-	-	-	Unknown
Jaguar Tooth	Unknown	CVE-2017-6742	Cisco IOS and IOS XE Software		SNMP vulnerability in Cisco IOS routers
EvilExtractor	Information Stealer	-	-	-	Phishing Email
MgBot	Framework	-	-	-	AnyDesk remote desktop software
BellaCiao	Dropper	CVE-2022-47966	Zoho ManageEngine		Unknown
PingPull	Backdoor	-	-	-	Unknown
VEILEDSIGNAL	Backdoor	-	-	-	trojanized X_Trader
RustBucket	Downloader	-	-	-	Via PDF Viewer App

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT43	Information theft and espionage	North Korea	-	-	-
Winter Vivern (aka TA473 and UAC-0114)	Information theft and espionage	Unknown	CVE-2022-27926	-	Zimbra Collaboratio: 9.0.0 P23
Rorschach Ransomware (aka BabLock)	Information theft and espionage	Unknown	CVE-2022-41352	Rorschach/ BabLock Ransomwa re	Zimbra Collaboration (ZCS)
Money Message Ransomware	Information theft and espionage	Unknown	-	Money Message Ransomwa re	-
UNC4466	Information theft and espionage	Pakistan	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878	BlackCat Ransomwa re	Veritas Backup Exec
Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)	Information theft and espionage	Gaza	-	Micropsia backdoor and Arid Gopher info-stealer	-
MERCURY (MuddyWater, Seedworm, TEMP.Zagros, Static Kitten, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Information theft and espionage	Iran	-	-	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
DEV-1084	Information theft and espionage	Unknown	-	-	-
Bitter APT(T-APT-17, APT-C-08, Orange Yali)	Information theft and espionage	South Asia	-	CHM	-
APT 36(Transparent Tribe, ProjectM, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH)	Information theft and espionage	Pakistan	-	Crimson RAT	-
FIN7(aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)	Financial crime	-	-	Dave Loader, Domino Backdoor, NewWorld Order Loader, Carbanak Backdoor, Project Nemesis infostealer	-
Wizard Spider(aka ITG23, Grim Spider, TEMP.MixMaster, Gold Blackburn, Gold Ulrick)	Financial crime	Russia	-	Dave Loader, Domino Backdoor, NewWorld Order Loader, Carbanak Backdoor, Project Nemesis infostealer	-
LockBit Gang	Financial gain	Unknown	-	LockBit Ransomware	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT28(Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium , Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12 , ITG05, TAG-0700, UAC-0028, Grey-Cloud)	Information theft and espionage	Russia	CVE-2017-6742	Jaguar Tooth	Cisco IOS and IOS XE Software
Tomiris	Information theft and espionage	Russia	-	-	-
Daggerfly(Bronze Highland, Evasive Panda)	Information theft and espionage	China		MgBot	-
Alloy Taurus (GALLIUM, Softcell, Phantom Panda)	Information theft and espionage	China	-	PingPull	-
Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)	Information theft and espionage	Iran	CVE-2022-47966	BellaCiao	Zoho ManageEngine Multiple Products

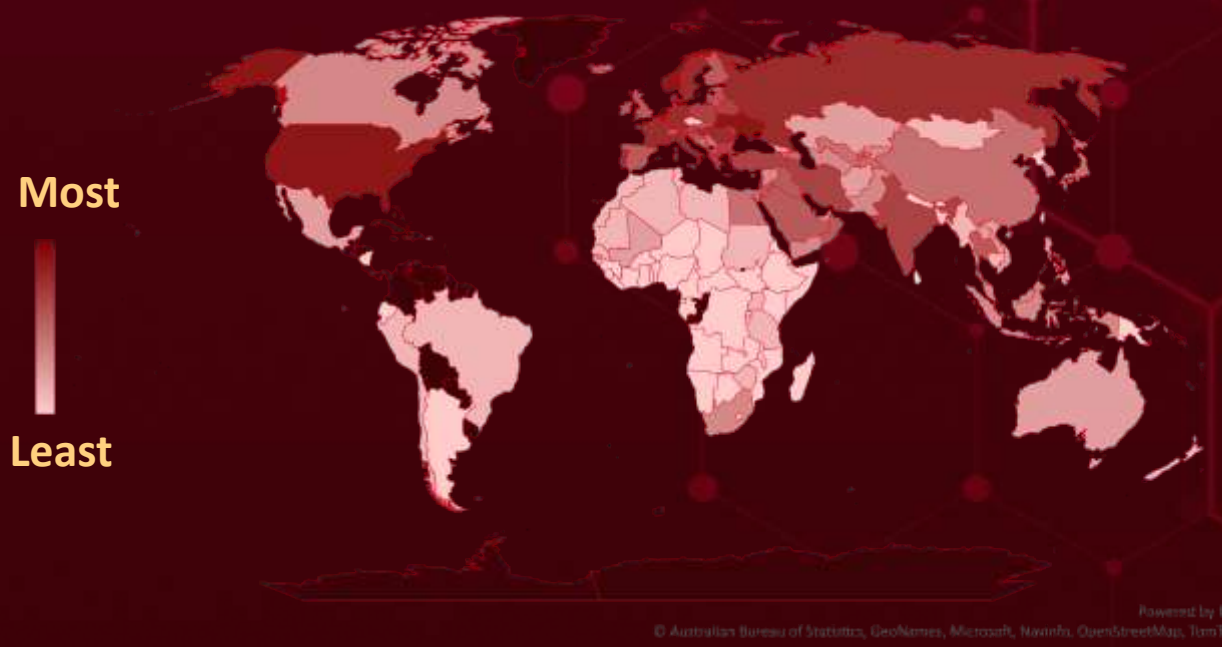
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
BlueNoroff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet)	Financial crime	North Korea	-	RustBucket	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
cisco	Network (EPN) Management	Evolved Programmable Network (EPN) Manager:7.0 Cisco Prime Infrastructure:3.9 - 3.10
	Identity Services Engine	Cisco Identity Services Engine (ISE): 3.2
	Infrastructure Management	Cisco Prime Infrastructure:3.9 - 3.10
	Operating System	Cisco IOS: 15.6.3 M1 - 16.5.1; Cisco IOS XE: 3.16.1aS
REALTEK	Software Development Kit	Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2
zimbra	Email messaging platform	Zimbra Collaboration: 9.0.0 P23
Cacti	Network monitoring tool	cacti: before 1.1.19-2.20
veritas	Backup Management	Veritas Backup Exec before 21.2
	Web Application	Apple Safari in macOS Big Sur and macOS Monterey: 16.0 - 16.4
	Operating System	macOS Ventura: 13.0 22A380 - 13.3 22E252
Microsoft	Operating System	Windows: 10 - 11 22H2 Windows Server: 2008-2022 20H2 Windows: Vista, XP, 7, 8, 8.1 Windows Server: 2003 - 2012
Google	Web Browser	Google Chrome: All versions (before 112.0.5615.121)

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
PaperCut	Print management software application	PaperCut MF: before 22.0.9; PaperCut NG: before 22.0.9
ZOHO	ManageEngine	ManageEngine Access Manager Plus: 4.1 4100 - 4.3 4307 Vulnerability Manager Plus: before 10.1.2220.18 Remote Monitoring and Management (RMM): before 10.1.41 Zoho ManageEngine Remote Access Plus: before 10.1.2228.11 Patch Manager Plus: before 10.1.2220.18 Password Manager Pro: before 12124 PAM 360: before 5713 OS Deployer: before 1.1.2243.1 Key Manager Plus: before 6401 Endpoint DLP: before 10.1.2137.6 Endpoint Central MSP: before 10.1.2228.11 Endpoint Central: before 10.1.2228.11 Device Control Plus: before 10.1.2220.18 ManageEngine Browser Security Plus: before 11.1.2238.6 ManageEngine Application Control Plus: before 10.1.2220.18 ManageEngine Analytics Plus: before 5150 Zoho ManageEngine ADManager Plus: before 7162 Zoho ManageEngine Active Directory 360: before 4310 ManageEngine AssetExplorer: before 6983 Zoho ManageEngine ServiceDesk Plus MSP: before 13001 Zoho ManageEngine SupportCenter Plus: before 11026 Zoho ManageEngine ADAudit Plus: before 7081 Zoho ManageEngine ADSelfService Plus: before 6211 Zoho ManageEngine ServiceDesk Plus: before 14.0 14004

Targeted Countries



Color	Countries
	Netherlands
	United States
	Norway
	Ukraine
	Belgium
	Germany
	Italy
	Denmark
	Romania
	Hungary
	Portugal
	France
	Sweden
	Russia
	Greece
	Bulgaria
	Turkey
	India
	Iran
	Poland
	Austria
	Belarus
	Moldova
	Albania

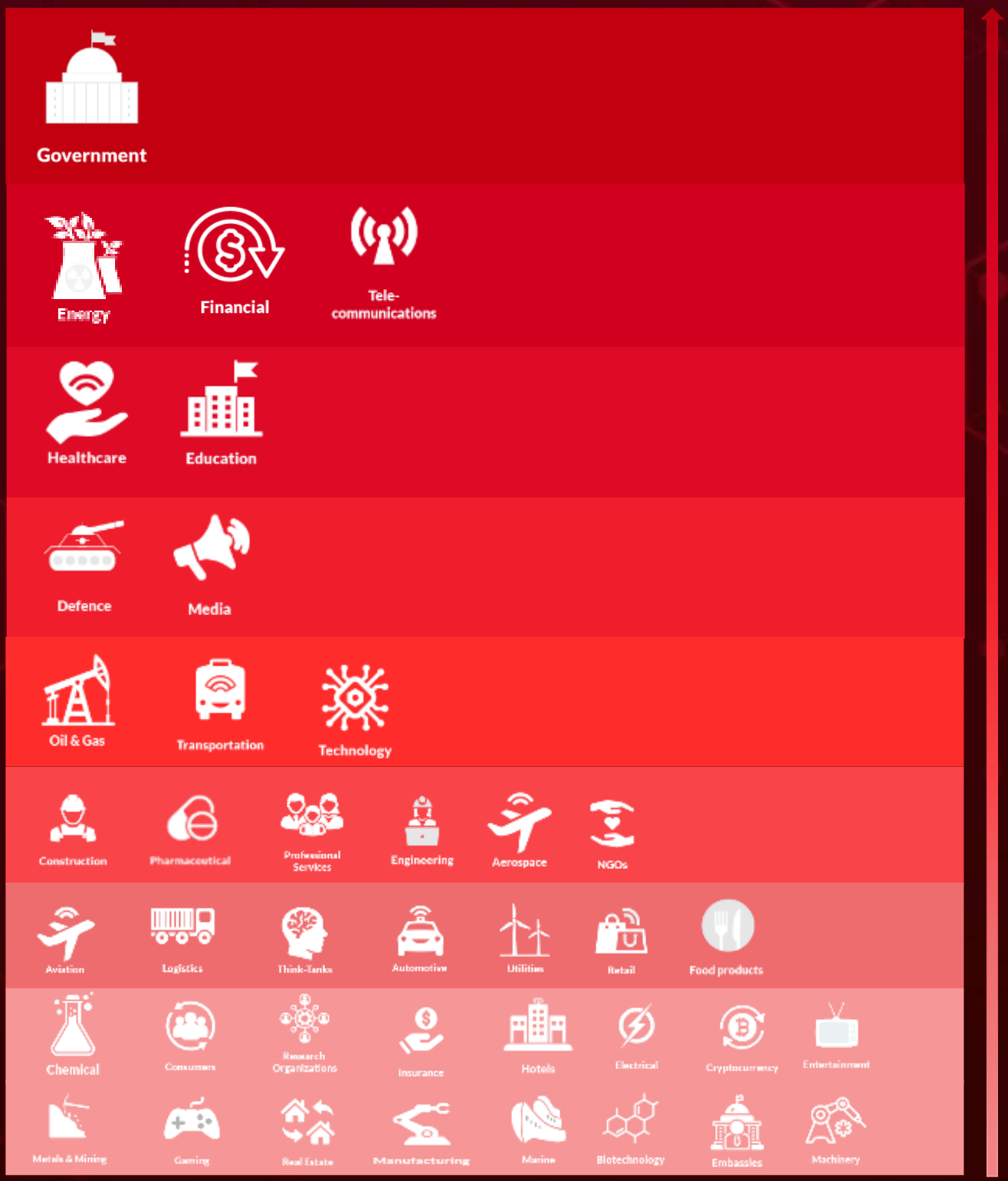
Color	Countries
	Saudi Arabia
	United Kingdom
	Thailand
	Iceland
	North Macedonia
	Bahrain
	Cyprus
	Lithuania
	Oman
	Lebanon
	Estonia
	Latvia
	Montenegro
	Kuwait
	Spain
	Jordan
	Slovenia
	Switzerland
	Finland
	Ireland
	Slovakia
	Iraq
	Croatia

Color	Countries
	Luxembourg
	Qatar
	Japan
	San Marino
	Tajikistan
	Armenia
	Malta
	Israel
	China
	Uzbekistan
	Bosnia and Herzegovina
	Egypt
	Holy See
	Serbia
	Azerbaijan
	Liechtenstein
	Monaco
	Andorra
	South Africa
	Malaysia
	UAE
	Palestine
	Vietnam
	Australia

Color	Countries
	Philippines
	Georgia
	Mali
	Afghanistan
	Senegal
	Brazil
	Uganda
	Timor-Leste
	Mongolia
	New Zealand
	Tanzania
	Türkiye
	Algeria
	Myanmar
	Hong Kong
	Zimbabwe
	Herzegovina
	Chile
	Peru
	Morocco
	Mauritius
	Cambodia
	Taiwan
	Sudan

Color	Countries
	Tunisia
	Brunei
	Mauritania
	Libya
	Argentina
	Kingdom
	Niger
	Seychelles
	UK
	Papua
	Nigeria
	Guinea-Bissau
	Burundi
	Guinea
	Bosnia
	Spain
	Somalia
	Ghana
	State of Palestine
	Germany
	Central African Republic
	Maldives

Targeted Industries



TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter

T1027 Obfuscated Files or Information

T1083 File and Directory Discovery

T1566 Phishing

T1082 System Information Discovery

T1190 Exploit Public-Facing Application

T1036 Masquerading

T1071 Application Layer Protocol

T1486 Data Encrypted for Impact

T1204 User Execution

T1055 Process Injection

T1497 Virtualization /Sandbox Evasion

T1564 Hide Artifacts

T1068 Exploitation for Privilege Escalation

T1140 Deobfuscate/ Decode Files or Information

T1574 Hijack Execution Flow

T1095 Non-Application Layer Protocol

T1078 Valid Accounts

T1113 Screen Capture

T1134 Access Token Manipulation

T1016 System Network Configuration Discovery

T1102 Web Service

T1203 Exploitation for Client Execution

T1562.001 Disable or Modify Tools

T1005 Data from Local System

Top Indicators of Compromise (IOCs)

Attack	TYPE	VALUE
APT43	MD5	982fc9ded34c85469269eacb1cb4ef26 de9a8c26049699dbbd5d334a8566d38d 144bd7fd423edc3965cb0161a8b82ab2 cd83a51bec0396f4a0fd563ca9c929d7 33df74cbb60920d63fe677c6f90b63f9 ebaf83302dc78d96d5993830430bd169 b846fa8bc3a55fa0490a807186a8ece9 f92a75b98249fa61cf62e8b63cb68fae 1dcd5afeccfe2040895686eefa0a9629 5fe4da6a1d82561a19711e564adc7589
	SHA1	636f2c20183b45691b742949d49b3d6c218c9cce 1f6c7c9219f6b6ea30cd481968ae1a038789be67 6618e25dd49b68f7b2b266eb2d787e6f05c964bc 700acc4e48eae84f80f4dbaf74bf60b79efd49bd 25d94c9ab7635ff330dabe96780f330f7f2ba775 851ba2182b37bc7380420a986840e16f73947413 d3b233d6d8b11235929e4a0cbdb12eefdd47d927 e5b312155289cdc6a80a041821fc82d2cca80bcd 40826e2064b59b8b7b3e514b9ef2c1479ac3b038
	SHA256	43c2d5122af50363c29879501776d907eaa568fa142d935f6c80e823d18223f5 557ff6c87c81a2d2348bd8d667ea8412a1a0a055f5e1ae91701c2954ca8a3fdb 2b78d5228737a38fa940e9ab19601747c68ed28e488696694648e3d70e53eb5a fb7fb6dbaf568b568cd5e60ab537a42d5982949a5e577db53cc707012c7f20e3 94aa827a514d7aa70c404ec326edaaad4b2b738ffaea5a66c0c9f246738df579 5cbc07895d099ce39a3142025c557b7fac41d79914535ab7ffc2094809f12a4b 855656bfecc359a1816437223c4a133359e73ecf45acda667610fbe7875ab3c8 d0971d098b0f8cf2187feeed3ce049930f19ec3379b141ec6a2f2871b1e90ff7 07aed9fa864556753de0a664d22854167a3d898820bc92be46b1977c68b12b34

Attack	TYPE	VALUE
Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)	Domains	jumpstartmail[.]com paydayloansnew[.]com picture-world[.]info rnacgroup[.]com salimafia[.]net seomoi[.]net soft-utils[.]com chloe-boreman[.]com criston-cole[.]com
	URLs	hxxp[:]//5.182.39[.]44/esuzmwmrtajj/cmsnvbyawttf/mkxnhqwdywbu
	IPV4	104.194.222[.]50:4444
	SHA256	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311 3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529 82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4 85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097 cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341 f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8 21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8 58331695280fc94b3e7d31a52c6a567a4508dc7be6bdc200f23f5f1c72a3f724 5af853164cc444f380a083ed528404495f30d2336ebe0f2d58970449688db39e 0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038 1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa 211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d

Attack	TYPE	VALUE
Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)	SHA256	d10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798 5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4 f38ad4aa79b1b448c4b70e65aecc58d3f3c7eea54feb46bdb5d10fb92d880203 c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b f98bc2ccac647b93f7f7654738ce52c13ab477bf0fa981a5bf5b712b97482dfb 411086a626151dc511ab799106cfa95b1104f4010fe7aec50b9ca81d6a64d299 5ea6bdae7b867b994511d9c648090068a6f50cb768f90e62f79cd8745f53874d 6a0686323df1969e947c6537bb404074360f27b56901fa2bac97ae62c399e061 11b81288e5ed3541498a4f0fd20424ed1d9bd1e4fae5e6b8988df364e8c02c4e 1b62730d836ba612c3f56fa8c3b0b5a282379869d34e841f4dca411dce465ff6 220eba0feb946272023c384c8609e9242e5692923f85f348b05d0ec354e7ac3c 4840214a7c4089c18b655bd8a19d38252af21d7dd048591f0af12954232b267f 4a25ca8c827e6d84079d61bd6eba563136837a0e9774fd73610f60b67dca6c02 624705483de465ff358ffed8939231e402b0f024794cf3ded9c9fc771b7d3689 7ae97402ec6d973f6fb0743b47a24254aaa94978806d968455d919ee979c6bb4 8d1c7d1de4cb42aa5dee3c98c3ac637aebfb0d6220d406145e6dc459a4c741b2 b6a71ca21bb5f400ff3346aa5c42ad2faea4ab3f067a4111fd9085d8472c53e3 bb6fd3f9401ef3d0cc5195c7114764c20a6356c63790b0ced2baceb8b0bdac51 bc9a4df856a8abde9e06c5d65d3bf34a4fba7b9907e32fb1c04d419cca4b4ff9 d420b123859f5d902cb51cce992083370bbd9deca8fa106322af1547d94ce842

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20121		Evolved Programmable Network (EPN) Manager:7.0 Cisco Identity Services Engine (ISE): 3.2 Cisco Prime Infrastructure:3.9 - 3.10	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco_systems:evolved_programmable_network_manager:*:*:*:*:*:*:*:*	-
Cisco EPNM, Cisco ISE, and Cisco Prime Infrastructure Command Injection Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-77	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20122		Cisco Identity Services Engine (ISE): 3.2	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco_systems:cisco_identity_services_engine:3.2:*:*:*:*:*:*:*	-
Cisco ISE Command Injection Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-77	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-35394		Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:realtek:realtek_jungle_sdk:*:*:*:*:*:*:*:*	Shellbot and Moobot
Realtek Jungle SDK Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77 CWE-787	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-27926		Zimbra Collaboration: 9.0.0 P23	Winter Vivern
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41352	✗	Zimbra Collaboration(ZCS)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zimbra:collaboration:8.8.15:-:*:*:*:*:*:*	Rorschach/BabLock Ransomware
Zimbra Collaboration (ZCS) Arbitrary File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1608.001: Stage Capabilities: Upload Malware	https://wiki.zimbra.com/wiki/Security_Center

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-46169	✗	cacti: before 1.1.19-2.20	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cacti:cacti:*:*:*:*:*:*:*:*	ShellBot and Moobot
Cacti Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77 CWE-74	T1202: Indirect Command Execution	https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27876	✗ ZERO-DAY	Veritas Backup Exec before 21.2	UNC4466
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent File Access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27877	✗ ZERO-DAY	Veritas Backup Exec before 21.2	UNC4466
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent Improper Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27878	✗	Veritas Backup Exec before 21.2	UNC4466
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*:*	BlackCat ransomware
Veritas Backup Exec Agent Command Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1090: Proxy; T1134: Access Token Manipulation; T1185: Browser Session Hijacking; T1505: Server Software Component	https://www.veritas.com/support/en_US/security/VTS21-001

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28205	✗	Apple Safari in macOS Big Sur and macOS Monterey: 16.0 - 16.4 macOS Ventura: 13.0 22A380 - 13.3 22E252	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:apple_safari:*:*:*:*:*:*:*:*, cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple WebKit Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1102: Web Service; T1005: Data from Local System; T1048: Exfiltration Over Alternative Protocol	https://support.apple.com/en-us/HT213722 https://support.apple.com/en-us/HT213721

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28206	✗ ZERO-DAY	macOS Ventura: 13.0 22A380 - 13.3 22E252	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1189: Drive-by Compromise; T1190: Exploit Public-Facing Application; T1547: Boot or Logon Autostart Execution; T1547.006: Kernel Modules and Extensions; T1014: Rootkit	https://support.apple.com/en-us/HT213721

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28252	✗ ZERO-DAY	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Nokoyawa ransomware
Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2013-3900	✗	Windows: Vista, XP, 7, 8, 8.1; Windows Server: 2003 - 2012	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*; cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Microsoft WinVerifyTrust function Remote Code Execution	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20 CWE-310	T1027: Obfuscated Files or Information; T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2033	✗	Google Chrome: All versions (before 112.0.5615.121)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:google_chrome:-:*:*:*:*:*:*:*	-
Google Chrome Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-843	T1203:Exploitation for Client Execution; T1068:Exploitation for Privilege Escalation; T1190:Exploit Public-Facing Application; T1588:Obtain Capabilities; T1588.006:Vulnerabilities; T1588.005:Exploits	Upgrade the chromium package to version 112.0.5615.121. https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-6742	ZERO-DAY	Cisco IOS: 15.6.3 M1 - 16.5.1; Cisco IOS XE: 3.16.1aS	APT28
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios:*:*:*:*:*:*:*:*	Jaguar Tooth
Cisco SNMP Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1574: Hijack Execution Flow; T1499.004: Endpoint Denial of Service: Application or System Exploitation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350	ZERO-DAY	PaperCut MF: before 22.0.9; PaperCut NG: before 22.0.9	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*; cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*;	-
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1505: Server Software Component	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966	 ZERO-DAY	Zoho ManageEngine Multiple Products	Charming Kitten
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine:*:*:*:*:*:*:*:*	BellaCiao
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1499: Endpoint Denial of Service; T1090: Proxy	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AlienFox	AlienFox is a toolkit used by attackers to target email and web hosting services, particularly cloud-based and software-as-a-service (SaaS) email hosting services	Compromise email and web hosting services	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular Toolkit		Collecting credentials for multiple cloud service providers	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShellBot (aka PerlBot, DDoS Perl IrcBot)	ShellBot is a type of malware coded in Perl and utilizes the Internet Relay Chat (IRC) protocol to communicate with the server, also known as PerlBot.	Exploiting Cacti and Realtek vulnerabilities	CVE-2021-35394 CVE-2022-46169
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnets		Remote attackers gain control of the vulnerable systems	Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2; cacti: before 1.1.19-2.20
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en; https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf

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
Moobot	Moobot, is a variant of the Mirai botnet that aims to exploit exposed networking devices.	Exploiting Cacti and Realtek vulnerabilities	CVE-2021-35394 CVE-2022-46169
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnets		Remote attackers gain control of the vulnerable systems	Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2; cacti: before 1.1.19-2.20
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en; https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rorschach/babLock	Rorschach is a new and highly effective ransomware that uses a hybrid-cryptography scheme and fast thread scheduling via I/O completion ports.	Malicious email attachment	CVE-2022-41352
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	Zimbra Collaboration(ZCS)
ASSOCIATED ACTOR			**PATCH LINK**
Rorschach/babLock			https://wiki.zimbra.com/wiki/Security_Center

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
Money Message	'Money Message' is a new ransomware group that targets victims all over the world, demanding million-dollar ransoms to avoid data leaks and deliver a decryptor.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	-
ASSOCIATED ACTOR			PATCH LINK
Money Message			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackCat (aka ALPHV and Noberus) ransomware	BlackCat ransomware is known for being based on the Rust programming language and for its use of evasion techniques to avoid detection by security software.	Internet-exposed Windows server, running Veritas Backup Exec version 21.0	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, unauthorized access, and infrastructure damage	Veritas Backup Exec
ASSOCIATED ACTOR			PATCH LINK
UNC4466			https://www.veritas.com/support/en_US/security/VTS21-001

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cylance	Cylance ransomware is a new malware that can adjust to customized encryption tactics and can accept different command-line parameters.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Micropsia	Micropsia is a backdoor used by attackers to run secondary payloads and perform various functions, such as keylogging and data exfiltration.	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Gain unauthorized access to a system or network	-
ASSOCIATED ACTOR			PATCH LINK
Desert Falcons			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Arid Gopher	Arid Gopher is a Go-written malware used in cyber campaigns that contain embedded components and is regularly updated and rewritten by attackers to evade detection	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Credential theft and exfiltration of stolen data	-
ASSOCIATED ACTOR			PATCH LINK
Desert Falcons			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nokoyawa	Nokoyawa ransomware is a new threat that exploits vulnerability to infiltrate and encrypt victims' files, demanding a ransom for their release.	Through CVE-2023-28252	CVE-2023-28252
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, unauthorized access, and infrastructure damage	Windows & Windows Server
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252

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
CHM	The CHM dropper is distributed via CHM files, which have the capability to gather user data, establish persistence, and perform various malicious actions according to the attacker's command	Via Email attachments	-
TYPE		IMPACT	AFFECTED PRODUCTS
Dropper		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Bitter APT			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Trigona	Trigona ransomware is installed on vulnerable MS-SQL servers that are not properly managed, allowing attackers to execute malicious commands and encrypt files without distinguishing file extensions.	Improperly managed MS-SQL servers	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Havoc Demon	Havoc Demon Backdoor malware attack targets Windows users through a spoofed document from Energoatom, a state-owned enterprise that operates Ukraine's nuclear power plants.	Via Email attachments	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Gain control over the compromised machines	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rilide	The Rilide Stealer Extension is a sophisticated malware that disguises itself as a benign Google Drive extension and targets Chromium-based browsers, carrying out various malicious activities such as injecting scripts and exfiltrating sensitive information.	By mimicking Google Drive extensions	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal data and exfiltrate URLs and screenshots.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Kadavro Vector Ransomware	Kadavro Vector is a specific variation of NoCry ransomware. The attackers demand payment in Monero (XMR) cryptocurrency in exchange for the decryption of the files.	Fake Tor Browser Installers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial loss, unauthorized access, and exfiltration of stolen data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crimson RAT	APT36 is targeting educational institutions and students in the Indian subcontinent by distributing malicious documents disguised as education-themed content to stage the Crimson RAT malware using tactics like OLE embedding.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
APT 36			-

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
Zaraza bot	A new credential-stealing malware named Zaraza bot uses Telegram as its command and control, targeting 38 web browsers	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		exfiltrating sensitive data for potential identity theft and financial fraud.	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Dave Loader	Dave Loader is developed by members of the Wizard Spider group. Dave Loader has been utilized this year to load IcedID and Emotet serve as initial access vectors for ransomware attacks.	Phishing or Malvertising	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Gain unauthorized access to a system or network	-
ASSOCIATED ACTOR			PATCH LINK
FIN7 & Wizard Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Domino Backdoor	The Domino Backdoor obtains fundamental system information, which it then transmits to the C2, and receives an AES-encrypted payload in return.	Dave Loader	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Credential theft and exfiltration of stolen data	-
ASSOCIATED ACTOR			PATCH LINK
FIN7 & Wizard Spider			-

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
NewWorldOrder Loader	The NewWorldOrder loader, typically used in FIN7's Carbanak attacks was recently employed to distribute the Domino malware.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7 & Wizard Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Carbanak Backdoor	The Carbanak Backdoor was loaded using NewWorldOrder Loader samples with the same filename ThunderboltService.exe. FIN7 has been using Carbanak since late 2015.	NewWorldOrder Loader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data loss, unauthorized access, and infrastructure damages	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7 & Wizard Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Project Nemesis infostealer	The Domino Loader includes an encrypted payload in its resources, which it decrypts using AES. The decrypted payload is a .NET infostealer identified as "Nemesis Project," which is one of Domino's final payloads.	Domino Loader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7 & Wizard Spider			-

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 ransomware, known as the oldest ransomware affiliate program, has been discovered on VirusTotal compiled for Apple's macOS arm64 architecture, raising concerns about the ransomware threat on Mac devices.	Ransomware affiliate program	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and Financial Fraud	-
ASSOCIATED ACTOR			**PATCH LINK**
LockBit Gang			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
QBot (also known as QakBot, QuackBot, and Pinkslipbot)	The QBot malware is capable of intercepting traffic and giving operators remote access to the infected system. The Trojan can also download additional malware, such as CobaltStrike or ransomware and turn the victim's computer into a proxy server to facilitate the redirection of traffic.	Malicious PDF attachments in emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Credential theft, data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CrossLock	CrossLock ransomware, implemented in Go programming language, uses double extortion technique to encrypt and exfiltrate data, posing a significant threat to businesses and organizations.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Jaguar Tooth	Jaguar Tooth is a non-persistent malware that exploits the patched SNMP vulnerability to collect device information, exfiltrate it over TFTP, and enable unauthenticated backdoor access to target Cisco IOS routers.	Via SNMP vulnerability in Cisco IOS routers	CVE-2017-6742
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Unknown		Obtain device information	Cisco IOS and IOS XE Software
ASSOCIATED ACTOR			**PATCH LINK**
APT 28			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EvilExtractor	EvilExtractor is a novel type of malware that functions as an all-in-one stealer, allowing cybercriminals to extract sensitive information and files from Windows operating systems.	Via Phishing email campaign	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MgBot	MgBot is a modular malware framework that is actively maintained and equipped with various plugins, allowing attackers to gather extensive information from compromised machines, indicating that the attackers' primary objective was information-gathering.	Legitimate AnyDesk remote desktop software	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Framework		Data theft and espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Daggerfly			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BellaCiao	BellaCiao is a personalized dropper malware used to deliver other malware payloads, with samples tailored to specific victims and countries, and named after an Italian folk song.	Unknown	CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Data loss, unauthorized access, and infrastructure damage	Zoho ManageEngine
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PingPull	The PingPull malware variant that targets Linux systems is linked to Alloy Taurus, and it communicates with a domain over HTTPS to receive encrypted commands for executing specific functions.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft and espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Alloy Taurus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VEILEDSIGNAL	VEILEDSIGNAL backdoor uses Windows named pipes for C2 communication and can execute shellcode.	Via trojanized X_Trader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Compromise critical infrastructure and sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustBucket	RustBucket macOS malware family split into two stages, with the second stage application appearing as a legitimate PDF viewer but becoming malicious when a specific PDF is loaded.	Via PDF Viewer App	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Compromise critical infrastructure and sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
BlueNoroff			-

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT43	North Korea	NGOs, Education, Governments, Media and entertainment, Construction, Materials, Defense, Aerospace, Telecoms, High-tech , Pharmaceuticals, Consulting and Professional services	United States, Germany, Belgium, United Kingdom, Sweden, Norway, Thailand, South Korea, Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

T1566 Phishing;T1566.001 Spearphishing Attachment;T1566.002 Spearphishing Link;Resource Development;T1583.003 Virtual Private Server;T1584 Compromise Infrastructure;T1588.003 Code Signing Certificates;T1588.004 Digital Certificates;T1608.003 Install Digital Certificate;T1608.005 Link Target;T1047 Windows Management Instrumentation;T1053.005 Scheduled Task;T1059 Command and Scripting Interpreter;T1059.00: PowerShell;T1059.003 Windows Command Shell;T1059.005 Visual Basic;T1059.007 JavaScript;T1129 Shared Modules;T1203 Exploitation for Client Execution;T1204.001 Malicious Link;T1204.002 Malicious File;T1569.002 Service Execution;Command and Control;T1071.001 Web Protocols;T1071.004 DNS;T1090.003 Multi-hop Proxy;T1095 Non-Application Layer Protocol;T1102 Web Service;T1102.002 Bidirectional Communication;T1105 Ingress Tool Transfer;T1132.001 Standard Encoding;T1573.002 Asymmetric Cryptography;T1007 System Service Discovery;T1010 Application Window Discovery;T1012 Query Registry;T1016 System Network Configuration;T1033 System Owner/User Discovery;T1057 Process Discovery;T1082 System Information Discovery;T1083 File and Directory Discovery;T1087 Account Discovery;T1518 Software Discovery;T1614.001 System Language Discovery;T1056.001 Keylogging;T1113 Screen Capture;T1115 Clipboard Data;T1213 Data from Information Repositories;T1560 Archive Collected Data;T1560.001 Archive via Utility;T1137 Office Application Startup;T1505.00 Web Shell;T1543.003 Windows Service;T1547.001: Registry Run Keys / Startup Folder;T1547.004 Winlogon Helper DLL;T1547.009 Shortcut Modification;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;T1055.003 Thread Execution Hijacking;T1070.004 File Deletion;T1070.006 Timestomp;T1112 Modify Registry;T1134 Access Token Manipulation;T1140 Deobfuscate/Decode Files or Information;T1218.005 Mshta;T1497 Virtualization/Sandbox Evasion;T1497.001 System Checks;T1548.002: Bypass User Account Control;T1553.002 Code Signing;T1564.003 Hidden Window;T1564.007 VBA Stomping;T1620: Reflective Code Loading;T1622 Debugger Evasion;T1489 Service Stop;T1529 System Shutdown/Reboot;T1020 Automated Exfiltration;T1110 Brute Force;T1555.003 Credentials from Web Browsers

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Winter Vivern (aka TA473 and UAC-0114)	Unknown	Government, Telecommunications, Private businesses, military, and diplomatic organizations	Europe and NATO
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-27926	-	Zimbra Collaboration: 9.0.0 P23
TTPs			
T1027: Obfuscated Files or Information;T1068: Exploitation for Privilege Escalation;T1134: Access Token Manipulation;T1566: Phishing;T1555: Credentials from Password Stores;T1114: Email Collection			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Rorschach Ransomware (aka BabLock)	Unknown	-	Worldwide except CIS countries
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-41352	Rorschach/BabLock Ransomware	Zimbra Collaboration(ZCS)
TTPs			
T1552 Unsecured Credentials; T1106 Native API;T1569 System Services;T1027 Obfuscated Files or Information;T1055 Process Injection;T1140 Deobfuscate/Decode Files or Information;T1615 Group Policy Discovery;T1069 Permission Groups Discovery;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;T1055.002 Portable Executable Injection;T1562 Impair Defenses;T1562.001 Disable or Modify Tools;T1564 Hide Artifacts;T1564.010 Process Argument Spoofing;T1497 Virtualization/Sandbox Evasion;T1486 Data Encrypted for Impact;T1574 Hijack Execution Flow;T1552.004 Private Keys;T1574.002 DLL Side-Loading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Money Message Ransomware	Unknown	BFSI, Transportation and Logistics, Professional Services, Airline, and Education	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Money Message Ransomware	-
TTPs			
T1204 User Execution, T1140 Deobfuscate/Decode Files or Information, T1562 Impair Defenses, T1007 System Service Discovery, T1083 File and Directory Discovery, T1135 Network Share Discovery, T1021 Remote Services, T1486 Data Encrypted for Impact, T1490 Inhibit System Recovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Bitter APT(T-APT-17, APT-C-08, Orange Yali)	South Asia	Government	China
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	CHM	-
TTPs			
T1007: System Service Discovery; T1204: User Execution; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1053: Scheduled Task/Job; T1083: File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC4466	Unknown	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-27876 CVE-2021-27877 CVE-2021-27878	BlackCat Ransomware	Veritas Backup Exec
TTPs			
T1486: Data Encrypted for Impact; T1489: Service Stop; T1490: Inhibit System Recovery; T1529: System Shutdown/Reboot; T1047: Windows Management Instrumentation; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1569: System Services; T1569.002: Service Execution; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1027.009: Embedded Payloads; T1055: Process Injection; T1070: Indicator Removal; T1070.001: Clear Windows Event Logs; T1070.004: File Deletion; T1112: Modify Registry; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1222: File and Directory Permissions Modification: T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1564: Hide Artifacts; T1564.010: Process Argument Spoofing; T1574: Hijack Execution Flow; T1574.011: Services Registry Permissions Weakness; T1620: Reflective Code Loading; T1622: Debugger Evasion; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1007: System Service Discovery; T1012: Query Registry; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1087: Account Discovery; T1135: Network Share Discovery; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1095: Non-Application Layer Protocol; T1105: Ingress Tool Transfer; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1213: Data from Information Repositories; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server		

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

Desert Falcons (Mantis, APT-C-23, Two-tailed Scorpion, Arid Viper, ATK 66, TAG-CT1)</td><td>Gaza</td><td rowspan="3">Government, Media, Financial, Research Institutions, Education, Activists, Political Leaders, Energy Firms, Physical Security Companies, Critical infrastructure, Defense, Transportation, Utilities, Aerospace, Think Tanks</td><td rowspan="3">Akrotiri and Dhekelia, Albania, Algeria, Australia, Bahrain, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherland, Netherlands, Norway, Oman, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen, Zimbabwe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Micropsia backdoor and Arid Gopher info-stealer</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1053: Scheduled Task/Job; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1548: Abuse Elevation Control Mechanism; T1055: Process Injection; T1564: Hide Artifacts; T1562: Impair Defenses; T1070: Indicator Removal; T1036: Masquerading; T1212: Exploitation for Credential Access; T1056: Input Capture; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1001: Data Obfuscation; T1105: Ingress Tool Transfer; T1571: Non-Standard Port; T1047: Windows Management Instrumentation; T1566.002: Spearphishing Link</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 MERCURY (MuddyWater, Seedworm, TEMP.Zagros, Static Kitten, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

T1083: File and Directory Discovery; T1190: Exploit Public-Facing Application; T1505: Server Software Component; T1505.003: Web Shell; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1518: Software Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1590: Gather Victim Network Information; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1047: Windows Management Instrumentation; T1136: Create Account; T1136.001: Local Account; T1548: Abuse Elevation Control Mechanism; T1548.004: Elevated Execution with Prompt; T1070: Indicator Removal; T1070.004: File Deletion; T1578: Modify Cloud Compute Infrastructure; T1578.003: Delete Cloud Instance; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1572: Protocol Tunneling; T1210: Exploitation of Remote Services; T1003: OS Credential Dumping; T1078: Valid Accounts; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1059: Command and Scripting Interpreter; T1046: Network Service Discovery; T1069: Permission Groups Discovery; T1018: Remote System: Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1027: Obfuscated Files or Information; T1569: System Services; T1569.002: Service Execution; T1573: Encrypted Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Unknown	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
DEV-1084	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

T1083: File and Directory Discovery; T1190: Exploit Public-Facing Application; T1505: Server Software Component; T1505.003: Web Shell; T1546: Event Triggered Execution; T1546.013: PowerShell Profile; T1518: Software Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1590: Gather Victim Network Information; T1484: Domain Policy Modification; T1484.001: Group Policy Modification; T1047: Windows Management Instrumentation; T1136: Create Account; T1136.001: Local Account; T1548: Abuse Elevation Control Mechanism; T1548.004: Elevated Execution with Prompt; T1070: Indicator Removal; T1070.004: File Deletion; T1578: Modify Cloud Compute Infrastructure; T1578.003: Delete Cloud Instance; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1572: Protocol Tunneling; T1210: Exploitation of Remote Services; T1003: OS Credential Dumping; T1078: Valid Accounts; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1059: Command and Scripting Interpreter; T1046: Network Service Discovery; T1069: Permission Groups Discovery; T1018: Remote System: Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1027: Obfuscated Files or Information; T1569: System Services; T1569.002: Service Execution; T1573: Encrypted Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT 36(Transparent Tribe, ProjectM, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH)	Pakistan	Education	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Crimson RAT	-
TTPs			
T1566:Phishing; T1559:Inter-Process Communication; T1547:Boot or Logon Autostart Execution; T1113:Screen Capture; T1102:Web Service; T1127:Trusted Developer Utilities Proxy Execution; T1531:Account Access Removal; T1140:Deobfuscate/Decode Files or Information; T1027:Obfuscated Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 FIN7(aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)	Russia	-	Worldwide
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer	-
TTPs			
T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1129:Shared Modules; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1562:Impair Defenses; T1562.001:Disable or Modify Tools; T1027:Obfuscated Files or Information; T1497.002:User Activity Based Checks; T1564:Hide Artifacts; T1564.003:Hidden Window; T1003:OS Credential Dumping; T1056:Input Capture; T1056.001:Keylogging; T1010:Application Window Discovery; T1057:Process Discovery; T1518:Software Discovery; T1115:Clipboard Data; T1005:Data from Local System; T1071:Application Layer Protocol; T1573:Encrypted Channel; T1518.001:Security Software Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Wizard Spider(aka ITG23, Grim Spider, TEMP.MixMaster, Gold Blackburn, Gold Ulrick)	Russia	-	Worldwide
	MOTIVE		
	Financial crime, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer	-
TTPs			
T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1129:Shared Modules; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1562:Impair Defenses; T1562.001:Disable or Modify Tools; T1027:Obfuscated Files or Information; T1497.002:User Activity Based Checks; T1564:Hide Artifacts; T1564.003:Hidden Window; T1003:OS Credential Dumping; T1056:Input Capture; T1056.001:Keylogging; T1010:Application Window Discovery; T1057:Process Discovery; T1518:Software Discovery; T1115:Clipboard Data; T1005:Data from Local System; T1071:Application Layer Protocol; T1573:Encrypted Channel; T1518.001:Security Software Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 LockBit Gang	Unknown	Automotive, Aviation, Biotechnology, Chemicals, Construction & Engineering, Consumer, Defense, Distributors, Education, Electrical, Energy, Family Services, Financial, Food Products, Healthcare, Hotels, Insurance, IT, Machinery, Marine, Media, Metals & Mining, Oil and Gas, Pharmaceuticals, Professional Services, Real Estate, Retail, Telecommunication, Transportation, Utilities	Argentina, Australia, Austria, Bahrain, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Cyprus, Czech Republic, Denmark, Ecuador, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Ireland, Isle of Man, Italy, Japan, Kuwait, Lebanon, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Oman, Peru, Poland, Portugal, Puerto Rico, Qatar, Romania, Saudi Arabia, Senegal, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Tanzania, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Vietnam, Ukraine
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	LockBit Ransomware	-
TTPs			
T1486:Data Encrypted for Impact; T1059:Command and Scripting Interpreter; T1195:Supply Chain Compromise; T1553:Subvert Trust Controls; T1553.002:Code Signing; T1566:Phishing; T1566.001:Spearphishing Attachment; T1219:Remote Access Software:T1560:Archive Collected Data; T1027:Obfuscated Files or Information; T1204:User Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 APT28(Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium , Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12 , ITG05, TAG-0700, UAC-0028, Grey-Cloud)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.	Asia, Europe, North America, South America, Oceania, Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-6742	Jaguar Tooth	Cisco IOS and IOS XE Software

TTPs

T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1078.001: Default Accounts; T1590: Gather Victim Network Information; T1556: Modify Authentication Process; T1601: Modify System Image; T1601.001: Patch System Image; T1048: Exfiltration Over Alternative Protocol; T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol; T1020: Automated Exfiltration; T1119: Automated Collection; T1602: Data from Configuration Repository; T1602.002: Network Device Configuration Dump; T1018: Remote System Discovery; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery: T1082: System Information Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Russia	Government and Diplomatic Entities	Commonwealth of Independent States (CIS)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Tomiris	-	-	-
TTPs			
T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation; T1566: Phishing; T1027: Obfuscated Files or Information; T1189: Drive-by Compromise; T1041: Exfiltration Over C2 Channel; T1127: Trusted Developer Utilities Proxy Execution: T1110: Brute Force; T1105: Ingress Tool Transfer; T1049: System Network Connections Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	China	Telecommunication	South Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Daggerfly(Bronze Highland, Evasive Panda)	-	MgBot	-
TTPs			
T1012: Query Registry; T1016: System Network Configuration Discovery; T1018: Remote System Discovery; T1027: Obfuscated Files or Information; T1027.005: Indicator Removal from Tools; T1036: Masquerading; T1055: Process Injection; T1056: Input Capture; T1056.001: Keylogging; T1057: Process Discovery; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestomp; T1082: System Information Discovery; T1083: File and Directory Discovery; T1106: Native API; T1112: Modify Registry; T1125: Video Capture; T1129: Shared Modules; T1497: Virtualization/Sandbox Evasion			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)	Iran	Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications	US, Europe, the Middle East, and India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-47966	BellaCiao	Zoho ManageEngine Multiple Products
TTPs			
T1071.001: Web Protocols; T1071: Application Layer Protocol; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1584: Compromise Infrastructure; T1203: Exploitation for Client Execution; T1083: File and Directory Discovery; T1059: Command and Scripting Interpreter; T1059.001: Power Shell; T1071.004: DNS; T1104: Multi-Stage Channels; T1505: Server Software Component; T1505.003: Web Shell; T1048: Exfiltration Over Alternative Protocol; T1505: Server Software Component; T1036: Masquerading; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Alloy Taurus (GALLIUM, Softcell, Phantom Panda)</td><td>China</td><td rowspan="3">Financial, Government & Telecommunications</td><td rowspan="3">Southeast Asia, Europe and Africa</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>PingPull</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1027: Obfuscated Files or Information; T1027.005: Indicator Removal from Tools; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1082: System Information Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1571: Non-Standard Port</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 BlueNoroff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet)	North Korea	Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchange	Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Netherlands, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RustBucket	-

TTPs
T1082: System Information Discovery; T1071: Application Layer Protocol; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1518: Software Discovery; T1518.001: Security Software Discovery; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1547: Boot or Logon Autostart Execution; T1070: Indicator Removal; T1070.006: Timestomp; T1222: File and Directory Permissions Modification: T1553: Subvert Trust Controls; T1553.002: Code Signing; T1083: File and Directory Discovery; T1566: Phishing; T1036: Masquerading

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
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 April, there were **six zero-day** vulnerabilities. One of these vulnerabilities was exploited by **Rorschach Ransomware group**

#2 Throughout the month, various ransomware strains including **as Rorschach, Money message, Blackcat, Trigona, Cylance, Nokoyawa,** and **LockBit** were active.

#3 Attackers are leveraging two vulnerabilities (CVE-2023-27350 and CVE-2023-27351)in PaperCut MF/NG software to install Atera remote management software

#4 Numerous malware families have been observed targeting victims worldwide. These include **Jaguar Tooth, BellaCiao, QBot, MgBot, Domino Backdoor,** and **Carbanak Backdoor.**

#5 **CVE-2023-2033** high-severity vulnerability is the first zero-day of 2023 Google Chrome.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **17 significant vulnerabilities** and block the indicators related to the **19 active threat actors, 32 active malware,** and **196 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 (APR 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

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
AlienFox	SHA1	c0184407dcbec911a325d41e9a9ef1dbed524fe5 41a2cab42a08adf93b5ada1eafb75d5b4f496853 3cb5b4182ef6e8174f87c8ed3551f91b72c47370 17592a2fdb8dae9c4c88f1fbf7e9c632129f98df ab8d480c090ab8be0cdb0ff5bc0f59972845b125 15ade0df5b4e6a82ceec429a2673fd1ed011eb93 aa8be80db30c4f5a49c3e75254ef6d0101c37987 064734bc43ee2d83e8a275293d17fc925620bba1 9381c30e29089639249e67b62f61c6df4869c6c1 fd5228889cd12f343236f7d51c98fab4db6c4763 fd3375553dda2347c0b383d8e800bfe4f93d3af0 F4ef68d3d2b58a58a82e00ebeaaed556e03328af 8e6e18ba7e251d31b46d17535010a8c583345b23 b3559eeac9a9caa840cc96980fe0bbd1c7da37d3 40df29a738fd5cab0face169d8a8426dff7d2d10 e663e24fc6aadbaae5bbf722a84097a6127f4066 c2f51b44e26e4aca40beb887ac4d36f3e091e26a 4266bdb139ae6d22ddf98501cc3af280aa488b42 329328dc57acece8c47ab5c73f7b9c7e4e09981a fc08c15dfd6074d80e1f8d777fb49f8c14b4af20 aa4672621f81f601882ad13f26d37dc8218bb06a 07289c56e65a98a85bc794374949aae98b819823 4ab401d4c490460fd457151f643b5ec7e594cd41 7848e53133f4470c29e33ee6dd87f8f326c5fa38 7d7bad6282531521b9103817a38bff3a34b89428 15129436f5bab6c3eea9b2dfc4d0f0043438e013
	SHA1	15aec55e56225700766d79b6fb9d212cced21951 ebdc60f33d22c4256ca6ab4058059db1d618ec11 894fd799168f9ff11e74ee37d5bec35387feef24 28de7d7fcd18471f53737fd8a3df3a23a34cf758 3ddb8dc53b6151ea036db3d2a5f34e5f5b39e044 ceda47dd1aacc515d8bdda04299ab1ebf1ba0d73 23abd146befe761337e5155a116138acf81331d9 ac265c12a4f08378e2519e290b0c45a1adc7156f b8dc12cc600aced9d34c463c5bf5edb53db605fb 45a0675088afdcf2ec059510fc2a4905957c2a69 c3464926cf2075595c77dc5b3fbcf1f014c8046b fc0479a3d1188384613f437f28e28614a6118e94 5c9993e5d7468551c60e6dab488eccea7f4ef007 ece7e6727d2daa254e4d4a6be62744d6f3a2a2ef

Attack Name	TYPE	VALUE
AlienFox	SHA1	afb7b010bafb9f7faf2b528f128ff24da94e0190 959e377131762ccb879c36c53e3b71473d3b72fd 48afb7ac8fdf6a8da47601806a8028c61dad2eb7 23abd146befe761337e5155a116138acf81331d9 f5af939480fc86a086bc589047444b1c448ebb09 ac265c12a4f08378e2519e290b0c45a1adc7156f 0f1583b56dd02fc200c7dae0d3c9b32b4278846b 74c4cfa0edae5e87001c901214789cb0f0087031 ec5b2efe8eadfac7ceca545e25f06240bbf16960 9eb13d9a678cd2e78da41563b7461887ce5997b6 25bbda606c72e81fac9abe76e0f00f9cd12770e4 E786fc1fdfcb7be28650383eb33cdf6c90f1d033
	URLs	https://t[.]co/0LjXP5lJFn https://t[.]co/dxSqA1kGrF https://t[.]co/p2DVjbm0qj http://t[.]me/xMarvel_official https://rtvsmkqfa3clrvgj6f-9fd73c[.]ingress-daribow[.]easywp[.]com/wp-admin/v1/1[.]php https://t[.]me/xcatzechat https://t[.]me/tutorials_zone https://t[.]me/xxyz4 hostnamertvsmkqfa3clrvgj6f-9fd73c[.]ingress-daribow[.]easywp[.]com https://rentry[.]co/3cii9/raw https://t[.]me/DailyTools https://t[.]me/exploi7 https://t[.]me/FoxCyberSecurity https://t[.]me/inscamwetrust0 https://t[.]me/official_xcatze https://t[.]me/sendgrid_aws_smtp https://t[.]me/Pegasus_Hub https://t[.]me/spamworldpro https://t[.]me/toxiarc
Shellbot	IPV4	104[.]244[.]76[.]105 156[.]224[.]24[.]249 206[.]217[.]205[.]24 199[.]195[.]250[.]172 80[.]68[.]196[.]6 85[.]239[.]33[.]32 46[.]101[.]183[.]162 49[.]212[.]234[.]206:3303 198[.]98[.]61[.]106:8080

Attack Name	TYPE	VALUE
Shellbot	Domains	apid[.]mutoujs[.]xyz troon[.]dns[.]army botnet[.]goelites[.]cc j[.]xnyidc[.]top www[.]xiaojue[.]cyou bot[.]layer7[.]top juice[.]baselinux[.]net:6667
	SHA256	c05cf5b2c94edd15c40db1ce52f97bdc09ec61e78386c8878b15515cbde99528 47ac3a2c51fc64479ceff1e842a414bc11dc59b9dcdbd3dd1bf011e243f91ffa 0c67234ce88958c9319ca9a8f8fdc4b4869013687151532450 9ac956704f1373 b7d62d1a145ddda241e624ef94ab31fcca1a13f79e130d0a704586e35745282a
Moobot	SHA256	e2075d6b723d7daf2303af31e3970ed79d435e52b4338ee63499c4644332ea10,3dbea4436ef3e00dcfb73608164e3d1ded9434f8ee1679cd3a790e22c91cbe11,455314a186b4a9a1788e2acb85a9b6b34fb0a7700d0decc6de056030fea543df,cd47c9db5e3ec59221361ca7459bb12a5a84014c1f8aa2e2bdad07ccb37a4e29,9144c4768b457fb5384bc807d9e992671c25dbefe9d2781672c018e1b4d8c36a,979bf642f67d5df2e8fa664c0bdecbc2954c9ced44f47122c71ad5f71a52aa0d,e2ff90f5bdf51da577be88266cc9dc8be48f1776af46949dcdd2d54e4c84449f,0cb77fabcef38d5ec4e1e64945bac8c33ea8e97346a3140e67ec30eecedc9ea0,0cd6a246eb6933bf5ac8639d8972e2c80dcdb7723a15435a914cf6b5bd30af4c,cf1b136558e7b5faf6bfce3b460afed06e613ca6747257273571399d106dea2b,175b536d5c825b78bd2567b836bb18046928f33f7ae1865afb66a4fe064ebb81,cdf1c2610bde8ae870bc083d06fb00ba1c3441c075fc6c26e9cc9f93c9a3703f,903c340da7c6ef32b2e3098389748fc5d94e88e61bfeea8a67313327f021fb9f,33aa8e731eca7ba051626845541f91fad6f69862aa1deaea7b80a15dae8d67bf,f473597e5fda9051522a52c78965d0eb050ff2971cfce8d359618e1c136ad77b,de5e60ab541838c4c3cb0bfd0733417f2fe4a19bac08683391022cdaabe263de,565d09c8fc9f712b82eae45a39029ac996904564cc08dae6306678081087e933,c33c66e7a161718da4535b34078edb04600c5a06eb1e05fe514a5ad5ac149594,e356ba8fe6ae21fbbba785ade3220a666e3fae947c68093e05b01f0c3f98e15f,7e4dadf93fbb7a01b55eadacbb40ae8d5e95f5b9592e55f0fb2340d89fc78f17,ae2c71e3e177721c336f76946d24b95512accf677c87e829a31b315d56624df3,e1366976365db1f2bffdc37d4e64e12f883f9a20e02b12d52b6a1b346b8f0692,abb3d04a081ee199cfb5687361fbbca3fa2012f588832e05de0e21874f162afd

Attack Name	TYPE	VALUE
Moobot	SHA256	5f0f2b2e3e839e50631b89cc2e9d980b337db417cab51f21beb0a56043297a6f,7d2c0cba18d51ed84e7a888d56dbcb5e73c1d076ed5f8e5db2528f826601b2cc,9a067e32dd6c25053c302de7caf61cdc0f3982289eb91d06c449fe08a47fc6d3,6804cebbf837d7c5559519c364cc0b20c4f9b514c74039321bc69bcfdbfb5e93,947675c8b2a65bf9b38f4d3d15d108e0826f570086c6a758d3e02be9315da1cd,c05cf5b2c94edd15c40db1ce52f97bdc09ec61e78386c8878b15515cbde99528,47ac3a2c51fc64479ceff1e842a414bc11dc59b9dcdbd3dd1bf011e243f91ffa,0c67234ce88958c9319ca9a8f8fdc4b4869013687151532450 9ac956704f1373,b7d62d1a145ddda241e624ef94ab31fcca1a13f79e130d0a704586e35745282a
	IPV4	104[.]244[.]76[.]105 156[.]224[.]24[.]249 206[.]217[.]205[.]24 199[.]195[.]250[.]172 80[.]68[.]196[.]6 85[.]239[.]33[.]32 46[.]101[.]183[.]162 49[.]212[.]234[.]206:3303 198[.]98[.]61[.]106:8080
	Domains	apid[.]mutoujs[.]xyz troon[.]dns[.]army botnet[.]goelites[.]cc j[.]xnyidc[.]top www[.]xiaojue[.]cyou bot[.]layer7[.]top juice[.]baselinux[.]net:6667
Rorschach/Bab Lock Ransomware	SHA256	38c610102129be21d8d99ac92f3369c6650767ed513e5744c0cda54e68b33812 e14b88795bde45cf736c8363c71a77171aa710a4e7fa9ce38470082cb1bdadbb 7d62a33e9a2fedff6cf27aaa142ff15838a766ccd4a8d326424611e155442775 83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00 b711579e33b0df2143c7cb61246233c7f9b4d53db6a048427a58c0295d8daf1c De5a53131225dd97040d48221d9afd98760f7ff2f55613f0d08436891ca632b9 4874d336c5c7c2f558cfd5954655cacfc85bcfcb512a45fb0ff461ce9c38b86d 2fd264f58ba82a2675280ec8c6759612def2bcc62aa6160f5e23071f67bb67ab

Attack Name	TYPE	VALUE
Rorschach/Bab Lock Ransomware	SHA256	03c41019faf7e4cc26ca0dd3a2c41b2115e4c4ebd561402079bc4a20256c1813 88081a21e500e831d86666ca5d7a3d348f7c03bc5c471b6d17d8b18a022f25be aa48acaef62a7bfb3192f8a7d6e5229764618ac1ad1bd1b5f6d19a78864eb31f b99d114b267ffd068c3289199b6df95a9f9e64872d6c2b666d63974bbce75bf2 66bcad0829a59c424d062b949c2a556b11c509b17515dffecb9cbf65f13f3dc6
	MD5	2237ec542cdcd3eb656e86e43b461cd1 4a03423c77fe2c8d979caca58a64ad6c 6bd96d06cd7c4b084fe9346e55a81cf9
	Emails	dcqyvp1@onionmail[.]org DcqYvp@onionmail[.]org dyhdsak@onionmail[.]org dyhdsak1@onionmail[.]org jzmc2t@tutanota[.]com jzmc2t@onionmail[.]org ngoueeb@onionmail[.]org ngoueeb1@onionmail[.]org vvbured@onionmail[.]org vvbured1@onionmail[.]org wvpater@onionmail[.]org wvpater1@onionmail[.]org
Money Message Ransomware	URLs	hxxp[:]//blogvl7tjyjvsfthobttze52w36wwiz34hrfcmorgvdzb6hikucb7aqd[.]onion hxxp[:]//p6kxp556kkcbjdjsg24g3edmvr7v7ujecuychw4ibvqhl6wuomnrgbqd[.]onion/
	MD5	400fa5d02c1ac704cd290d959b725e67 abe3c3cc45dec9c01762ba3e534564ed 163e651162f292028ca9a8d7f1ed7340
	SHA1	456e5cb1739cb5f29020d1a692289a5af07ce90d 3b4ecff980285461642cc4aef60d4a1b9708453e a85ff9091f298ea2d6823a7b0053daa08b237423
	SHA256	Dc563953f845fb88c6375b3e9311ebed49ce4bcd613f7044989304c8de384dac 4f8bd37851b772ee91ba54b8fd48304a6520d49ea4a81d751570ea67ef0a9904 bbdac308d2b15a4724de7919bf8e9ffa713dea60ae3a482417c44c60012a654b

Attack Name	TYPE	VALUE
BlackCat	IPV4	45[.]61[.]138[.]109 185[.]141[.]62[.]123 5[.]199[.]169[.]209
	URL	hxxp://185[.]141[.]62[.]123:10228/update[.]exe
	MD5	da202cc4b3679fdb47003d603a93c90d 5fe66b2835511f9d4d3703b6c639b866 1f437347917f0a4ced71fb7df53b1a05 b41dc7bef82ef384bc884973f3d0e8ca c590a84b8c72cf18f35ae166f815c9df 24b0f58f014bd259b57f346fb5aed2ea e31270e4a6f215f45abad65916da9db4 4fdabe571b66ceec3448939bfb3ffcd1 68d3bf2c363144ec6874ab360fdda00a ee6e0cb1b3b7601696e9a05ce66e7f37 f66e1d717b54b95cf32154b770e10ba4 17424a22f01b7b996810ba1274f7b8e9
	IPV4:PORT	45[.]61[.]138[.]109:45815 45[.]61[.]138[.]109:43937 45[.]61[.]138[.]109:36931 5[.]199[.]169[.]209:31600 45[.]61[.]138[.]109:41703 185[.]99[.]135[.]115:39839 185[.]99[.]135[.]115:41773 45[.]61[.]138[.]109:33971 185[.]141[.]62[.]123:50810 185[.]99[.]135[.]115:49196
Cylance	SHA256	ec8952dc14bac73174cef02a489539e244b378b7de76c771126a8ba7ce532efd D1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c
	SHA1	933ad0a7d9db57b92144840d838f7b10356c7e51 663081e2767df7083f765a3a8a994982959d4cbe
	MD5	521666a43aeb19e91e7df9a3f9fe76ba 4601076b807ed013844ac7e8a394eb33
Micropsia	SHA256	0a6247759679c92e1d2d2907ce374e4d6112a79fe764a6254baff4d14ac55038,1d1a0f39f339d1ddd506a3c5a69a9bc1e411e057fe9115352482a20b63f609aa,211f04160aa40c11637782973859f44fd623cb5e9f9c83df704cc21c4e18857d,D10a2dda29dbf669a32e4198657216698f3e0e3832411e53bd59f067298a9798,c4b9ad35b92408fa85b92b110fe355b3b996782ceaafce7feca44977c037556b
	Domains	criston-cole[.]com chloe-boreman[.]com

Attack Name	TYPE	VALUE
Arid Gopher	SHA256	0fb4d09a29b9ca50bc98cb1f0d23bfc21cb1ab602050ce786c86bd2bb6050311 3d649b84df687da1429c2214d6f271cc9c026eb4a248254b9bfd438f4973e529 82f734f2b1ccc44a93b8f787f5c9b4eca09efd9e8dcd90c80ab355a496208fe4 85b083b431c6dab2dd4d6484fe0749ab4acba50842591292fdb40e14ce19d097 cb765467dd9948aa0bfff18214ddec9e993a141a5fdd8750b451fd5b37b16341 f2168eca27fbee69f0c683d07c2c5051c8f3214f8841c05d48897a1a9e2b31f8 21708cea44e38d0ef3c608b25933349d54c35e392f7c668c28f3cf253f6f9db8 5405ff84473abccc5526310903fcc4f7ad79a03af9f509b6bca61f1db8793ee4
	Domains	jumpstartmail[.]com paydayloansnew[.]com picture-world[.]info salimafia[.]net seomoi[.]net
Nokoyawa	MD5	46168ed7dbe33ffc4179974f8bf401aa 1e4dd35b16ddc59c1ecf240c22b8a4c4 f23be19024fcc7c8f885dfa16634e6e7 A2313d7fdb2f8f5e5c1962e22b504a17 8800e6f1501f69a0a04ce709e9fa251c
	Domains	vnssinc[.]com qooqle[.]top vsexec[.]com devsetgroup[.]com
CHM	Hostname	msdata[.]ddns[.]net bluelotus[.]mail-gdrive[.]com
	URLs	hXXps://coauthcn[.]com/hbz[.]php?id=%computername% hXXps://bluelotus[.]mail-gdrive[.]com/Services[.]msi hXXp://msdata[.]ddns[.]net:443
	SHA256	cd3effd25629ab9c440ed8bedb9bfb312c73a022cad5078684784ea07eff2c68 43c8ada7cb7c046893dd96aef195856ec94f62823ca1a2987adf31899788c92d
	SHA1	365203360046573682932 69d72dfc535f30fd8a619875ccc639e103e9045bbc71f4a5ce44433d1c0
	MD5	a7e8d75eae4f1cb343745d9dd394a154

Attack Name	TYPE	VALUE
Trigona	MD5	1cece45e368656d322b68467ad1b8c02 530967fb3b7d9427552e4ac181a37b9a 1e71a0bb69803a2ca902397e08269302 46b639d59fea86c21e5c4b05b3e29617 5db23a2c723cbceabec8d5e545302dc4
	Website	hxxp://3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion/
Havoc Demon	SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328 b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c
	URLs	hxxps://ukrtatnafta[.]org hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/avias.js hxxps://ukrtatnafta[.]org/wpcontent/themes/pressa/js/mobile_menu.js hxxps://ukrtatnafta[.]org/wp-content/plugins/contact-form-7/includes/js/scripts.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/bootstrap.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/hovermenu.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/retina1.1.0.js hxxps://ukrtatnafta[.]org/wpcontent/plugins/js_composer/assets/lib/bower/isotope/dist/isotope.pkgd.min.js hxxps://ukrtatnafta[.]org/wp-content/themes/pressa/js/custom-script.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-emoji-release.min.js hxxps://ukrtatnafta[.]org/maps-api-v3/api/js/52/1/intl/uk_ALL/util.js hxxps://ukrtatnafta[.]org/wp-includes/js/wp-embed.min.js
Rilide	Domains	nvidia-graphics[.]top nch-software[.]info 45[.]15[.]156[.]210 vceilinichego[.]ru ashgrrwt[.]click

Attack Name	TYPE	VALUE
Rilide	Wallet Address	bc1qkczacyp5jq29s5kaphth4asu8cv2y4u4gdgj7q bc1qsjg8dqx6ga30h6szjd8dv2wg50ch50qrey4t7j 0xDBc1330056E2F5e2FB11FB3C96dE2c44B313eA8d 1KqequymujeNJuyB4gH7oJSFTB3En3Hf5n LRYpzmnqBVozkbzJhTWndzYDPfjmNPyaLv rUPTadzFN6LS662Z2d2AvNyqU1xwg2japJ THiD8hFLiEyULVKLp3DSbBXQSbR3MQxm4X D5asYfjtbTtFmFkrEwqVgbJKYv9YT7Tgjh
	MD5	558104b26ccadec3d3eb2925113387a6 c28a180de1f80c8c98d0904e64142bef 1baaeedd1a26edf4fa79ded370e3d19a 0a4f321c903a7fbc59566918c12aca09 561797d7e5cf956e33735180d93be5b6 766d020e902b6470d0510e5c6cfcd6e8 d9cca3dd5bdaeb0466d52821b584602b 9e5f43b2dc1606e27fa0cfdfb4e363d2 740606987f4d588c89d0a5b68648e31e 1c54dd00bc7cc52b60ad4a46e2fb3a77 d54fa225b07298ec34be872cd4ebf4ae baee9ba0b94ea1e2b2e566fc8a615554 99dc4073f2fe91f48fd16bc65e7dcbc2 2cc204564b68c5a98b1ff68d861b66c5 646b9404a29febe9f3741797b79e300c 253f4319673673d2bf5285558a6903df 50e363409ba77b20fb6f0bce4eff7b1 c1f40584e4ac391d97218ce137a63fb3 ebce63fdc8ef245f117f06ada3ba0f6d 4abe60d2c3506f4767e163d135f89f92 b85c5659e946b5d7ad78410356288928 ff4e2df1a46d49862ab2a0af830a007e c0e120778853f0a4865e006a07cd728a
	SHA1	add0d61399c8c47f8ac73dc83cc83dfa31cddeca 415d790b54ca8e374f37fdbb00090110b823ba18 ec6de82efa93e59da148f4d696efcfca851e051e 2449e4b27d778f6a4ffc00bb7b73926ac2c54e8a 0ead1d32ce6b15c4a90373fce58d1554035cd40f 39f546a4ec94e63e603e3c2481fecab2b5e8a475 61acdad59223a9eb0b392ccd085db1e49700d65 28ae2440c56350f65b607e4e99b67a2632db873b 05536aa80f8280ddc31be5c0ac3ca995f2190a0a f689396c73055e99a06e002c39e3a74d3d402607 84db08e3dcbe40c7cbc998a77788f7303d4a2905 0cb1d9c2a3c8b776ef1e3ec1316fbf595ced7863 eafdc35b233600ef552b87e684faa3ab3396eae9

Attack Name	TYPE	VALUE
Rilide	SHA1	5012e783b2ee29cb40b04a10d1a40d0bfda683d9 a46586bfe22f4d84cd9174238740af275bf50c69 ffebf78a9692293a23f9a477ea8a79f7f6ef5aa2 a39d252e7927ae1adf518e6a3dd08f37e7ee7c26 70167e7e5d71fba7d92796324b488c0fb9727712 25f3fb6d2dab206a5e9b2c0ef26ec6d6a56c5767 b4b918a5898463dad1c7d823e0b3f828bac15aad abaaa2644b1e84e8b39119988dd711572377c839 b1c100d5a99ae34ccb3654c7b7f8573376a44fd9 E049f56198c23d86e9083142bfe80042e21d4b8e
	SHA256	0e31ff6406b03982581246b7dd60f3b96edcf0bd007b317669 54df001fd68f69 e623984143e0dc6e35c79869ab1521c6714e588e8e6486064 96f8372ca0d8416 ebd72806abd354f3162eec0991d127f993a5dde1a0c719b470 87c9ee0edefeaf 0f11aeecbde1f355d26c9d406dad80cb0ae8536aea31fdddaf9 15d4afd434f3f 8342b134cddeaf34ce05bafa9e860dacf6cd01b85fd00147d90 a350516c055e5 4cc83be0fa496855d244050616ee2e86b044a9bc87bc5ca70b 305986c1ba3bb8 55251c725e9f6f51b8db7a631b54dd85b1b59d644c3219e03c effb0c49cd00a4 1b01c3e554700e1282c7fdd2dcb54314516ee1f0c5eef3560cd babc1ba776293 a28c623d120a76dcfeef9504eaeefabac9d33f292576ccf012fa 458b8d7bc6ef 8989f4244667626728c6c0083422ff714cb622c92c35a53f9cb 1e9891f4528ff 170a13a7a8757336babe857804fa24b6cb20aaa9593b32546d 7151f23095a510 bb57a504e0b821552344cecb3da9ecdd0d61817264617a491 7d6f5e64a1df7e5 d70e933e10e667ae7ef6e68a625c447be8aabe9b29affdad99 9c969bd8769003 c8939f8d6237fcc17d486981a800b1e7e9974377de21d7e766 77babe8ed536af 2e310391d77022bcc708c354140319718777ca35efdfb76d6c 80cb9de8c8091e 4bbb0584eed0c082b5c43d3f259f37cf1a0b64eabb485e8509 0951a6566d98d4 9dca66f52f31dca921fb238bd36bfc1b1a59d3e4af7b071da9b c4c6bf294e402

Attack Name	TYPE	VALUE
Rilide	SHA256	4df0f18a7e05518bbe93758e751f1f462fef212cdc786c7217d50ddbda14efb5 ef20c929f5204b223b6e53dc406ea0bcd76d9e98c9ae4942037902883d4bb22a e1ad66cc0244fc075e0aabe0fd19502d4c9617829b90aa210e74be1d915275d2 a7f0fdfdfdf1ef65799fd2114bf5c1e133a8b7635b498b334553fbb64b218a05 68278b40b59b1b0db2f814d2d864f0b9c2b4285f5795d22cabf60715f922989c 2f947644c7752ba014eae7971b247be60249a6088923c66ffe9886a7f5c5fe1c
Kadavro Vector Ransomware	SHA256	8dc6ff90357e8e2d598bebe3240cefabe22054036ec2e2e91377c7125f8f8b89,39308dee3ad1f5ce7ccc3d52b3783db204d12694d6c00ec7ec301ecb73e7c8b6,b30ef4dbcc89cd4bf0da3e7787f43e42023ddc2b5f0bb4f24937538e10e17533,b7ca2dde7789da13d1b8729cc2ef3d5dc596cbd710a06c17ff6eb4ef2d9d1182,124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969
	Pastebin Address	124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969
Crimson RAT	Domains	richa-sharma.ddns[.]net cloud-drive[.]store drive-phone[.]online s1.fileditch[.]ch
	SHA1	738d31ceca78ffd053403d3b2bc15847682899a09ed39c6a3faab057e6c962f0b2aaab07728c5555 af6608755e2708335dc80961a9e634f870aecf3c e000596ad65b2427d7af3313e5748c2e7f37fba7 fd46411b315beb36926877e4b021721fcd111d7a

Attack Name	TYPE	VALUE
Crimson RAT	SHA1	516db7998e3bf46858352697c1f103ef456f2e8e 842f55579db786e46b20f7a7053861170e1c0c5e 87e0ea08713a746d53bef7fb04632bfcd6717fa9 911226d78918b303df5110704a8c8bb599bcd403 973cb3afc7eb47801ff5d2487d2734ada6b4056f
Zaraza bot	MD5	41D5FDA21CF991734793DF190FF078BA
	SHA1	b50a8e2a7998e17286d2e18d1cf3f7e4e84482c6
	SHA256	2cb42e07dbdfb0227213c50af87b2594ce96889fe623dbd73d 228e46572f0125
Dave Loader	SHA256	de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba 618252585923a, b14ab379ff43c7382c1aa881b2be39275c1594954746ef58f6a 9a3535e8dc1a8, dbdfc3ca5afa186c1a9a9c03129773f7bc17fb7988fe0ca40fc3c 5bedb201978, ce99b4c0d75811ce70610d39b1007f99560e6dea887a451e08 916a4f8cf33678
Domino Backdoor	IPV4	88.119.175[.]124 94.158.247[.]72 185.225.17[.]202 5.182.37[.]118
	URLs	hxxp://170.130.55[.]250/x64.exe hxxps://upperdunk[.]com/mr64.exe
	SHA256	de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba 618252585923a,b14ab379ff43c7382c1aa881b2be39275c159 4954746ef58f6a9a3535e8dc1a8,dbdfc3ca5afa186c1a9a9c03 129773f7bc17fb7988fe0ca40fc3c5bedb201978,ce99b4c0d75 811ce70610d39b1007f99560e6dea887a451e08916a4f8cf33 678,f4ebd59fb578a0184abf6870fc652210d63e078a35dace0 a48c5f273e417c13d,92651f9418625e5281b84cccb817e94e6 294b36c949b00fcd4046770b87f10e4,e5af0b9f4650dc0193c9 884507e6202b04bb87ac5ed261be3f4ecfa3b6911af8
NewWorldOrder Loader	SHA256	f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b5 0f40712dd37cb,51e0512a54640be8e3477363c8d72d893c6e dd20399bddf71e95eec3ddfdb42e,f4ebd59fb578a0184abf68 70fc652210d63e078a35dace0a48c5f273e417c13d,92651f94 18625e5281b84cccb817e94e6294b36c949b00fcd4046770b8 7f10e4
Carbanak Backdoor	IPV4	178.23.190[.]73
	SHA256	f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b5 0f40712dd37cb,51e0512a54640be8e3477363c8d72d893c6e dd20399bddf71e95eec3ddfdb42e

Attack Name	TYPE	VALUE
Project Nemesis infostealer	IPV4	45.67.34[.]236
	Domain	es-megadom[.]com
LockBit Ransomware	SHA1	2d15286d25f0e0938823dcd742bc928e78199b3d, 864f56b25a34e9532a1175d469715d2f61c56f7f, ef958f3cf201f9323ceae9663d86464021f8e10d
QBot (also known as QakBot, QuackBot, and Pinkslipbot)	MD5	253e43124f66f4faf23f9671bbba3d98 39fd8e69eb4ca6da43b3be015c2d8b7d 299fc65a2eecf5b9ef06f167575cc9e2 a6120562eb673552a61f7eeb577c05f8 1fbfe5c1cd26c536fc87c46b46db754d fd57b3c5d73a4ecd03df67ba2e48f661 28c25753f1ecd5c47d316394c7fcede2
	Domain	cica.com[.]co/stai/stai.php abhishekmeena[.]in/ducs/ducs.php rosewoodlaminates[.]com/hea/yWY9SJ4VOH agtendelperu[.]com/FPu0Fa/EpN5Xvh capitalperurrhh[.]com/vQ1iQg/u6oL8xlJ centerkick[.]com/IC5EQ8/2v6u6vKQwk8 chimpcity[.]com/h7e/p5FuepRZjx graficalevi.com[.]br/0p6P/R94icuyQ kmphi[.]com/FWovmB/8oZ0BOV5HqEX propertynear.co[.]uk/QyYWyp/XRgRWEdFv theshirtsummit[.]com/MwBGSm/lGP5mGh
CrossLock	MD5	9756b1c7d0001100fdde3efefb7e086f
	SHA1	55de88118fe8abefb29dec765df7f78785908621
	SHA256	495fbfecbcadb103389cc33828db139fa6d66bece479c7f7027 9834051412d72
EvilExtractor	IPV4	45[.]87[.]81[.]184 193[.]42[.]33[.]232
	Domain	evilextractor[.]com
	SHA256	352efd1645982b8d23a841107007c8b4b024eb6bb5d6b312e 5783ce4aa62b685 023548a5ce0de9f8b748a2fd8c4d1ae6c924c40acbde32e9599 c868115d11f4e 75688c32a3c1f04df0fc02491180c8079d7fdc0babed981f5860 f22f5e118a5e 826c7c112dd1ae80469ef81f5066003d7691a349e6234c8f8ca 9637b0984fc45 b1ef1654839b73f03b73c4ef4e20ce4ecdef2236ec6e1ca3688 1438bc1758dcd 17672795fb0c8df81ab33f5403e0e8ed15f4b2ac1e8ac9fef1fec 4928387a36d

Attack Name	TYPE	VALUE
MgBot	SHA256	c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab 90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe 706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36 017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7 cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a 2dcf9e556332da2a17a44dfceda5e2421c88168aafea73e2811d65e9521c715c a6ed16244a5b965f0e0b84b21dcc6f51ad1e413dc2ad243a6f5853cd9ac8da0b ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024 585db6ab2f7b452091ddb29de519485027665335afcdb34957ff1425ecc3ec4b 29df6c3f7d13b259b3bc5d56f2cdd14782021fc5f9597a3ccece51ffac2010a0 ea2be3d0217a2efeb06c93e32f489a457bdea154fb4a900f26bef83e2053f4fd 54198678b98c2094e74159d7456dd74d12ab4244e1d9376d8f4d864f6237cd79 d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934 cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5 2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc a16a70b0a1ac0718149a31c780edb126379a0d375d9f6007a6def3141bec6810 0bcdcc0515d30c28017fd7931b8a787feebe9ee3819aa2b758ce915b8ba40f99 C31b409b1fe9b6387b03f7aedeafd3721b4ec6d6011da671df49e241394da154 db489e9760da2ed362476c4e0e9ddd6e275a84391542a6966dbcda0261b3f30a 632cd9067fb32ac8fbbe93eb134e58bd99601c8690f97ca53e8e17dda5d44e0e C1e91a5f9cc23f3626326dab2dcdf4904e6f8a332e2bce8b9a0854b371c2b35 5a0976fef89e32ddcf62c790f9bb4c174a79004e627c3521604f46bf5cc7bea2 7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453 3f75818e2e43a744980254bfdc1225e7743689b378081c560e824a36e0e0a195

Attack Name	TYPE	VALUE
MgBot	SHA256	1b8500e27edc87464b8e5786dc8c2beed9a8c6e58b82e50280cebb7f233bcde4 03bc62bd9a681bdcb85db33a08b6f2b41f853de84aa237ae7216432a6f8f817e ae39ced76c78e7c2043b813718e3cd610e1a8adac1f9ad5e69cf06bd6e38a5bd f6f6152db941a03e1f45d52ab55a2e3d774015ccb8828533654e3f3161cfcd21 2f4a97dc70f06e0235796fec6393579999c224e144adcff908e0c681c123a8a2 22069984cba22be84fe33a886d989b683de6eb09f001670dbd8c1b605460d454 7b945fb1bdeb27a35fab7c2e0f5f45e0e64df7821dd1417a77922c9b08acfdc3 e8be3e40f79981a1c29c15992da116ea969ab5a15dc514479871a50b20b10158 b5c46c2604e29e24c6eb373a7287d919da5c18c04572021f20b8e1966b86d585 53d2506723f4d69afca33e90142833b132ed11dd0766192a087cb206840f3692 26d129aaa4f0f830a7a20fe6317ee4a254b9caac52730b6fed6c482be4a5c79d b45355c8b84b57ae015ad0aebfa8707be3f33e12731f7f8c282c8ee51f962292 17dce65529069529bcb5ced04721d641bf6d7a7ac61d43aaf1bca2f6e08ead56 98b6992749819d0a34a196768c6c0d43b100ef754194308eae6aaa90352e2c13 6d5be3e6939a7c86280044eebe71c566b48981a3341193aa3aff634a3a5d1bbd 1cf04c3e8349171d907b911bc2a23bdb544d88e2f9b8fcc516d8bcf68168aede
BellaCiao	MD5	284cdf5d2b29369f0b35f3ceb363a3d1 2daa29f965f661405e13b2a10d859b87 3fbea74b92f41809f46145f480782ef9 5a487c41efa2f3055d641591d601977c 7df50cb7d4620621c2246535dd3ef10c 95c6fdc4f537bccca3079d94e65bc0b0 c450477ed9c347c4c3d7474e1f069f14 c6f394847eb3dc2587dc0c0130249337 e7149c402a37719168fb739c62f25585 f56a6da833289f821dd63f902a360c31
	SHA256	2aa1bbbe47f04627a8ea4e8718ad21f0d50adf6a32ba4e6133ee46ce2cd13780,Ca57391cdbac224f159e858425d231d068aa76316e0345cb8d58c716b9eff587

Attack Name	TYPE	VALUE
BellaCiao	SHA1	736ba9daf63a2add3217c79fa9d83088358f7012
	Domains	mail-updateservice[.]info maill-support[.]com mailupdate[.]com mailupdate[.]info msn-center[.]uk msn-service[.]co twittsupport[.]com
	IPV4	188[.]165[.]174[.]199 88[.]80[.]148[.]162
PingPull	SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae,5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507,e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253
	Domains	yrhsywu2009.zapto[.]org *.saspecialforces.co[.]za vpn729380678.softether[.]net
	IPV4	5.181.25[.]99 196.216.136[.]139
VEILEDSIGNAL	SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae,5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507,e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253
	URLs	hxxps[://]www.tradingtechnologies[.]com/trading/order-management
RustBucket	Domains	cloud[.]dnx[.]capital deck[.]31ventures[.]info
	File Path	/Users/Shared/Internal PDF Viewer.app
	SHA1	dabb4372050264f389b8adcf239366860662ac520be69bb9836b2a266bfd9a8b93bb412b6e4ce1bee0e42ac374443500c236721341612865cd3d1eecac08406818bbf4fe24ea04bfd72f747c89174bdb72167ec09d62cdfb04698c3f96a6131dceb24a9cfd1cef5abe3e0c275671916a1f3a566f13489416ca59874172660e6180af2815c3a42c85169aa0b2d9f1392fb7ed010a0ecc4f819782c179efde96879121509d674091ce1f5f30e9a372b5dcf9bcd257a1a85cba1bc4ac9f6eafc548b1454f57b4dff7e07a5d57c7e2b0c8ab7d60f7a7c7f4649f33fea8aa182760cbe11fa0316abfb8b7b00b63f83159f5aa7e69cb4f9c37fad13de85e91b5a05a816d14f490

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

May 03, 2023 . 05:00 AM

More at www.hivepro.com