Date of Publication
September 4, 2023

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

AUGUST 2023

Table Of Contents

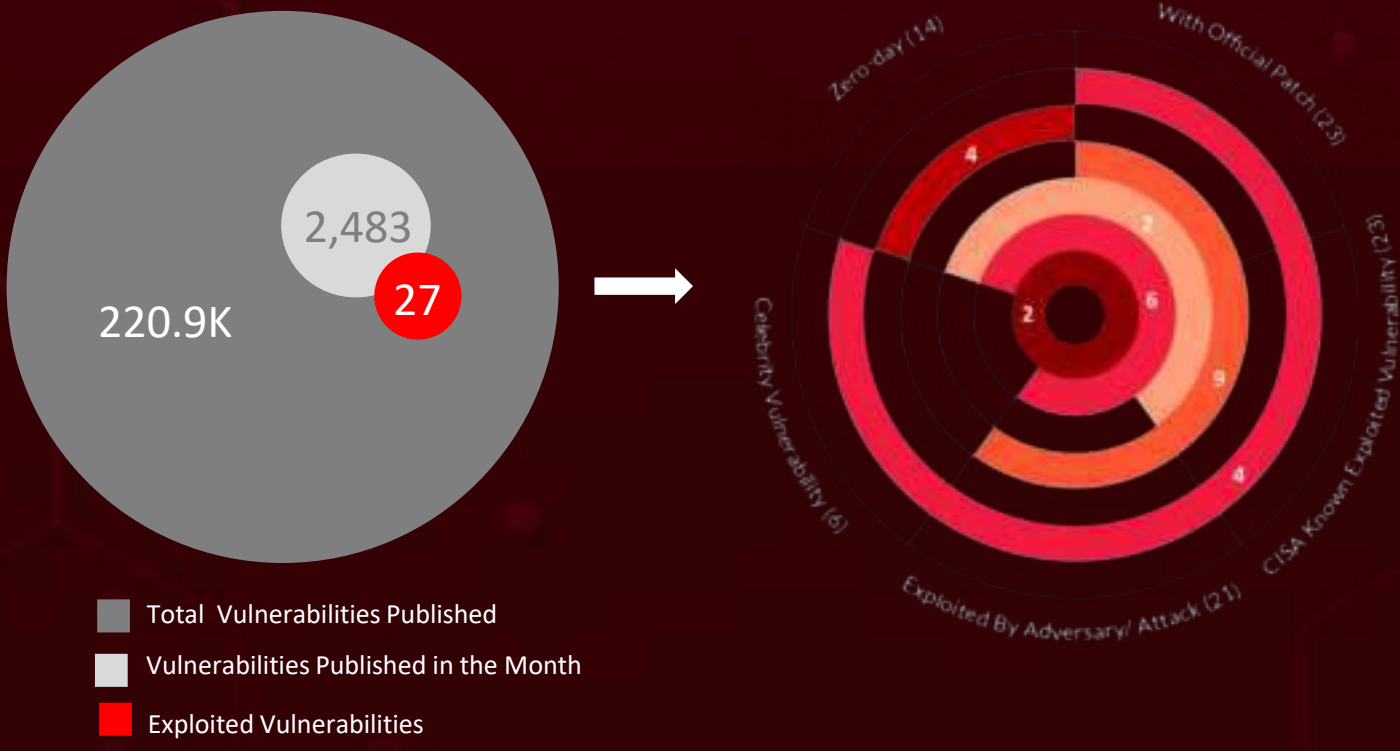
Summary

In **August**, the discovery of **thirteen zero-day** vulnerabilities drew significant attention from the cybersecurity community. One of these vulnerabilities was exploited by the **Storm-0978 group**, leading to sense of urgency among security teams to patch their systems.

The month of August saw a rise in ransomware attacks, with various strains such as **Cuba**, **Akira**, **TargetCompany**, **Yashma**, **WannaCry**, **LOLKEK**, **Monti**, **Rhysida**, and **Scarab** 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 a five year old vulnerability (**CVE-2017-18368**) in Zyxel P660HN-T1A router allowing the **Gafgyt Botnet** to execute unauthorized commands, potentially leading to complete takeover of affected devices. In addition to ransomware attacks, several malware families, including **Rilide Stealer**, **STRRAT**, **Reptile**, **DroxiDat**, **PlugX**, **DarkMe**, **GuLoader**, and **Remcos RAT**were observed widely targeting victims. These malware families are designed to steal sensitive data, disrupt systems, and evade detection by security tools.

Lastly, the **CVE-2023-38831** vulnerability is a high-severity zero-day vulnerability that was found in WinRAR, allowing hackers to install malware through manipulated archives, exposing users to hidden malicious scripts and potential cyberattacks.



Insights

Reptile

An open-source Linux rootkit, targeting South Korea and has Similarities with Mélofée malware

Flax Typhoon

Targets Taiwan, Southeast Asia, North America and Africa

Yashma ransomware

New Variant mimics WannaCry ransomware in new attack

APT 29

Russian threat actor targeting Microsoft Teams worldwide

Government, Healthcare, IT Services, Education, and **Manufacturing** were the most targeted sectors

73

vulnerabilities were patched during August Microsoft Patch Tuesday

UNC4841

Threat group has been actively exploiting the CVE-2023-2868 vulnerability

Agniane Stealer

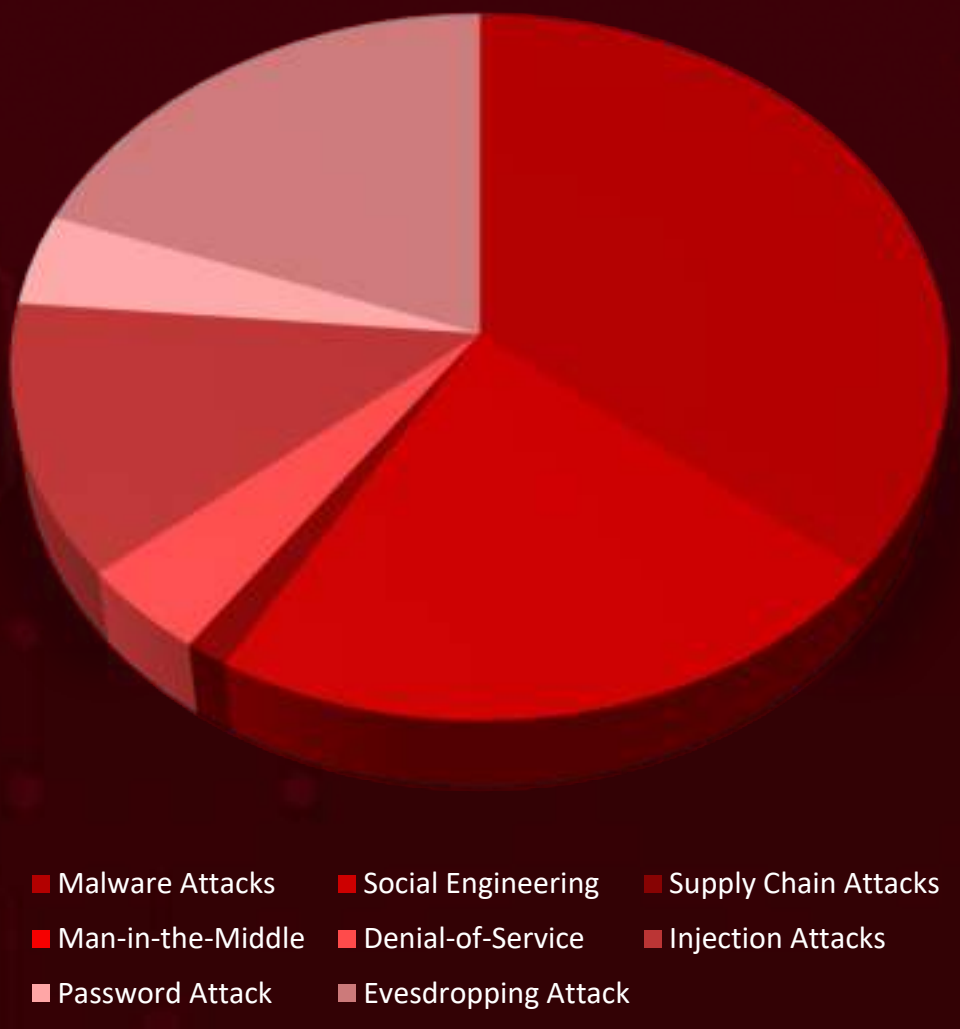
Written in C#, operates as an information pilferer, targeting cryptocurrency wallets

Singapore, Mexico, Brazil, Indonesia, and **Cuba,** were the most targeted countries

CVE-2023-35081

Ivanti second zero-day Path Traversal vulnerability in Ivanti Endpoint Manager Mobile(EPMM)

Threat Landscape



Celebrity Vulnerabilities

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Windows Server: 2008 – 2022, Windows: 7 - 11 21H2	APT28, FIN7, GoldenJackal APT, Asylum Ambuscade
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**ZERO-DAY**	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher, Lokibot, Woody RAT, Black Basta, NODEBOT, AHKBOT, SunSeed
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	✓	Apache Log4j2	Muddy Water, APT41, Lazarus, UNC961
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**ZERO-DAY**	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Prophet Spider, Muhstik botnet, Deep Panda, Enemybot, LockBit, MuddyWater, Monti ransomware, Budworm
Apache Log4j2 Remote Code Execution Vulnerability (LOG4J)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-917 CWE-20 CWE-400 CWE-502	T1059:Command and Scripting Interpreter	https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472		Microsoft Netlogon	Cadet Blizzard, APT15
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	WhisperGate, LockBit Ransomware, and Backdoor.Graphical
Microsoft Netlogon Privilege Escalation Vulnerability (ZEROLOGON)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-330	T1068: Exploitation for Privilege Escalation, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207		Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	ChamelGang, UNC2596, APT35, Cadet Blizzard APT
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	Blackbyte Ransomware, cuba ransomware, AvosLocker Ransomware, Hive Ransomware, LV Ransomware
Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523		Microsoft Exchange Server	UNC2596, APT35, Worok gang, Cadet Blizzard APT, ChamelGang
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	LockFile, Blackbyte, Cuba, AvosLocker, Hive, LV Ransomware, WhisperGate & ChamelDoH
Microsoft Exchange Server Privilege Escalation Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1204: User Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473		Microsoft Exchange Server	ChamelGang, Cadet Blizzard APT, UNC2596, APT35
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	WhisperGate & ChamelDoHBlackByte Ransomware, LV Ransomware, cuba ransomware, AvosLocker Ransomware, Hive Ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability (PROXYSHELL)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059:Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS	✗	✓	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	Zoho ManageEngine ADSelfService Plus	✓	✓	✓
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Server	✗	✓	✓
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability	VMware Workspace ONE Access	✗	✓	✓
CVE-2022-22960	VMware Multiple Products Privilege Escalation Vulnerability	VMware Workspace ONE Access	✗	✓	✓
CVE-2022-1388	F5 BIG-IP Missing Authentication Vulnerability	F5 BIG-IP	✗	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓
CVE-2023-38180	.NET and Visual Studio Denial of Service Vulnerability	.NET and Visual Studio	✓	✓	✓
CVE-2023-36884	Microsoft Office and Windows HTML Remote Code Execution Vulnerability	Microsoft Office and Windows	✓	✓	✓
CVE-2017-18368	Zyxel P660HN-T1A Routers Command Injection Vulnerability	Zyxel P660HN-T1A Routers	✗	✓	✓
CVE-2023-27532	Veeam Missing Authentication for Critical Function	Veeam Backup & Replication & Veeam Cloud Connect	✗	✓	✓
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability	Ivanti Sentry	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	WinRAR	✓	✓	✓
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine	✗	✓	✓
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Openfire	✗	✓	✓
CVE-2023-2868	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	Barracuda Networks ESG Appliance	✓	✓	✓
CVE-2023-35838	WireGuard Client Denial of Service Vulnerability	WireGuard Client	✓	✗	✗
CVE-2023-36673	Avira Phantom VPN DNS Spoofing Vulnerability	Avira Phantom VPN	✓	✗	✗
CVE-2023-36672	Clario VPN Plaintext Traffic Leakage Vulnerability	Clario VPN	✓	✗	✗
CVE-2023-36671	Clario VPN Traffic to The Real IP Address of The VPN Server Vulnerability	Clario VPN	✓	✗	✗

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Rilide Stealer	InfoStealer	-	Google Chrome, Microsoft Edge, Brave, and Opera	-	Phishing, Malicious Extensions
STRRAT	RAT	-	Chrome, Firefox, Internet Explorer, Outlook, Thunderbird, and Foxmail	-	Spam Emails
TargetCompany Ransomware (aka Mallox, Fargo, and Tohnichi)	Ransomware	-	-	-	Exploiting vulnerabilities in SQL servers
Remcos RAT	RAT	-	-	-	TargetCompany Ransomware
Yashma Ransomware	Ransomware	-	Windows	-	Exploiting vulnerabilities in the Windows OS
WannaCry Ransomware	Ransomware	-	Windows	-	Exploiting vulnerabilities in the Windows OS
Reptile	Rootkit	-	Linux	-	-
Mélofée	Rootkit	-	Linux	-	-
LOLKEK Ransomware (aka GlobeImposter)	Ransomware	-	Windows	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Rhysida Ransomware	Ransomware	-	-	-	Phishing
Gafgyt Botnet (aka Bashlite, Lizkebab, PinkSlip, Qbot, Torlus, and LizardStresser)	Botnet	CVE-2017-18368	Zyxel P660HN-T1A Routers		Exploiting Zyxel routers
DroxiDat	Backdoor	-	-	-	-
Cuba ransomware (aka Fidel, COLDDRAW)	Ransomware	CVE-2023-27532 CVE-2020-1472	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon		Compromised administrative credentials via Remote Desktop Protocol
BUGHATCH	Loader	CVE-2023-27532 CVE-2020-1472	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon		PowerShell dropper
BURNTCIGAR	Rootkit	CVE-2023-27532 CVE-2020-1472	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon		-
Akira Ransomware	Ransomware	-	Windows, Linux, macOS and VMware	-	Cisco VPN products
PlugX (aka Korplug)	Backdoor	-	-	-	EsafeNet Cobra DocGuard Client
DarkMe	Trojan	CVE-2023-38831	RARLAB WinRAR		Exploiting zero-day vulnerability in WinRAR

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
GuLoader (aka CloudEye)	Loader	CVE-2023-38831	RARLAB WinRAR	✓	Exploiting zero-day vulnerability in WinRAR
Remcos RAT(aka: Remcos, Remvio, Socmer)	RAT	CVE-2023-38831	RARLAB WinRAR	✓	Exploiting zero-day vulnerability in WinRAR
Scarab Ransomware	Ransomware	CVE-2020-1472	Microsoft Netlogon	✓	Exploiting Zerologon Vulnerability
Spacecolon	Toolkit	CVE-2020-1472	Microsoft Netlogon	✓	Exploiting Zerologon Vulnerability
QuiteRAT	RAT	CVE-2022-47966	Zoho ManageEngine	✓	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus
CollectionRAT	RAT	CVE-2022-47966	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus	✓	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus
Trash Panda ransomware	Ransomware	-	Windows	-	Phishing emails
Agniane Stealer	InfoStealer	-	-	-	Phishing Emails
DEPTHCHARGE (aka SUBMARINE)	Backdoor	CVE-2023-2868	Barracuda Networks Email Security Gateway (ESG) Appliance	✓	Exploitation of CVE-2023-2868

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SKIPJACK	Backdoor	CVE-2023-2868	Barracuda Networks Email Security Gateway (ESG) Appliance		Exploitation of CVE-2023-2868
FOXTROT	Trojan	CVE-2023-2868	Barracuda Networks Email Security Gateway (ESG) Appliance		Exploitation of CVE-2023-2868
FOXTGLOVE	Trojan	CVE-2023-2868	Barracuda Networks Email Security Gateway (ESG) Appliance		Exploitation of CVE-2023-2868

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT 29 (aka Midnight Blizzard, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)	Information theft and espionage	Russia	-	-	Windows
Winnti Group (Blackfly, APT41, Wicked Panda)	Information theft and espionage	China	-	Reptile and Mélofée	Linux
UNC3886	Financial Crime	China	-	Reptile and Mélofée	Linux
RomCom (Storm-0978, DEV-0978)	Espionage	Russia	CVE-2023-36884	-	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019
Carderbee	Financial Crime	-	-	PlugX (aka Korplug)	-

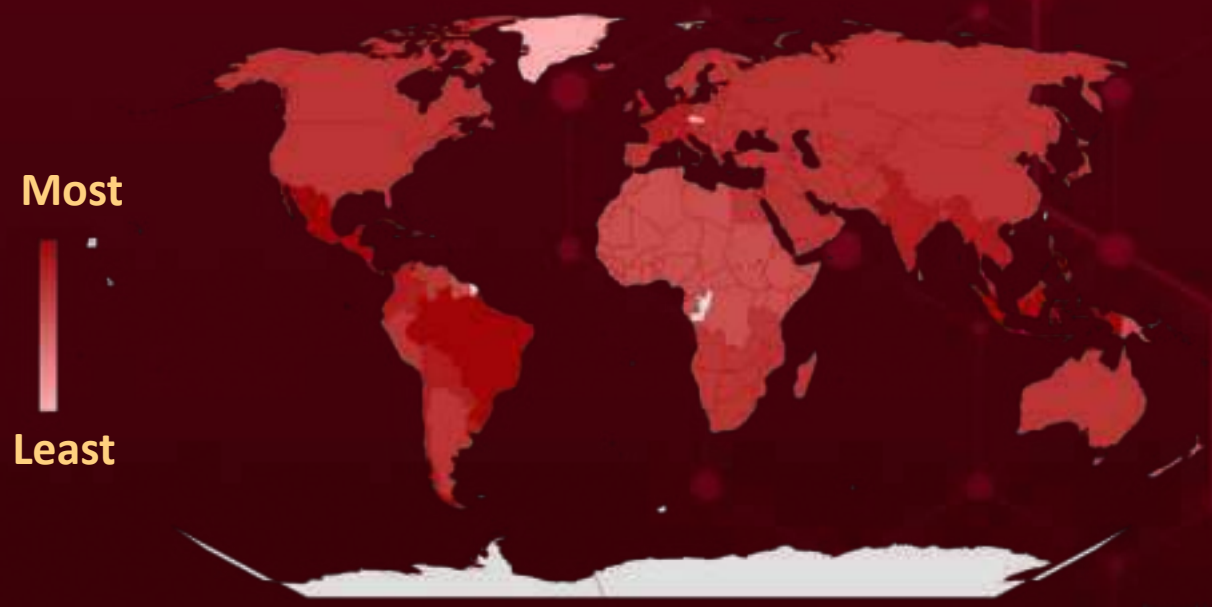
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
CosmicBeetle	Financial gains	-	CVE-2020-1472	Scarab Ransomware, Spacecolon	Microsoft Netlogon
Lazarus Group (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, Diamond Sleet)	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2022-47966	QuiteRAT, CollectionRAT	Zoho ManageEngine
Flax Typhoon	Espionage	China	-	-	Windows
UNC4841	Information theft and espionage	China	CVE-2023-2868	DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE	Barracuda Networks Email Security Gateway (ESG) Appliance
Bronze Starlight (aka DEV-0401, Cinnamon Tempest, SLIME34, Emperor Dragonfly)	Information theft and espionage	China	-	-	Windows, Linux, macOS

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
ZOHO	ManageEngine	Zoho ManageEngine ADSelfService Plus: 6000 -6113
ivanti	Mobile device management (MDM) and application management (MAM) solution	Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3
	Enified endpoint management	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions
ATLASSIAN	Server	Atlassian Confluence Server: 6.0.1 - 7.12.4; Atlassian Confluence Server: 5.0 - 7.18.0 Jira Data Center: 6.0.0 - 8.22.3
LOG4J	login utility	Apache Log4j: 2.0 - 2.14.1
FORTINET	Operating System	FortiOS: 5.6.3 - 6.0.4
vmware	Workspace	VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1
f5	Security solutions	BIG-IP: 11.6.1 - 16.1.2.1
	IDE	.NET: 6.0.0 - 7.0.9, Visual Studio: 17.2.0 17.2.32505.173 - 17.6.5 17.6.33829.357, ASP.NET Core: before 2.1.40

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
Microsoft	Microsoft Exchange Server	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2013 Cumulative Update 23 15.00.1497.002; 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005
	Windows Server	Windows Server: 2008 – 2022, Windows: 7 - 11 21H2, Windows Server: 2008 - 2022 20H2
	Operating System	Windows: 10 - 11 22H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019
ZYXEL	Router	Zyxel P660HN-T1A Routers
	VPN	Wireguard Client 0.5.3 on Windows
AVIRA	VPN	Avira Phantom VPN through 2.23.1 for macOS
CLARIO.	VPN	Clario VPN client through 5.9.1.1662 for macOS
Barracuda	Email Security Gateway	Barracuda Networks Email Security Gateway (ESG): 5.1.3 - 9.2.0.008
openfire	Openfire	Openfire versions: 3.10.0 - 4.7.4
	File compression and archive utility	WinRAR version 6.22 and older versions
VEEAM	Data protection and backup solutions	Veeam Backup & Replication & Veeam Cloud Connect

Targeted Countries



Color	Countries
	Haiti
	Panama
	Mexico
	Brazil
	South Korea
	Costa Rica
	Indonesia
	Cuba
	Nicaragua
	Dominican Republic
	Singapore
	El Salvador
	Guatemala
	Honduras
	Myanmar
	Thailand
	Paraguay
	Germany
	Belize
	Cambodia
	Bolivia
	Chile
	Ecuador

Color	Countries
	United Kingdom
	Malaysia
	Uruguay
	Monaco
	Colombia
	Netherlands
	Ireland
	Belgium
	Israel
	Philippines
	Italy
	Brunei
	Jamaica
	France
	Luxembourg
	Vietnam
	India
	Laos
	Saint Lucia
	Azerbaijan
	Bangladesh
	Finland
	Cyprus

Color	Countries
	Belarus
	Bahrain
	Georgia
	United States
	Albania
	Norway
	Greece
	Portugal
	Grenada
	Dominica
	Andorra
	Switzerland
	Bhutan
	Turkmenistan
	Angola
	Estonia
	Hungary
	North Korea
	Iceland
	Pakistan
	Bosnia and Herzegovina
	Denmark
	Botswana
	Romania
	Iran

Color	Countries
	Moldova
	Turkey
	Saudi Arabia
	Iraq
	Slovenia
	Antigua and Barbuda
	Sri Lanka
	Argentina
	Tajikistan
	Bulgaria
	Trinidad and Tobago
	Armenia
	United Arab Emirates
	Japan
	Uzbekistan
	Jordan
	Eswatini
	Kazakhstan
	Croatia
	Kuwait
	North Macedonia

Color	Countries
	Kyrgyzstan
	Oman
	Bahamas
	Zimbabwe
	Peru
	Lebanon
	Poland
	Lesotho
	Qatar
	Liechtenstein
	Russia
	Afghanistan
	San Marino
	Canada
	Serbia
	Madagascar
	Slovakia
	Malawi
	South Africa
	Australia
	Spain
	Maldives
	Sweden
	China

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1068 Exploitation for Privilege Escalation	**T1059** Command and Scripting Interpreter	**T1083** File and Directory Discovery	**T1082** System Information Discovery	**T1027** Obfuscated Files or Information
T1190 Exploit Public-Facing Application	**T1140** Deobfuscate/ Decode Files or Information	**T1055** Process Injection	**T1486** Data Encrypted for Impact	**T1566** Phishing
T1071 Application Layer Protocol	**T1547.001** Registry Run Keys / Startup Folder	**T1203** Exploitation for Client Execution	**T1036** Masqueradin g	**T1588** Obtain Capabilities
T1588.005 Exploits	**T1095** Non-Application Layer Protocol	**T1059.001** PowerShell	**T1497** Virtualization /Sandbox Evasion	**T1005** Data from Local System
T1562.001 Disable or Modify Tools	**T1105** Ingress Tool Transfer	**T1574** Hijack Execution Flow	**T1016** System Network Configuration Discovery	**T1547** Boot or Logon Autostart Execution

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Yashma Ransomware	SHA1	367411a1e2efde7eb9d39de66be90a96012d5d7b
	SHA256	3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac, de68f4bce05a856ad949e6fb1738559fc506d491d4f6227553695aa9558b64be
	Hostname	www.fxxz[.]com
WannaCry Ransomware	SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa, 74d72f5f488bd3c2e28322c8997d44ac61ee3ccc49b7c42220472633af95c0c0, 994b41a5d3b6d031d9256ed757da213829c7345580819ae574c21eda19ae29db, 4a45fba2077320cbe23c36a025dc37006f73aa97b57abf8404e6c72e7223f0c8, 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Gafgyt Botnet	SHA256	21ecc53c3fe5336dd717b50fa70e281c5612b0c770f68d9f38c93e13e8357e21, 08d221d2d98a81d85e8bf0e8f3c8c4ddb35cc32c268a2cfe2cb2837e7f8fc731, e1cb8cf85745f7a771b33eab060e04556b1b33d186a65ae069377668fcea47b7, 9fea55b5dd337dcd5c00f4b9c1a09ad2ed5cb7f2c69dc21a7f50f55af0809f89, 06ad76f4b19be8706f98441d926142af824bd2983217f6c2c02201dbb07d0224, 2481e420138bb0bcc52d43a127e76887cc7419ac46e7495f55493d7fccbbec1b, fc76a4046efbaaab93261806f52afcd6cdf88c2784ec2ed7e862089f3d6bbbb8, 8131b5119e869e1ebf7ebce50837f12fa86fa24008d5534b757c23e91e8f401f, 20770419f79550e46c9bdc2dab792cc96792b7ec4dbd8fcc0cedd7c726ae7987, b8baa7b5d0d60070ef78ad846e17198e891093a84a00e3029dad0ffd77c78b7a, 4f6d665fa107ba9d7313ff6bf1527dddf18bcf178ae34c0e573b3afcb52d685f,

Attack Name	TYPE	VALUE
Gafgyt Botnet	SHA256	b14eb9596f91c1625c3df29413fa08ba313a6b9e6d7fb1297fba74761c135568, a908289bef30086660453ab8809af758af3d445ecda4010211282eb067fef3ab, 9db1a5e089a0b16b3b9a584cb3e5e55eb68620d0ab6b229cf24d49f32b9391be, 94797cd702cf50fea6d780ab0d94cb2a0aa8ee9aa5332e71479adaa7a5245f27, 8ef658a73b292410dd6a570bc65a0f398e838b5adb141eb9dc81ad124fb46f80,
LummaC Stealer	MD5	507bddfabd74a3d024b2ad5f67d666ea
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock
Monti Ransomware	SHA1	f1c0054bc76e8753d4331a881cdf9156dd8b812a, a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef
	URLs	hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion, hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion

Attack Name	TYPE	VALUE
HUI Loader	MD5	b16bb2f910f21e2d4f6e2aa1a1ea0d8b, 809fcab1225981e87060033d72edaeaf
	SH1	a75e9b702a892cc3e531e158ab2e4206b939f379, 64f5044709efc77230484cec8a0d784947056022
	SHA256	8502852561fcb867d9cbf45ac24c5985fa195432 b542dbf8753d5f3d7175b120, 62fea3942e884855283faf3fb68f41be747c5baa 922d140509237c2d7bacdd17
Cuba Ransomware	SHA256	8a8cb6bd09ef535bfa09bee2678e0c75a0216b0cebd8fda5c9a 6f9735822e329, c6753d4cfe9072acce9c0a6fc84a15bd582d66d5e0a3a65c36c 6a3ba05b80a65, 7af49e468b3b2cc75b25ebcd711294373714585dca56196ed0 8430ba2fc849bd, 20c596d73812a9e9798e56cd6857451cad4686ed9212a4008 7d5a9fd9ab2532, a059ec5278a63614d358a743774bfb380dea1b370d9896104 9e6ba0ed754b234, 0910d1d5d0efa08c295f777551ec787511ab7625f0d08fed6d0 a5c9d6d6b963e, 65a60352271ce7ee4934967173ab68896726fe8e922e39fd2a 399d468657d2a5, 1cde997078f553ab9dbb0d94f948a26fbf4d3d3a20e801677d8 8daeb1dfb9e66, 81a22a4224f71bd66a89f2778b5842957b313ee5593c7c3e42 8d7a22507cda67
PlugX	SHA256	041d8c3460ce0b25dc6b597a69cbe0bc95f9f281bb66e4cbcd0 45ea69e308777, 10e60613394aa48b99b5bbaa13df6d5209912e64612e8dd2d 09d24546e09d74f, 8649235c0c4deecabf319fb0b7e4842bdac75baa221973bf9f0 95114c3cbb252, 8978af4528721d4e1178ab36f7d90bc5d5206610178d5491fd 58105c8eaf0448, 995664972e499c9ff036241dca05d03d902916d9c5c126f27d2 3403288cf8144, b2f005fc3eeff7ba5f8adac02705ad271381ac1a296e716da0a8 eccf13161362, 03c559361d21802ea29a2803584af1bf41ced2989cdddec694 995ae193622e10

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35081		Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-22	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379		FortiOS: 5.6.3 - 6.0.4	MuddyWater, APT29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Conti Ransomware, LockBit Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://fortiguard.com/advisory/FG-IR-18-384

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26084		Atlassian Confluence Server: 6.0.1 - 7.12.4	UNC961, Cadet Blizzard APT
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	Cerber Ransomware, Muhstik botnet
Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-174	T1055: Process Injection	https://jira.atlassian.com/browse/CONFSERVER-67940

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40539		Zoho ManageEngine ADSelfService Plus: 6000 -6113	APT27, Volt Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:-:*:*:*:*:*:*:*	-
Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22954		VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	Rocket Kitten
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:identity_manager:-:*:*:*:*:*:*:*	Enemybot
VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1221: Template Injection	https://www.vmware.com/security/advisories/VMSA-2022-0011.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22960		VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	-
VMware Multiple Products Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://www.vmware.com/security/advisories/VMSA-2022-0011.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-1388		BIG-IP: 11.6.1 - 16.1.2.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	Enemybot, Zerobot
F5 BIG-IP Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://support.f5.com/csp/article/K23605346

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38180		.NET: 6.0.0 - 7.0.9, Visual Studio: 17.2.0 17.2.32505.173 - 17.6.5 17.6.33829.357, ASP.NET Core: before 2.1.40	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:.net:-:*:*:*:*:*:*:*	-
.NET and Visual Studio Denial of Service Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1499.004:Application or System Exploitation, T1499:Endpoint Denial of Service	https://msrc.microsoft.com/vulnerability/CVE-2023-38180

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36884	✗	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019	RomCom
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Microsoft Office and Windows HTML Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-18368	✗	Zyxel P660HN-T1A Routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:billion:5200w-t_firmware:-:*:*:*:*:*:*:*	Gafgyt Botnet
Zyxel P660HN-T1A Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1059: Command and Scripting Interpreter	The Zyxel P660HN-T1A is a legacy product that has reached end-of-life. For the best defense, legacy products should be replaced with newer-generation equipment.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35838		WireGuard Client 0.5.3 on Windows	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:wireguard:client:0.5.3:*	-
WireGuard Client Denial of Service Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1498: Network Denial of Service	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36673		Avira Phantom VPN through 2.23.1 for macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:avira:phantom_vpn:*	-
Avira Phantom VPN DNS Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1498: Network Denial of Service, T1566: Phishing	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36672		Clario VPN client through 5.9.1.1662 for macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:clario:vpn_client:*	-
Clario VPN Plaintext Traffic Leakage Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1562: Impair Defenses	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36671		Clario VPN client through 5.9.1.1662 for macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:clario:vpn_client:*	-
Clario VPN Traffic to The Real IP Address of The VPN Server Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1562: Impair Defenses	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27532		Veeam Backup & Replication & Veeam Cloud Connect	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:backup_\&_replication:11.0.1.1261:*:*:*:*:*:*:*	Cuba ransomware BUGHATCH, and BURNTCIGAR
Veeam Missing Authentication for Critical Function			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-306	T1078: Valid Accounts, T1040: Network Sniffing	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32315		Openfire versions: 3.10.0 - 4.7.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*:*:*	-
Ignite Realtime Openfire Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1202: Indirect Command Execution, T1059: Command and Scripting Interpreter, T1505: Server Software Component	Upgrade Openfire versions to 4.6.8, 4.7.5, 4.8.0 or newer versions Link: https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38035	✗	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*:*:*	-
Ivanti Sentry Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	DarkMe, GuLoader, and Remcos RAT
WinRAR Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966		Zoho ManageEngine	Lazarus Group
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	QuiteRAT, CollectionRAT
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2868		Barracuda Networks Email Security Gateway (ESG): 5.1.3 - 9.2	UNC4841
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:barracuda_networks:esg:9.2:*:*:*:*:*:*:*	DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE
Barracuda Networks ESG Appliance Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	https://status.barracuda.com/incidents/34kx82j5n4q9;https://www.barracuda.com/company/legal/esg-vulnerability

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rilide Stealer	A new version of the Rilide Stealer malware, evading Chrome's security measures to target Chromium-based browsers in campaigns that exploit user trust through fake plugins and games	Phishing, Malicious Extensions	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data Theft, Financial Loss, Espionage	Google Chrome, Microsoft Edge, Brave, and Opera
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
STRRAT	STRRAT, a Java-based RAT, its latest version, STRRAT 1.6, is notable for employing diverse infection paths and conducting startup host queries to understand system architecture and anti-virus defenses.	Spam Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Extraction	Chrome, Firefox, Internet Explorer, Outlook, Thunderbird, and Foxmail
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TargetCompany Ransomware (aka Mallox, Fargo, and Tohnichi)	The new TargetCompany ransomware version begins by exploiting insecure SQL servers to consistently install its first stage. The routine attempts persistence by altering the URLs or suitable routes until it successfully locates a location to run the Remcos RAT.	Exploiting vulnerabilities in SQL servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Loss	-
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
Remcos RAT	The Remcos RAT, which acts as a loader, is delivered with TargetCompany Ransomware campagin. Remcos is a lightweight, easy-to-use, and highly flexible Remote Administration Tool with many features.	TargetCompany Ransomware	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Yashma Ransomware	The Yashma ransomware was identified in May 2022 as a modified variant of the Chaos malware. The ransom message used in this effort looks like the well-known WannaCry ransomware note, potentially misleading attribution. The message includes a Bitcoin wallet address but no payment information for ransom payments.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Vietnamese-origin threat actor			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WannaCry Ransomware	WannaCry Ransomware encrypts files or locks the device down. It then demands payment in the form of a cryptocurrency, such as Bitcoin, using GitHub's unique ransom note distribution method.	Exploiting vulnerabilities in the Windows OS	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Vietnamese-origin threat actor			-

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
Reptile	Reptile, a malware with extensive capabilities that is an open-source kernel module rootkit targeting Linux computers, has surfaced. Its availability on GitHub makes it freely available, and it goes beyond standard malware by providing more than simply concealing techniques. Reptile, unlike other rootkits, includes a reverse shell functionality that gives attackers direct access to infiltrated computers.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit			
ASSOCIATED ACTOR		Exfiltration of Data	Linux
Winnti Group (aka APT 41, Blackfly, Wicked Panda), UNC3886			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mélofée	The Mélofée malware incorporates a kernel-mode rootkit based on the Reptile open-source project. Discovered linkages to the Winnti Group, which operates out of China, based on the malware and infrastructure utilized in the attacks.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Exfiltration of Data	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Winnti Group (aka APT 41, Blackfly, Wicked Panda), UNC3886			-

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
LOLKEK Ransomware (aka GlobeImposter)	LOLKEK is a ransomware family that has been around since 2016. New samples have been observed in the wild in May 2023. These samples use a number of new tactics to evade detection, including obfuscation of the code, use of legitimate tools and services, and encryption of network shares in addition to local drives.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and Information loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhysida Ransomware	The Rhysida ransomware-as-a-service (RaaS) emerged in May 2023, in parallel with the launch of their victim assistance chat platform, accessible via the TOR network.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DroxiDat	In a targeted operation, an unidentified actor strategically deployed the advanced DroxiDat proxy-capable backdoor alongside Cobalt Strike beacons. The operation was aimed at a critical power utility.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Sensitive Data Theft	-
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
Gafgyt Botnet (aka Bashlite, Lizkebab, PinkSlip, Qbot, Torlus, and LizardStresser)	Gafgyt is a botnet that was first uncovered in 2014. It targets vulnerable Internet of Things (IoT) devices. Gafgyt botnet malware is actively trying to exploit a vulnerability in the end-of-life Zyxel P660HN-T1A router, which it then uses to launch large-scale distributed denial-of-service (DDoS) attacks.	Exploiting Zyxel routers	CVE-2017-18368
		IMPACT	**AFFECTED PRODUCT**
TYPE		Compromise of sensitive data and complete takeover of affected devices.	Zyxel P660HN-T1A Routers
Botnet			**PATCH DETAILS**
ASSOCIATED ACTOR			The Zyxel P660HN-T1A is a legacy product that has reached end-of-life. For the best defense, legacy products should be rep laced with newer-generation equipment.
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LummaC Stealer	LummaC Stealer is a malware that steals sensitive information from infected devices. It is distributed through a Malware-as-a-Service (MaaS) model on Russian-speaking forums. The malware is written in C language and is constantly being updated with new features.	Malware-as-a-Service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Amadey Bot	Amadey Bot is a modular Trojan malware that steals sensitive information and can download other malware. It can be customized to perform a variety of tasks.	Phishing emails, exploit kits, and drive-by downloads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft, Malicious Downloads	-
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
SectopRAT	SectopRAT is a remote access trojan (RAT) that is used to steal sensitive information from infected devices. It is a .NET-based malware that is first compiled in November 2019. It can steal a variety of data, including browser history, cookies, and cryptocurrency wallet information.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Monti	Monti ransomware, resembling Conti, resurfaces after a break, targeting legal and government sectors. A new Linux variant diverges significantly, using distinct tactics for encryption and virtual machine termination.	Phishing emails	CVE-2021-44228 (Log4Shell)
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial loss	VMware Horizon
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.vmware.com/security/advisories/VMSA-2021-0028.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BX RAT	BX RAT is a remote access trojan (RAT) that was first discovered in 2014. It is a modular malware, meaning that it can be customized to perform a variety of tasks. BX RAT is primarily used to steal sensitive information from infected devices	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Steal	-
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
JanelaRAT	JanelaRAT is a remote access trojan (RAT) that is targeting users in Latin America (LATAM). It is a heavily modified variant of BX RAT, which was first discovered in 2014. JanelaRAT can steal a variety of sensitive information from infected devices.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data steal	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AdLoad	AdLoad malware persists on Mac systems with a new proxy application payload, converting infected devices into a proxy botnet. This scheme, involving thousands of IP addresses, points to a monetization strategy by a company offering proxy services, emphasizing the evolving nature of cyber threats.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Steal, system damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HUI Loader	HUI Loader is a malware loader that is used to download and install other malware on infected devices. It is distributed through a variety of methods. Once HUI Loader is installed on a victim's computer, it will download and install other malware.	Phishing emails, Malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data steal, compromise system	-
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
Cuba ransomware (aka Fidel, COLDDRAW)	The Cuba ransomware gains initial access through compromised administrative credentials via Remote Desktop Protocol (RDP), avoiding the need for brute force methods. The Bring Your Own Vulnerable Driver (BYOVD) technique is used to bypass endpoint protection tools.	Compromised administrative credentials via Remote Desktop Protocol	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss and Information theft	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BUGHATCH	BUGHATCH is a custom loader exclusively linked to the Cuba ransomware group. This tool establishes a connection to a command-and-control (C2) server, fetching a payload, usually small PE files or PowerShell scripts.	PowerShell dropper	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information Theft	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

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
BURNTCIGAR	BURNTCIGAR is an anti-malware utility that terminates kernel processes tied to endpoint security products. The threat actor has made some modifications, likely as a mechanism to impede both detections with the inclusion of the hashing functionality to BURNTCIGAR's codebase.	Unknown	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Endpoint Security Products were decommissioned.	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira Ransomware	Akira, a relatively new ransomware operation, emerged in March 2023 and is written in C++. It has expanded its tactics by adding a Linux encryptor to target VMware virtual machines. Malware has been leveraging compromised Cisco VPN accounts to breach corporate networks without needing additional backdoors or persistence mechanisms.	Cisco VPN products	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware			
ASSOCIATED ACTOR		Extortion of data and Financial Loss	Windows, Linux, macOS and VMware
-			**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
PlugX (aka Korplug)	The Carderbee advanced persistent threat (APT) group executed a supply chain attack by exploiting the legitimate Cobra DocGuard software. Their objective was to deploy the PlugX backdoor onto targeted organizations primarily situated in Hong Kong.	EsafeNet Cobra DocGuard Client	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor			
ASSOCIATED ACTOR		Data Theft, Malicious Downloads	-
Carderbee			**PATCH LINK**
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkMe	DarkMe is a VisualBasic spy Trojan first spotted in September 2021. The vulnerability allowed hackers to distribute malware by creating seemingly harmless archives that contained files like JPG images, text documents, or PDFs. When users opened these files, the flaw triggered a script that installed malware on their devices.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan			
ASSOCIATED ACTOR		Financial Loss	RARLAB WinRAR
-			**PATCH DETAIL**
			Update WinRAR version to 6.23 or later versions

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GuLoader (aka CloudEye)	GuLoader is used to load other malicious files and employs various obfuscation and anti-reverse analysis techniques to evade detection by security products. Once the initial setup is done, different PowerShell scripts will run to launch the GuLoader payload.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader			
ASSOCIATED ACTOR		Malicious Downloads and Financial Loss	RARLAB WinRAR
-			**PATCH DETAIL**
			Update WinRAR version to 6.23 or later versions

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
Remcos RAT(aka: Remcos, Remvio, Socmer)	Remcos RAT (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers, granting attackers significant control over the compromised system.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and Financial Loss	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH DETAIL**
-			Update WinRAR version to 6.23 or later versions

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Scarab Ransomware	The attacks aim to utilize ScService's access to introduce a variant of the Scarab ransomware. Scarab, coded in Delphi. It uses an embedded configuration similar to Zeppelin ransomware, determining encrypted file details, filenames, targeted extensions, and ransom messages.	Exploiting Zerologon Vulnerability	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data Theft and financial loss	Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH DETAILS**
CosmicBeetle			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Spacecolon	Spacecolon consists of three core Delphi components: ScHackTool, ScInstaller, and ScService. The primary orchestrator component is ScHackTool, which enables CosmicBeetle to deploy the other components.	Exploiting Zerologon Vulnerability	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Toolkit		Data Theft and financial loss	Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINK**
CosmicBeetle			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

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
QuiteRAT	QuiteRAT consists of a compact set of statically linked Qt libraries along with some user-written code. The QuiteRAT can also receive a command code along with a numeric value from the C2 server.	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus.	CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Sensitive Data Theft	Zoho ManageEngine
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CollectionRAT	Exhibiting conventional RAT capabilities, CollectionRAT enables the execution of arbitrary commands on compromised systems. CollectionRAT appears to share connections with Jupiter/EarlyRAT, another strain of malware attributed to Andariel, a subgroup nestled within the Lazarus Group threat actor-network.	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus.	CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Sensitive Data Theft	Zoho ManageEngine
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agniane Stealer	The Agniane Stealer, coded in C#, operates as an information pilferer. It primarily focuses on extracting stored credentials from a wide array of sources, with a specific emphasis on targeting cryptocurrency extensions and wallets.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Credential theft	-
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
Trash Panda	Trash Panda is a ransomware that encrypts files on Windows machines, replaces the desktop wallpaper, and drops a ransom note with political messages. It adds a '.monochrome' extension to the encrypted files and demands payment for decryption.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DEPTHCHARGE (aka SUBMARINE)	DEPTHCHARGE. It is a modular backdoor trojan that was used by the UNC4841 threat group. Communicates via TCP, it comes with features to capture keystrokes, run shell commands, transfer files, and set up a reverse shell.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SKIPJACK	SKIPJACK is a backdoor trojan that was used by the Chinese-nexus threat group UNC4841. It is a modular malware that can be customized to perform a variety of tasks. It's delivered via phishing emails or exploit kits. Once it is installed on a system, it can be used to steal sensitive information.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FOXTROT	FOXTROT is a malware family that has been used by the Chinese-nexus threat group UNC4841. It is a C++ implant that is launched using a C-based program dubbed FOXGLOVE. Communicating via TCP, it comes with features to capture keystrokes, run shell commands, transfer files, and set up a reverse shell.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft and espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FOXGLOVE	FOXGLOVE is a malware family that has been used by the Chinese-nexus threat group UNC4841. It is a modular malware that can be customized to perform a variety of tasks.	Exploitation of CVE-2023-2868	CVE-2023-2868
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft and espionage	Barracuda Networks Email Security Gateway (ESG) Appliance
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://status.barracuda.com/incidents/34kx82j5n4q9

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT 29 (aka Midnight Blizzard, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)	Russia	Government, Non-Government Organizations (NGOs), IT services, Technology, Discrete manufacturing, and Media	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows
TTPs			
T1036:Masquerading, T1621:Multi-Factor Authentication Request Generation, T1566:Phishing , T1110.003:Password Spraying, T1110:Brute Force , T1484.002:Domain Trust Modification, T1484:Domain Policy Modification, T1583.001:Domains, T1583:Acquire Infrastructure , T1566.003:Spearphishing via Service , T1586:Compromise Accounts , T1530:Data from Cloud Storage			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Winnti Group (Blackfly, APT41, Wicked Panda)	China	Materials, composites semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food.	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Reptile and Mélofée	Linux
TTPs			
T1105: Ingress Tool Transfer, T1070.004: File Deletion, T1070: Indicator Removal, T1014: Rootkit, T1205.001: Port Knocking, T1205: Traffic Signaling, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1095: Non-Application Layer Protocol, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	Defense, Technology, and Telecommunication.	South Korea
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Reptile and Mélofée	Linux
TTPs			
T1105: Ingress Tool Transfer, T1070.004: File Deletion, T1070: Indicator Removal, T1014: Rootkit, T1205.001: Port Knocking, T1205: Traffic Signaling, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1095: Non-Application Layer Protocol, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 RomCom (Storm-0978, DEV-0978)	Russia	Finance, Telecommunications, Political, Defense, and Government	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-36884	-	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019
TTPs			
T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1588.005: Exploits, T1040: Network Sniffing, T1005: Data from Local System, T1036: Masquerading, T1574: Hijack Execution Flow, T1211: Exploitation for Defense Evasion			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Flax Typhoon	China	Government agencies, Education, Critical Manufacturing, and Information Technology Organizations	Taiwan, Southeast Asia, North America and Africa
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows
TTPs			
T1190: Exploit Public-Facing Application; T1505.003: Web Shell; T1505: Server Software Component; T1059: Command and Scripting Interpreter; T1546: Event Triggered Execution; T1546.008: Accessibility Features;T1105: Ingress Tool Transfer ; T1543: Create or Modify System Process; T1543.003: Windows Service; T1003.001: LSASS Memory; T1550: Use Alternate Authentication Material; T1003: OS Credential Dumping; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1003.002: Security Account Manager; T1572: Protocol Tunneling; T1550.002: Pass the Hash			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Bronze Starlight (aka DEV-0401, Cinnamon Tempest, SLIME34, Emperor Dragonfly)	China	Gambling sector	Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows, Linux, macOS
TTPs			
T1053:Scheduled Task/Job, T1129:Shared Modules, T1574:Hijack Execution Flow, T1574.002:DLL Side-Loading, T1027:Obfuscated Files or Information, T1027.002:Software Packing, T1036:Masquerading, T1070.006:Timestomp, T1140:Deobfuscate/Decode Files or Information, T1497:Virtualization/Sandbox Evasion, T1562.001:Disable or Modify Tools, T1010:Application Window Discovery, T1012:Query Registry, T1057:Process Discovery, T1083:File and Directory Discovery, T1560:Archive Collected Data, T1071:Application Layer Protocol, T1095:Non-Application Layer Protocol, T1573:Encrypted Channel, T1018:Remote System Discovery, T1082:System Information Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Carderbee	Unknown	-	Asia
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PlugX (aka Korplug)	-
TTPs			
T1129: Shared Modules, T1543.003: Windows Service, T1547.008: LSASS Driver, T1027: Obfuscated Files or Information, T1036: Masquerading, T1070.004: File Deletion, T1112: Modify Registry, T1056: Input Capture, T1012: Query Registry, T1018: Remote System Discovery, T1082: System Information Discovery, T1518.001: Security Software Discovery, T1071: Application Layer Protocol, T1095: Non-Application Layer Protocol, T1105: Ingress Tool Transfer, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 CosmicBeetle	Unknown	Hospital, Hospitality, Insurance, Government, Entertainment, Education	Thailand, Israel, Poland, Brazil, Turkey, Mexico
	MOTIVE		
	Financial gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2020-1472	Scarab Ransomware, Spacecolon	Microsoft Netlogon
TTPs			
T1595.002: Vulnerability Scanning, T1583.001: Domains, T1587.001: Malware, T1587.003: Digital Certificates, T1190: Exploit Public-Facing Application, T1059.003: Windows Command Shell, T1059.001: PowerShell, T1059.005: Visual Basic, T1053.005: Scheduled Task, T1133: External Remote Services, T1547.001: Registry Run Keys / Startup Folder, T1136.001: Local Account, T1543.003: Windows Service, T1078.003: Local Accounts, T1140: Deobfuscate/Decode Files or Information, T1070.001: Clear Windows Event: Logs, T1003.001: LSASS Memory, T1082: System Information Discovery, T1115: Clipboard Data, T1071.001: Web Protocols, T1041: Exfiltration Over C2 Channel, T1095: Non-Application Layer Protocol, T1529: System: Shutdown/Reboot, T1486: Data Encrypted for Impact			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Lazarus Group (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, Diamond Sleet)</td><td>North Korea</td><td rowspan="2">Healthcare, IT, Critical Infrastructure</td><td rowspan="2">Europe and the U.S.</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2022-47966</td><td>QuiteRAT, CollectionRAT</td><td>Zoho ManageEngine</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1059: Command and Scripting Interpreter, T1574.002: DLL Side-Loading, T1497: Virtualization/Sandbox Evasion, T1056: Input Capture, T1018: Remote System: Discovery, T1082: System Information: Discovery, T1518.001: Security Software: Discovery, T1087.002: Domain Account, T1071: Application Layer Protocol, T1095: Non-Application Layer: Protocol, T1105: Ingress Tool Transfer, T1574: Hijack Execution Flow</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC4841	China	Government, High-Tech, IT, Healthcare, Biotechnology, Telecommunication, Defense, Aerospace, Education, Consulting and Professional Services, Trade, Semiconductor, Energy, Non-Profit, Logistics, Manufacturing, Foreign Affairs	Parts of Europe, Asia, South Africa, Australia, and the USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	CVE-2023-2868	DEPTHCHARGE (aka SUBMARINE), SKIPJACK, FOXTROT, and FOXGLOVE	Barracuda Networks Email Security Gateway (ESG) Appliance
TTPs			
T1543: Create or Modify System Process; T1543.004: Launch Daemon; T1574: Hijack Execution Flow; T1068: Exploitation for Privilege Escalation; T1055: Process Injection; T1211: Exploitation for Defense Evasion; T1059: Command and Scripting Interpreter; T1212: Exploitation for Credential Access; T1056: Input Capture; T1056.001: Keylogging; T1057: Process Discovery; T1082: System Information Discovery T1560 Archive Collected Data T1005 Data from Local System T1071 Application Layer Protocol; T1132: Data Encoding; T1105: Ingress Tool Transfer; T1588.006: Vulnerabilities; T1041: Exfiltration Over C2 Channel			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1595: Active Scanning	
	T1598: Phishing for Information	
	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1595.002: Active Scanning: Vulnerability Scanning	
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1584: Compromise Infrastructure	T1584.004: Server
	T1583: Acquire Infrastructure	T1583.001: Domains
	T1586: Compromise Accounts	
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.006: SEO Poisoning
	T1584: Compromise Infrastructure	T1584.005: Botnet
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.003: Digital Certificates
TA0001: Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003:Spearphishing via Service
	T1189: Drive-by Compromise	
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1190: Exploit Public-Facing Application	
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.007: JavaScript
		T1059.005: Visual Basic
		T1059.008: Network Device CLI
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1204: User Execution	T1204.002: Malicious File
	T1203: Exploitation for Client Execution	
	T1129: Shared Modules	
	T1047: Windows Management Instrumentation	
	T1106: Native API	
	T1569: System Services	T1569.002: Service Execution
	T1204: User Execution	T1204.001: Malicious Link
	T1559: Inter-Process Communication	T1559.001: Component Object Model

Tactic	Technique	Sub-technique
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
		T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1543: Create or Modify System Process	T1543.001: Launch Agent
	T1133: External Remote Services	
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1556: Modify Authentication Process	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1547: Boot or Logon Autostart Execution	T1547.008: LSASS Driver
	T1136: Create Account	T1136.001: Local Account
	T1098: Account Manipulation	
	T1136: Create Account	
	T1546: Event Triggered Execution	T1546.008: Accessibility Features
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
	T1055: Process Injection	
	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
		T1547.008: LSASS Driver
		T1547.001: Registry Run Keys / Startup Folder
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1055: Process Injection	T1055.012: Process Hollowing
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1546: Event Triggered Execution	T1546.008: Accessibility Features
TA0005: Defense Evasion	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
	T1218: System Binary Proxy Execution	T1218.011: Rundll32

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.001: Invalid Code Signature
		T1036.006: Space after Filename
		T1036.007: Double File Extension
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.006: Timestomp
		T1070.004: File Deletion
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.009: Embedded Payloads
		T1027.001: Binary Padding
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.008: Stripped Payloads
	T1127: Trusted Developer Utilities Proxy Execution	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1211: Exploitation for Defense Evasion	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1140: Deobfuscate/Decode Files or Information	
	T1006: Direct Volume Access	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1014: Rootkit	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1112: Modify Registry	
	T1202: Indirect Command Execution	
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
		T1497.002: User Activity Based Checks
		T1497.001: System Checks
	T1620: Reflective Code Loading	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
	T1218: System Binary Proxy Execution	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash

Tactic	Technique	Sub-technique
TA0007: Discovery	T1018: Remote System Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1217: Browser Information Discovery	
	T1040: Network Sniffing	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1010: Application Window Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1012: Query Registry	
	T1033: System Owner/User Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.002: User Activity Based Checks
		T1497.003: Time Based Evasion
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
TA0008: Lateral Movement	T1021: Remote Services	
	T1570: Lateral Tool Transfer	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
TA0009: Collection	T1005: Data from Local System	
	T1530: Data from Cloud Storage	
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1056: Input Capture	T1056.001: Keylogging
	T1560: Archive Collected Data	
	T1123: Audio Capture	
	T1125: Video Capture	
TA0011: Command and Control	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1572: Protocol Tunneling	
	T1105: Ingress Tool Transfer	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1095: Non-Application Layer Protocol	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1219: Remote Access Software	
	T1132: Data Encoding	T1132.001: Standard Encoding
		T1132.002: Non-Standard Encoding

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1567: Exfiltration Over Web Service	
	T1041: Exfiltration Over C2 Channel	
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1498: Network Denial of Service	
	T1496: Resource Hijacking	
	T1529: System Shutdown/Reboot	
TA0006: Credential Access	T1110: Brute Force	T1110.003: Password Spraying
	T1621: Multi-Factor Authentication Request Generation	
	T1539: Steal Web Session Cookie	
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1212: Exploitation for Credential Access	
	T1556: Modify Authentication Process	
	T1552: Unsecured Credentials	T1552.002: Credentials in Registry
	T1606: Forge Web Credentials	T1606.001: Web Cookies

Top 5 Takeaways

#1 In August, there were **thirteen zero-day** vulnerabilities. One of these vulnerabilities was exploited by **Storm-0978 group.**

#2 Throughout the month, various ransomware strains including Cuba, Akira, TargetCompany, Yashma, WannaCry, LOLKEK, Monti, Rhysida, and Scarab actively targeting victims.

#3 There were a total of 10 active adversaries identified across multiple campaigns. Their focus was directed toward the following key industries: Government, Healthcare, IT Services, Education and Manufacturing.

#4 Numerous malware families have been observed targeting victims worldwide. These include **Rilide Stealer, STRRAT, Reptile, DroxiDat, PlugX, DarkMe, GuLoader, and Remcos RAT**.

#5 Finally, the zero-day vulnerability **CVE-2023-38831** in WinRAR, allowing hackers to install malware through manipulated archives, exposing users to hidden malicious scripts and potential cyberattacks.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **27 significant vulnerabilities** and block the indicators related to the **10 active threat actors, 30 active malware,** and **227 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 (AUGUST 2023)

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

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

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

Appendix

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

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

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

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

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

Glossary:
CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
CVE - Common Vulnerabilities and Exposures
CPE - Common Platform Enumeration
CWE - Common Weakness Enumeration

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Rilide Stealer	MD5	0f8c7037ba4cf9736a5ac22cde94b7ed, 0fb39568d9ba07e39f64d64510832a99, 172f5c41250ef3e84579645e5b1a22bc, 1c683f7e8ede935de16fe1af8d920b4e, 1de4b5ff5035d3df6ab27d12c83b18f5, 20d8abba528c323668911a7da1993336, 23fc39223b0225998a70a3cb2e05ad4b, 367300209532298c12b8678a1699b6ff, 403dd2a2a6163c07710fabc08f71bec8, 44cf3fe19f92cfac81d74ec366302104, 47c7a9d2010c0f1d1c20fec47339451b, 4a0e5fee91b361a09cd9d70e5f6ffb3d, 4aa44852969f4c603bf9e8e3799d6984, 59998a5c7c0f31adc47f3d05333ff8cc, 59e77f77b458eb0c390f90e2daa35504, 5a439a865ba82b35ef8eeacc1a778e0c, 5e8d7b2ea9c184a5a88edd0e507571ed, 614ce2b5df0dd74d1bc5b0bde55edd53, 63e9249d7950ca2e03c40a64a76a3951, 66e05bc7b8e8ccd31415e22272f03bd4, 678a0f6c5a0662b8f42fca2f6788e3c6, 79f586fe64498205b1aab8ece4b2e944, 7a60adb662556863752bd2ab1c25c727, 7ba207ff437a0df9b5a05a01c0d548b9, 7ca9216d43d51507d326a72c4d27056e, 8080ad6ea6102d445ea16169a990cb5e, 89d7bf4d70efaeb4e63eddd179df9829, 8b008a8f776b57060b5ce42b6ea2b8f6, 97a42807acd13205c1a2937850416439, 9f806a3d233ffbbb58cf82c3e769d6a5, a404c8f69888159b85aa2b069f0d0f90, a906698ebe07eac71494052bb82cd3f2, adbc8e285c7657615b2ebee344390952, ae249d95c6ac779246b8eea93730801f, b4867df506f38736c0f6ce56decad080, bb8315ba98e0cb251453d58cf2048f3b, bc9472ab59a9625003190b2dfcd1c502, bda2f43f6a08de8e0d41aa704a796eb1, c8805c7f4224c02b173f6beab132638c, ced4052c3d3d32e21df075d68b5a4494, cfe9ec19dd3991c45c76493d9598141b, d2b07b0e4142bbcb1457d51e25da416d, D504505d18408343a5f1225a0d0f3c1b, ddddeb26f795fd7658720d5ae80a310d,

Attack Name	TYPE	VALUE
Rilide Stealer	MD5	df7d7dc978275f8c85ab8408abc8df95, e879d0f7540ce7b3365c7f79a461ec98, f1f97bcec87f298f3f533fbcb0de034e, f5dc1259e5300b8d4711ca7bf51c6e9f, f8653cd2a1c7cea7509abd6cd52078b3, fa3509f5adb6b3c8857194083af87edd, fc3afbea35d3844550af54a2506a5f64, fd59031e1c35e5fb1ecbaff6c64a31e8
	Domains	blackfox.lol, eaougheofhuoaez.top, edd2ed2.online, ext-panel.website, extension-login.com, extensionsupdate.com, faugzeazdezgzgfm.top, frz-panel.su, getvoyagebox.org, io-web.cc, lsadksajpenal.su, nightpredators.com, proyectopatentadomxapostol.com, pupkalazalupka.com, riotrevelry.com, silent-scale.com, tes123123t.com, web-lox.com
	SHA1	018caa6adbd983fd2e2ba46670196a41669b4cef, 027268c51892ca07c36b66ae31dbe33c2afeb789, 060ac379851786e61d081b1471ee15347185e56c, 10d3d6bf88bead7180e84a2b7acf3abc60e14e81, 16f46139147f5f6dcd521840951860c299982587, 173065e688b008e208d6ffd62ea2b5a15cf66552, 18ccba913df5b8867c6ef066f121fb8cd03a7518, 2700d7a6c6f5abdea5972c9d5a67603216870af4, 29dd8609c74cc54d60bab53c6e83a3cb641f8b4a, 2c98abcaea10d3abd307c68cbf95f3e4af40ec04, 3197073f18ce0432691d61f09302f949d3283e0b, 3976d181a1bdeaca94c072d672ee90750865ee96, 397a40a2f5047db13bf84bd7e6296c12dc317933, 3c6fcd01f513df3480930924bd82d2abdb19266a, 5174127b62bd3a1e983dd8a33e3efa5ec54471c8, 52a1ee4060e13790501163c78d3475be90f05584, 552b715702d8b4b0f035a92d5ab5bb1f0712ac32, 69fb5b178f369beaac85f02791fd8f85facdd20b, 70cae8f5f2d6573510f5f4400a8baba89e5bcd2f,

Attack Name	TYPE	VALUE
Rilide Stealer	SHA1	92a030999013b6835b39d2cce951fcb258107bc8, 92d4921b1fc15ae389a59b5df90614d7926f95e9, 937e03c89c33bbd5c7727c3f8e00aecdf22afa7f, 946ac4d655bc77624b912ad42431c8a692cac6a4, a1456ea8696c755d1d2c4d1f27661f9388f805b9, a1b9fd0577f6cc0ff87010a651ff123b8285289c, a25fccb0455f8e9d3751f5127dd6867aecb58b45, a468269647f3b9909f4df27b74711d56adaf87a4, aa7929ba89295c732398c63a574a49f035b9ca52, ace802a22a69b2d6fe305d407212c0919671f81a, b0c587068505fcbdb55d263dff03f3abbeeb0842, b27a56ee3262c4d87bae60c514ea7056a4ec7c6f, b3d59d7caab786cb92639a8c8bc17f73da26c788, c84a3774eea3c7c3069964fff500eb498a3e3fa0, cba87daff1cf961fe941489cfcc80f074f8d49ed, cc7949e9587b7f64049ab5b9b3603eb831f47808, ccbf7ed9d3c2b606b753359cb4b10caa2570a571, cde2d4b70d374fca96951a13f056f778258aeb45, d033569c97f382b21ce83439dae0cab5bd28e135, d85c34f3cd20d24fde93f0e60d677d2aa8c48591, dc7fa285da2034a00ed2c66cb86c37e1a4bbd679, dd4e7e8230e14685d73d142efb337e75cb2d3581, dd6e2e93d80d9b5df93e17e714aee41534f1158a, dd7f3feb98e4d84817a84a9fdfddaed3b2719303, ddb5e3e03655fa8dd8690aeb81db00da84bd2c8b, e3476f4fb588b23bdd625bdc75a98a16d1acb4bd, e4aaef90c4284e923679e92e970396f7ef989087, ea4d7f31e889585d1a2c77e2b2823a4ccbd765d2, f2348f98a71afcc241c6e3d5777b300e5602a4e5, f5a5d008a70e1c632d7cb72b2f255f3e500b43e4, F637104610e14e2260a792fd17775a83d2551a38, 76fc50665aea80dca8844282804339b7351c3267, 8316ab2ee030c859d2952a0a0ee3fb8606b88816,
	SHA256	008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c, 0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb, 0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520, 14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc, 1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2, 1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b, 1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a,

Attack Name	TYPE	VALUE
Rilide Stealer	SHA256	2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d, 2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5, 35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31, 3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd, 3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473, 45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6, 461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11, 482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1, 48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460, 533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12, 54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c, 5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c, 687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde, 6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503, 6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0, 6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907, 6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e, 718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9, 7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794, 7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723, 7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7, 83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1, 8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8, a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a,

Attack Name	TYPE	VALUE
Rilide Stealer	SHA256	a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158, aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b, abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f, abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76, ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05, ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd, ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23, aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8, b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27, ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3, c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc, cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd, cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7, d4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779, d755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36, dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a, dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da, dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485, e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856, e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431, e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0, e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34, f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997, f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568

Attack Name	TYPE	VALUE
Rilide Stealer	Domains	blackfox.lol, eaougheofhuoaez.top, edd2ed2.online, ext-panel.website, extension-login.com, extensionsupdate.com, faugzeazdezgzgfm.top, frz-panel.su, getvoyagebox.org, io-web.cc, lsadksajpenal.su, nightpredators.com, proyectopatentadomxapostol.com, pupkalazalupka.com, riotrevelry.com, silent-scale.com, tes123123t.com, web-lox.com
STRRAT	SHA256	**3d3cb10a1a9059900ddeb58209edcfa52461806558ebbee422c417c6535aa3a5,** **8250d324bbc14e3b3a7abc032b6b55aa0699ff9bc784d6c67fdd381edc3b9e56,** **c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20,** **9714dce49616e48fc4851d05453056939ab08bf140fe9a786616fa914debb4f4,** **c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20,** **6ec3e682fbbd0c23fb4e3a2c2b28f03431b90a88651d227ae3f33b6fadf507cf,** **058c764614c8b0b457852a71ab93b559f81abb9e13b7fc2d6c6a4962881bf062,** **5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21,** **5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21,** **cbe7d5663fd5359a72f88e44d083703d9625235929c31e0f5b16a0b42cb44d35,** **8cae71910574fa96fdf20ddab8897e90d155e50036ddb2f3d033a7b13a45b90f,** **c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20,** **b74a0e8adc5f0681405c94a684d6b887fdc20cd6d198d069f0981d6ba7d658c6,** **31c2e51efcbff0aa489aa6af1a48cf78f6a9febfb449a19d029f8cc8ebb4495f,**

Attack Name	TYPE	VALUE
STRRAT	SHA256	ab6f8c51d1f15a18cd23e1ad5a34c82c83746befb7d11cce2860c971be35adaa, d634982709d3ebf1641b1160ed6452fa9e3bf2cc8d28f397e56ca9687b28ec84, a0670c21968e2b1256d72799c22a512e503597ab375d20c49d9ec43428c4c3b2, 3a74d083e1c4e30f1eedcb90c842bf1a7e65a979edab40e37885607bd566bee8, 569f5f6de156bec90f9b0b0e4e707a702c0fea26ab6a0711e32f4a413995ae7c, 176e45016749ec233b8fe1ce32ce2cd47dd5bc8da3663f1c6cf054f6ad58a187, 3094952f4e4c826cdfbc7b146212eec6094f5104b4ba0d70d3b2920a263add27, 4bf781354d02ca0d67a3a180fd6f0d183c6fba763caa660f986752be8b4bb586, 6f7180a451691ee975f516cfc6fb3f0c983bc80aebd1d662a899ff4344e4077e
	SHA1	4651326299d02ac07c0b51c0abb7067f24293a65, 8fa3c76f427f73cbfa864c380769825018cf72f5, f726bf1b6bc380c02d76d273765c888f6b41f197, 433b6ac1169a9bd7e0cfe7029954070cc2b4ebdf
	MD5	9af7e66c85e07a1e182fcb024e7048a2, c7130bf8bca520792f6eff1592a112b2, 61522d1e3290906215d580b8b59e6341, 9bc8ac6d3a38357488de33952e929143
	Domain	talibangeneral[.]dynamic-dns[.]net
	URLs	hxxp://jbfrost[.]live/strigoi/server/?hwid=1&lid=m&ht=5, hxxps://tatchumbemerchants[.]co.ke/Invo-0728403[.]zip.
	File Name	Invo-0728403.zip
TargetCompany Ransomware	SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115, 26a674f981da653d72d139331e0a46e7dc09142ce2bc602655d6fbb37626c668, bcff44c6673ded04c8fb76b733837ce109ac6cbb0e4d1ba5b290f76632a4e718, 22816dc4dda6beec453e9a48520842b8409c54933cc81f1a338bc77199ab917e,

Attack Name	TYPE	VALUE
TargetCompany Ransomware	SHA256	52fe40246265e29ab791c26e57e568b18cbc4f57c3db5b12beb1415c416d64bb, 1ef8aebbb3816d7d534a581c1d1d8730a73355068e8b39587b2363ccbe692c08, 2efdffd1cf3adab21ff760f009d8893d8c4cbcf63b2c3bfcc1139457c9cd430b, 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde, f0e68af393967d8a236461815dd601baf7ebced7b807c224bceb51d0e8bb4b87, 18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7, 08cfd5a321a47a55c5e8732e3d12bf937ca32426dcd668c7d620cfae48159348, e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173, e0d4dc05991211e86c920092966d7025f8e40b77a799428f8491c4f7fa6078a6, 12842d49038c066464ac723b9665ff93f634042646bdd6947b54042fd0e06342, bf28b8a8576beb4755ec6a9d93fc4539e40dee7197b6399dfad5224f5ee74b19, eb75b7d31a9bd3686fcb0088c6849724396871711013 68ebf9134a53abac3c20, 3c665d38c5ccb0b41983ad492b31c499b176219ca7a93494fd902f592cee2ff6, 777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899, 4b1949536f3f6140da0a9fc87eb0430b61206852145ada5cecbc279b242bce10
	URLs	hxxp://80.66.75[.]37, hxxp://185.209.230[.]21:8080, hxxps[:]//whyers[.]io/QWEwqdsvsf/ap[.]php
	IPv4	195.3.146[.]183, 80.66.75[.]116, 80.66.75[.]*
Remcos RAT	SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115
	URL	hxxp://185.209.230[.]21:8080

Attack Name	TYPE	VALUE
Yashma Ransomware	SHA1	367411a1e2efde7eb9d39de66be90a96012d5d7b
	SHA256	3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac, de68f4bce05a856ad949e6fb1738559fc506d491d4f6227553695aa9558b64be
	Hostname	www.fxxz[.]com
WannaCry Ransomware	SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa, 74d72f5f488bd3c2e28322c8997d44ac61ee3ccc49b7c42220472633af95c0c0, 994b41a5d3b6d031d9256ed757da213829c7345580819ae574c21eda19ae29db, 4a45fba2077320cbe23c36a025dc37006f73aa97b57abf8404e6c72e7223f0c8, 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Reptile	MD5	1957e405e7326bd2c91d20da1599d18e, 246c5bec21c0a87657786d5d9b53fe38, 5b788feef374bbac8a572adaf1da3d38, 977bb7fa58e6dfe80f4bea1a04900276, bb2a0bac5451f8acb229d17c97891eaf, c3c332627e68ce7673ca6f0d273b282e, cb61b3624885deed6b2181b15db86f4d, d1abb8c012cc8864dcc109b5a15003ac, f8247453077dd6c5c1471edd01733d7f
	SHA1	0c6d838c408e88113a4580e733cdb1ca93807989, 2ca4787d2cfffac722264a8bdae77abd7f4a2551, 3cc2d6bf5215de3c24fb194c232a0411cede78e0, 467ea946ac857471e2f01bbdc4258a0ff31c01ce, 76d6cb6b6e9b40b07944153b1f140e786e3ae381, 783736e9274bd2bb90390bb9c23a62c387cde3ef, 7d9eaefeb0c95473ad86abbdcffdbdf6950b8dd2, a5f6162c6b6b6f0c177771a56a6b1eb5d7b593a0, ee295ec546158e425a3660a4a9402916087ccd97
	SHA256	133d3e070e30c94a591450b0930daf9f751debc0f4384fac6ace63f60a383818, 1425a4a89b938d5641ed438333708d1728cfed8c124451180d011f6bbb409976, 15e4e936b2f47eb3fa2455b7c22b2714bebe9f8c01b24bbf7cb5f9559999d292, 17bbebd7d8982d580cc3dea35d988ae2bfd62d708b69662419c41682274e0a14, 4305c04df40d3ac7966289cc0a81cedbdd4eee2f92324b26fe26f57f57265bca,

Attack Name	TYPE	VALUE
Reptile	SHA256	7ce7b914bd434f8a45db1cb3ec783237a5485b7abcee4df06275ea274e095295, 99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c, cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec, d182239d408da23306ea6b0f5f129ef401565a4d7ab4fe33506f8ac0a08d37ba
Mélofée	Domain	update[.]ankining[.]com, www.data-yuzefuji.com, ssm[.]awszonwork[.]com
	IPv4	156.67.208[.]192, 5.61.57[.]80
LOLKEK Ransomware	SHA1	ed247b58c0680b7c92632209181733e92f1b0721, 768b8d81a6b0f779394e4af48755ca3ad77ed951, 88baff4e1751bd364cdb1a4bb5fda4a37ee127c4, 456b0bda3f6d9ec9a874daac050b75fc28174510
	SHA256	08029396eb9aef9b413582d103b070c3f422e2b56e1326fe318bef60bdc382ed, 58ac26d62653a648d69d1bcaed1b43d209e037e6d79f62a65eb5d059e8d0fc3f, 2c66e5f96470526219f40c6adfd6990cc28d520975da1fdb6bb5497d55a54117, 0b179973dc267d9c300e9b7d3c27c67a18d7c79b2cc34927cbe5a465f83c6190
	Domains	mmcbkgua72og66w4jz3qcxkkhefax754pg6iknmtfujvkt2j65ffraad[.]onion, filessupport[@]onionmail[.]org
	URL	https[:]//yip[.]su/2QstD5
	MD5	518a38b47292b1e809c5e6f0bb1858be
Rhysida Ransomware	SHA1	69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8, 7abc07e7f56fc27130f84d1c7935a0961bd58cb9, 2543857b275ea5c6d332ab279498a5b772bd2bd4, eda3a5b8ec86dd5741786ed791d43698bb92a262, 69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8
	MD5	59a9ca795b59161f767b94fc2dece71a

Attack Name	TYPE	VALUE
Rhysida Ransomware	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de, 3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96, 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951Bd6d1b2
	URL	hxxps://ipapi[.]com/json/
Gafgyt Botnet	SHA256	21ecc53c3fe5336dd717b50fa70e281c5612b0c770f68d9f38c93e13e8357e21, 08d221d2d98a81d85e8bf0e8f3c8c4ddb35cc32c268a2cfe2cb2837e7f8fc731, e1cb8cf85745f7a771b33eab060e04556b1b33d186a65ae069377668fcea47b7, 9fea55b5dd337dcd5c00f4b9c1a09ad2ed5cb7f2c69dc21a7f50f55af0809f89, 06ad76f4b19be8706f98441d926142af824bd2983217f6c2c02201dbb07d0224, 2481e420138bb0bcc52d43a127e76887cc7419ac46e7495f55493d7fccbbec1b, fc76a4046efbaaab93261806f52afcd6cdf88c2784ec2ed7e862089f3d6bbbb8, 8131b5119e869e1ebf7ebce50837f12fa86fa24008d5534b757c23e91e8f401f, 20770419f79550e46c9bdc2dab792cc96792b7ec4dbd8fcc0cedd7c726ae7987, b8baa7b5d0d60070ef78ad846e17198e891093a84a00e3029dad0ffd77c78b7a, 4f6d665fa107ba9d7313ff6bf1527dddf18bcf178ae34c0e573b3afcb52d685f, b14eb9596f91c1625c3df29413fa08ba313a6b9e6d7fb1297fba74761c135568, a908289bef30086660453ab8809af758af3d445ecda4010211282eb067fef3ab, 9db1a5e089a0b16b3b9a584cb3e5e55eb68620d0ab6b229cf24d49f32b9391be, 94797cd702cf50fea6d780ab0d94cb2a0aa8ee9aa5332e71479adaa7a5245f27, 8ef658a73b292410dd6a570bc65a0f398e838b5adb141eb9dc81ad124fb46f80,

Attack Name	TYPE	VALUE
Gafgyt Botnet	SHA256	8d65b1c26285a08ee8cb11aa868984bd37553e2d2a8e5171d2460c32ca89a2e6, bf4178df292e66a5b2eca7a70df0feb76dfb4463cf70d92ee27d71c77af24f2d, 503a6e977c8fb68ffd015b1f882acdd9f90b98612dd41b676ee08ff10c7d0a90, 84d19f243cae6d14a15eced6cadd77f95dc494058f18a463fdcb18c0b382fe0e, ac0151ff4434a5bb31a4ecbfecc0ba66a6deaf344b6a10a9abf7cce7f6eb094a, be98fcecb03b2638632ebb05c1274d276918408b5f6543c6c7f57c80a7802e98, b95c0e0ba3004f72e0da0f618fe230d5053b8ddd402fdb17088e1ad6e605ef4e, 7917138fac54741ec12ed4d79594f399854996b1abd81ae5fb040b14b8ff483c, 208e4ae853feeede9be36b9385aa38e8547d83c979825ba7b9cb53a53c51c513, ea92d80d8b7d8be657eb667347be9e92004a54bf6f124e143744b6efada650cc, 881e7126f65751a41d59e846908246030f834ec03b15c1ef2cae8c4a1098cf15, 8347e8933783cd4129240b96ae5e665cedc5848ce1cbb7d9f58eb97aaa29b108, 18c58f83cf1e51d23eff699bec82fdef08f8a6585f51610bce162c9de25bc549, 60372d900506da46bf83e318f5f8f8c3219dcda3fca977f0172367d6825dfcdb, 1ef241ca77d2de374113db8b9e9bad4133142326683f2c7954bbab6415780dff, ec83fcc94d1fd981d13c7e5f3318671f3c96e677eaa956c7c1df4de2444c326f, 46ff9f7c0e437df7dd6e1c69790c8fc94e65091e9f3cf1f3243c808f1a1e8621, f0eb89b91e787324bb6f4a082fccea951b00f32ae62f31c80d9d83f4c53a0a65, a580c913a1e16d3fe4e7ebf8d155ac9cb08c1fabf831905776aa5ad6a6361f6f,
DroxiDat	SHA1	be9e23e56c4a25a8ea453c093714eed5e36c66d0, f98b32755cbfa063a868c64bd761486f7d5240cc, fd9016c64aea037465ce045d998c1eead3971d35
	MD5	1957deed26c7f157cedcbdae3c565cff, 8d582a14279920af10d37eae3ff2b705, 19567b140ae6f266bac6d1ba70459fbd

Attack Name	TYPE	VALUE
DroxiDat	Domain	powersupportplan[.]com, epowersoftware[.]com
	SHA256	926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732, a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e, a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4
	IPv4	93.115.25[.]41, 179.60.146[.]6, 194.165.16[.]63
	File Paths	C:\perflogs\syscheck.exe, C:\perflogs\a.dll, C:\perflogs\hos.exe, C:\perflogs\host.exe, C:\perflogs\hostt.exe, C:\perflogs\svch.dll, C:\perflogs\svchoct.dll, C:\perflogs\admin\svcpost.dll, C:\perflogs\admin\syscheck.exe, C:\perflogs\sk64.dll, C:\perflogs\clinic.exe
LummaC Stealer	MD5	**507bddfabd74a3d024b2ad5f67d666ea**
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock

Attack Name	TYPE	VALUE
Amadey Bot	SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d, d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c
	URLS	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe
	MD5	952d825a264745bb52b6977ba5983568
SectopRAT	SHA256	501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4, a3ceda3ef0a7b72145124def334dd3fa337614a1170960826016996151188fc5, 033cafb9fcd3d50d858164c117ee2a1c9e7fe95b4d027315bc9d1186e655d583, 81f4e0d6a70f14c3e07241196bd7f5318e302c28c64ca4bb876f4e25fbc3e5d2, ffd45c2b562d30113cb9a4823025a9a162503017e9d81fd96ddb5b98e5bb89bd, 501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4, fb553e12381d42a612c713968078424201794a35fd13c681ae7faa77bf18e553, 641710df66c792439f85b79879a268caa17b78ea0bf6924369fa6131fda01cd5
	URLs	hxxp[:]//patriciabono[.]com/BRR[.]exe, hxxp://fuji-iasi[.]ro/BRR[.]exe, hxxps://earthqik[.]co[.]za/BR[.]exe, hxxp://silversoft[.]in/BR[.]exe, hxxp://tbmcoats[.]com/BRRR[.]exe, hxxp://aviangas[.]co[.]ke/BRRRRAS[.]exe
	IP:PORT	95[.]143[.]190[.]57:15648
Monti Ransomware	SHA1	f1c0054bc76e8753d4331a881cdf9156dd8b812a, a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef
	URLs	hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion, hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion
JanelaRAT	Domains	cnt-blackrock[.]geekgalaxy[.]com, aigodmoney009[.]access[.]ly, freelascdmx979[.]couchpotatofries[.]org, 439mdxmex[.]damnserver[.]com,

Attack Name	TYPE	VALUE
JanelaRAT	Domains	897midasgold[.]ddns[.]me, disrupmoney979[.]ditchyourip[.]com, kakarotomx[.]dnsfor[.]me, skigoldmex[.]dvrcam[.]info, i89bydzi[.]dynns[.]com, infintymexbrock[.]geekgalaxy[.]com, brockmex57[.]golffan[.]us, j1d3c3mex[.]homesecuritypc[.]com, myfunbmdablo99[.]hosthampster[.]com, irocketxmtm[.]hopto[.]me, hotdiamond777[.]loginto[.]me, imrpc7987bm[.]mmafan[.]biz, dmrpc77bm[.]myactivedirectory[.]com, jxjmrpc797bm[.]mydissent[.]net, askmrpc747bm[.]mymediapc[.]net, myinfintyme09[.]geekgalaxy[.]com, infintymex747[.]geekgalaxy[.]com, infintymexb[.]geekgalaxy[.]com, jinfintymexbr[.]geekgalaxy[.]com, minfintymexbr[.]geekgalaxy[.]com, cinfintymex[.]geekgalaxy[.]com, 9mdxmex[.]damnserver[.]com, ikmidasgold[.]ddns[.]me, rexsrupmoney979[.]ditchyourip[.]com, kktkarotomx[.]dnsfor[.]me, megaskigoldmex[.]dvrcam[.]info, izt89bydzi[.]dynns[.]com, zeedinfintymexbrock[.]geekgalaxy[.]com
	IPv4	191.96.224[.]215, 192.99.169[.]240, 191.96.79[.]24, 167.88.168[.]132, 102.165.46[.]28, 189.89.15[.]37
	MD5	99bf0fba15aa3a9a59cbf442a80364e5, 999a9af2cd20a8c4bcf652e3523aafa3, 8b83e6b2d891cdf9250e9afd17081eab, e56d8632db98b07d2b49423f7dd64b42, c2f4cb0da89b4ea86ab5369a942428eb, 897e8483b673db70fdc5d3d111600cac, 72c02b3181c763d0e67f060e91635a97, c39f75423862c1525f089a5e966b9d04, e841f4691e5107fe360b1528384a96f0, 526a0b2d142567d8078e24ab0758fad7
BX RAT	MD5	7e4592e02951be844a2ee603d75070a6

Attack Name	TYPE	VALUE
BX RAT	SHA1	be7e5282efe58018b462a5ba0a78a7f01108460d
	SHA256	c6b3f1648f7137df91606f6aaaa6d25d672e18c8adcb178c6d8cdcf3148a3c81
AdLoad	SHA256	d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc, 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264, 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87, 7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dffc3, 4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32, 68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3, 1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5, 2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa, ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51, c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d
	URLs	hxxp://m.skilledobject[.]com/a/rep, hxxp://m.browseractivity[.]com/a/rep, hxxp://m.enchantedreign[.]com/a/rep, hxxp://m.activitycache[.]com/a/rep, hxxp://m.activityinput[.]com/a/rep, hxxp://m.opticalupdater[.]com/a/rep, hxxp://m.connectioncache[.]com/a/rep, hxxp://m.analyzerstate[.]com/a/rep, hxxp://m.essencecuration[.]com/a/rep, hxxp://m.microrotator[.]com/a/rep, hxxp://m.articlesagile[.]com/a/rep, hxxp://m.progresshandler[.]com/a/rep, hxxp://m.originalrotator[.]com/a/rep, hxxp://m.productiveunit[.]com/a/rep, hxxp://api.toolenviroment[.]com/l, hxxp://api.inetfield[.]com/l, hxxp://api.operativeeng[.]com/l, hxxp://api.launchertasks[.]com/l,

Attack Name	TYPE	VALUE
AdLoad	URLs	hxxp://api.launchelemnt[.]com/l, hxxp://api.validexplorer[.]com/l, hxxp://api.majorsprint[.]com/l, hxxp://api.essentialenumerator[.]com/l, hxxp://api.transactioneng[.]com/l, hxxp://api.macreationsapp[.]com/l, hxxp://api.commondevice[.]com/l, hxxp://api.compellingagent[.]com/l, hxxp://api.lookupindex[.]com/l, hxxp://api.practicalsync[.]com/l, hxxp://api.accessiblelist[.]com/l, hxxp://api.functionconfig[.]com/l
HUI Loader	MD5	b16bb2f910f21e2d4f6e2aa1a1ea0d8b, 809fcab1225981e87060033d72edaeaf
	SH1	a75e9b702a892cc3e531e158ab2e4206b939f379, 64f5044709efc77230484cec8a0d784947056022
	SHA256	8502852561fcb867d9cbf45ac24c5985fa195432 b542dbf8753d5f3d7175b120, 62fea3942e884855283faf3fb68f41be747c5baa 922d140509237c2d7bacdd17
Cuba Ransomware	SHA256	8a8cb6bd09ef535bfa09bee2678e0c75a0216b0cebd8fda5c9a 6f9735822e329, c6753d4cfe9072acce9c0a6fc84a15bd582d66d5e0a3a65c36c 6a3ba05b80a65, 7af49e468b3b2cc75b25ebcd711294373714585dca56196ed0 8430ba2fc849bd, 20c596d73812a9e9798e56cd6857451cad4686ed9212a4008 7d5a9fd9ab2532, a059ec5278a63614d358a743774bfb380dea1b370d9896104 9e6ba0ed754b234, 0910d1d5d0efa08c295f777551ec787511ab7625f0d08fed6d0 a5c9d6d6b963e, 65a60352271ce7ee4934967173ab68896726fe8e922e39fd2a 399d468657d2a5, 1cde997078f553ab9dbb0d94f948a26fbf4d3d3a20e801677d8 8daeb1dfb9e66, 81a22a4224f71bd66a89f2778b5842957b313ee5593c7c3e42 8d7a22507cda67
BUGHATCH	SHA256	58ba30052d249805caae0107a0e2a5a3cb85f3000ba5479fafb 7767e2a5a78f3
BURNTCIGAR	SHA256	1c2d7f19f8c12e055e1ba8cdf5334e6cb5510847783fbe36121 a35ad70f09eb3

Attack Name	TYPE	VALUE
Akira Ransomware	SHA1	24e7848dab0b82b200781630e617d6ed7e6016e7, 2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc, 30d49ced95cb9a0fb6526b30131501b28cbbc388, 5e6d77960065df450e0533f9a8409c7463292243, 688d67eb4ff993963c86297ab8345962334ead27, 76beb70b06cfe714c4fa250b6b2d1e5025fe3c50, 843f3ad221a9da48d82df672bd8806cc090430b5, 9180ea8ba0cdfe0a769089977ed8396a68761b40, 923161f345ed3566707f9f878cc311bc6a0c5268, 9a14a69eb279513cde2de0be538cc8d275fd34e9, bdb3fa0c50db18f7ada02b2060b4c5110016e859, db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49, f070a115100559dcaf31ce34d9e809a3134b2511, f2e6853050f76517a9a7d472f3a994d0ae8411cf
	MD5	302f76897e4e5c8c98a52a38c4c98443, 431d61e95586c03461552d134ca54d16, af95fbcf9da33352655f3c2bab3397e2, c7ae7f5becb7cf94aa107ddc1caf4b03, d25890a2e967a17ff3dad8a70bfdd832, e44eb48c7f72ffac5af3c7a37bf80587
	IPv4	172.82.86.148, 195.123.234.101
	Domain	akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion
	SHA256	89f5f29cf6b5bcfc85b506fb916da66cb7fd398cf6011d58e9409c7813e1a6f3, 27009c0abd2709cd5cac4c0135b8f3bed3229b0921601638ba9e90713ede91ea, 379ef7c4f6dfae8cc0c8556861ff41930b88c7d9b107a5de10ccd194e1bda0cb, 8738ba49fcd520789569aea7bf7af890741a745c79ae2bef49b93fb46c076c2b, d371ee0aa4fa710c00173d296c999a5497a18b38c80095db68a2dc5e46ed35f7, 2a9257c6c74e37d051f78ed5abaa620b71b27fa3604798af077256a128d911bb, 3f4ceeada7ff021c30df1646437d2ab0e55997bbb281444501f6d1f4ea8fa209, fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776, c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777, 4cb8365b18b1c319d374be0b9d219144c20fb8714e9cf346e655f854d2c60170, 772eb611c9ca20b461536fd0bd87d553dcecf3f4c82e26c2378cad40bbf4b0b0, 2e2ad6392e75d5a5155498c2a76cb373d17ca3ad4ba57c6d33c623fca5e29342,

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda, 619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4, 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488, 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50, 99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba, a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce, b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa, c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598, d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee
PlugX	SHA256	041d8c3460ce0b25dc6b597a69cbe0bc95f9f281bb66e4cbcd045ea69e308777, 10e60613394aa48b99b5bbaa13df6d5209912e64612e8dd2d09d24546e09d74f, 8649235c0c4deecabf319fb0b7e4842bdac75baa221973bf9f095114c3cbb252, 8978af4528721d4e1178ab36f7d90bc5d5206610178d5491fd58105c8eaf0448, 995664972e499c9ff036241dca05d03d902916d9c5c126f27d23403288cf8144, b2f005fc3eeff7ba5f8adac02705ad271381ac1a296e716da0a8eccf13161362, 03c559361d21802ea29a2803584af1bf41ced2989cdddec694995ae193622e10, 49f98c7452670fde067ca85d51b44d8cb7109ead55fa94e2118b26716f78911b, 11be38b5e7d83ce275a39dc61bf40592131bfe8b8e22d70bd4c67395ee3679c9, 207d563033cb6c28d64b3b3ff6de64a9af510981bf82e48820cf223211a6b36b

Attack Name	TYPE	VALUE
GuLoader	SHA256	81d7b35cc9d332c69e374bb7727e3c63bc44caf1dc21a80cba841f532fdd359d, 7699f9c7977b3dff0510173ef2e9854dff1e2ede9a0b3be176a6c06cad46f6a9, 1c3898115a8187b236f40dbeb117557ab42489a2a1d1255fa0dbf12300096b73, 1c3898115a8187b236f40dbeb117557ab42489a2a1d1255fa0dbf12300096b73, 7c73489a0aa6bcabf4307d22af917a663dc8f6615312abd81806769e36232a04, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, e20123e0f8e42012759e848cb456c6bb60f09fcf0fc76b2494f8ce1dbb023e0b, b4d2e40296ddd8f6127f9d2ba3703b134fee350602ee9c90f6d73737a2186a86, b4d2e40296ddd8f6127f9d2ba3703b134fee350602ee9c90f6d73737a2186a86, 769e6002b8038a0a87c66347326d314fa597a228c04c9ec58e3c2a6e686da7db, 769e6002b8038a0a87c66347326d314fa597a228c04c9ec58e3c2a6e686da7db, dc3e8bcb96174f4eebeace1b2f8d1dd0e21f1113005c093d6605953e7f5d41e0, 88298b8df4baa6e0947191c55624418c9968940d5b4bee55c44d320b4bbcfb36, 7fbdcfc41f0c35738dc338732df68db6c9890f48b1281bf2f013cc892b5da202, b72134165e07293b02438e4ebf025481e11be7d5590d2714c383c216a53357c6, 97548d4f2ed2306e827adbe6d3ce84f1aca47e9a0be0c22dd0a7a053ebcd64b2, 6b91613f78377d180e0385169b9582636dabd880e7e956b2d42495d1b627e7ea, 91a0627626abd3ba900aa0c377d77da88ec4f7d24aedd09d0d9da344e46b992e, bc16b3c2eea43cd58cd903b2c9a80daecf5d0bde654f4b7cb3800d0ef152d32a, 6174c652fbbcd3fa7fb6b3c49f11304a75c089f12b20f21c5e2c05ef30d55c0e, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 33f0aeb010952556d8dd51e16a4c4440278a3d7c036cd4e666b1ac8233607e1b,

Attack Name	TYPE	VALUE
GuLoader	SHA256	42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, 42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, b3441cd04205175c973de6e529b4ce95c76b42b43c9ff6cf28d22cbf4c5abf95, 1d956e3ac17a4da68760e042410f5c27818f0257e7bb20a5460c76ca37370de5, b3441cd04205175c973de6e529b4ce95c76b42b43c9ff6cf28d22cbf4c5abf95, 61ba44ffbcc11625b7685394d28fd6022bc78c9aaf4342d55db66a6163fe7a06, 040e86b9d787d3d5af074511c8aeb6a0ca11225c1ce2dccdfc6980bdaa163647, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 50a055c22972c8fc0ab0a5f26afb453e630be88e9eb9c3592a137a2a7dd6a10c, 5cd77da31b20eb6c30380095e2fcc9711a305c8b1ddd9718d15149b04cae6495, 50a055c22972c8fc0ab0a5f26afb453e630be88e9eb9c3592a137a2a7dd6a10c, a37065097b533862a2432be87cb63a9dd755397439aae30a700b09e7abad0691, 3ab67edd421427d8e26c522fde52b72e0822fab92f3a4dae0b5305e2b908f15a, 3ab67edd421427d8e26c522fde52b72e0822fab92f3a4dae0b5305e2b908f15a, b4fe86bc79f2b87ee1467ba230c4f69839b7ef72df78b0ca70ed729b2a7f6936, 715f585fbea156c841e4f47a830c56842b01239ad3bc56a0f2fabe269a227aad, 0c068a91d2f44fd614d7429e9d13020d1f59031c26d5d8bf35e76cd3335f1d55, 67434f853750f35f663aea7c2a731961d02557766d0fb6492b86c5e4a155f560, a318c671ef27d19bdea95d9d20b6894a39bd156cf3ab7ff94e295117a3cdf910, df41db44dea7e6a49689e58efa4ee7f3a18ab82f77aff5cfc3fafa4ab3039956, e19c39ac680dec3b1003b2840f24976c1b86e6e09a4e27e8166df910f55ba917, ee6bfabb37ffee5c31e1de467a9b816d5d079d3867c107c7f16753c61dfc86ef, 236c73a241d229cc820b4fa2aa914403151deb84b90939ac4760460fc107dda4,

Attack Name	TYPE	VALUE
GuLoader	SHA256	236c73a241d229cc820b4fa2aa914403151deb84b90939ac4760460fc107dda4, ee6bfabb37ffee5c31e1de467a9b816d5d079d3867c107c7f16753c61dfc86ef, b48a5ebf4d21ce938606b70952e053ff15581a50d96e1e2cec000a8173edade3, b48a5ebf4d21ce938606b70952e053ff15581a50d96e1e2cec000a8173edade3
DarkMe	SHA256	a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569, 7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5, e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0
Remcos RAT	SHA256	08628529673070b41cd0774e0b5e1d22747cd0fc09c82b479143b538b67d976b, ca9c5b008a075bbdb57a89b0aef111458f5f9c8ee21f279a06abc481d35ba324, ec901217558e77f2f449031a6a1190b1e99b30fa1bb8d8dabc3a99bc69833784, b89e2bec5923fcd2b7c4f50f80dd5cd992a45409424a8cd1711c453dc38a2dc8, d5082b124437716d3f436aef25c69662dbed756d681e9f2a5a82d6c35fa0a7bb
Scarab Ransomware	SHA1	E2EAA1EE0B51CAF803CEEDD7D3452577B6FE7A8D, 8F1374D4D6CC2899DA1251DE0325A7095E719EDC
Spacecolon	IPV4	3.76.107[.]228, 87.251.64[.]19, 87.251.64[.]57, 87.251.67[.]163, 162.255.119[.]146, 185.170.144[.]190, 185.202.0[.]149, 193.37.69[.]152, 193.37.69[.]153, 193.149.185[.]23, 206.188.196[.]104, 213.232.255[.]131
	SHA1	40B8AF12EA6F89DB6ED635037F468AADEE7F4CA6, 1CB9320C010065E18881F0AAA0B72FC7C5F85956, EF911DB066866FE2734038A35A3B298359EDABCE

Attack Name	TYPE	VALUE
Spacecolon	SHA1	0A2FA26D6EAB6E9B74AD54D37C82DEE83E80BDD7, B916535362E2B691C6AEF76021944B4A23DDE190, 95931DE0AA6D96568ACEBC11E551E8E1305BF003, 6700AFB03934B01B0B2A9885799322307E3299D5, 4B07391434332E4F8FAADF61F288E48389BCEA08, B9CF8B18A84655D0E8EF1BB14C60763CEFFF9686
QuiteRAT	SHA256	ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
CollectionRAT	SHA256	db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984, 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df
Trash Panda ransomware	MD5	A0fea954561663f60059420e6c78fa5c
	SHA1	D5d37ae269008e9bfddc171c3b05bd3d43a5cd4d
	SHA256	ce5cf3b964e636d546bf2c52423296bda06b7fe47e6f8a757f165a3be93c88db
Agniane Stealer	MD5	522101881b87ccda4d78fac30e951d190d20e90382f881116201ac7c9298aab6a1b5e20b58d23b26f640f252ece0891b5C0F65523F7ECB773C599B59D5CC3578a2b20120a92c3de445b0b384a494ed39d811a57bc0e8b86b449277f9ffb50cc9b62ef0920a545f547d6cd3cd2abd60d2
	Host Name	Central-cee-doja[.]ru
DEPTHCHARGE	MD5	c5c93ba36e079892c1123fe9dffd660f, dde2d3347b76070fff14f6c0412f95ba, 03e07c538a5e0e7906af803a83c97a1e, 0dd78b785e7657999d05d52a64b4c4cf, 35a432e40da597c7ab63ff16b09d19d8, 806250c466824a027e3e85461dc672db, 830fca78440780aef448c862eee2a8ac, b354111afc9c6c26c1475e761d347144, b745626b36b841ed03eddfb08e6bb061, b860198feca7398bc79a8ec69afc65ed, c2e577c71d591999ad5c581e49343093, e68cd991777118d76e7bce163d8a2bc1, ed648c366b6e564fc636c072bbcac907, ff005f1ff98ec1cd678785baa0386bd1

Attack Name	TYPE	VALUE
SKIPJACK	MD5	d81263e6872cc805e6cf4ca05d86df4e, ad1dc51a66201689d442499f70b78dea, 3273a29d15334efddd8276af53c317fb, 446f3d71591afa37bbd604e2e400ae8b, 87847445f9524671022d70f2a812728f, 9aa90d767ba0a3f057653aadcb75e579, e4e86c273a2b67a605f5d4686783e0cc, ec0d46b2aa7adfdff10a671a77aeb2ae
FOXTROT	MD5	a28de396aa91b7faca35e861b634c502

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

September 04, 2023 . 5:45 AM

More at www.hivepro.com