Date of Publication
July 4, 2023

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

JUNE 2023

Table Of Contents

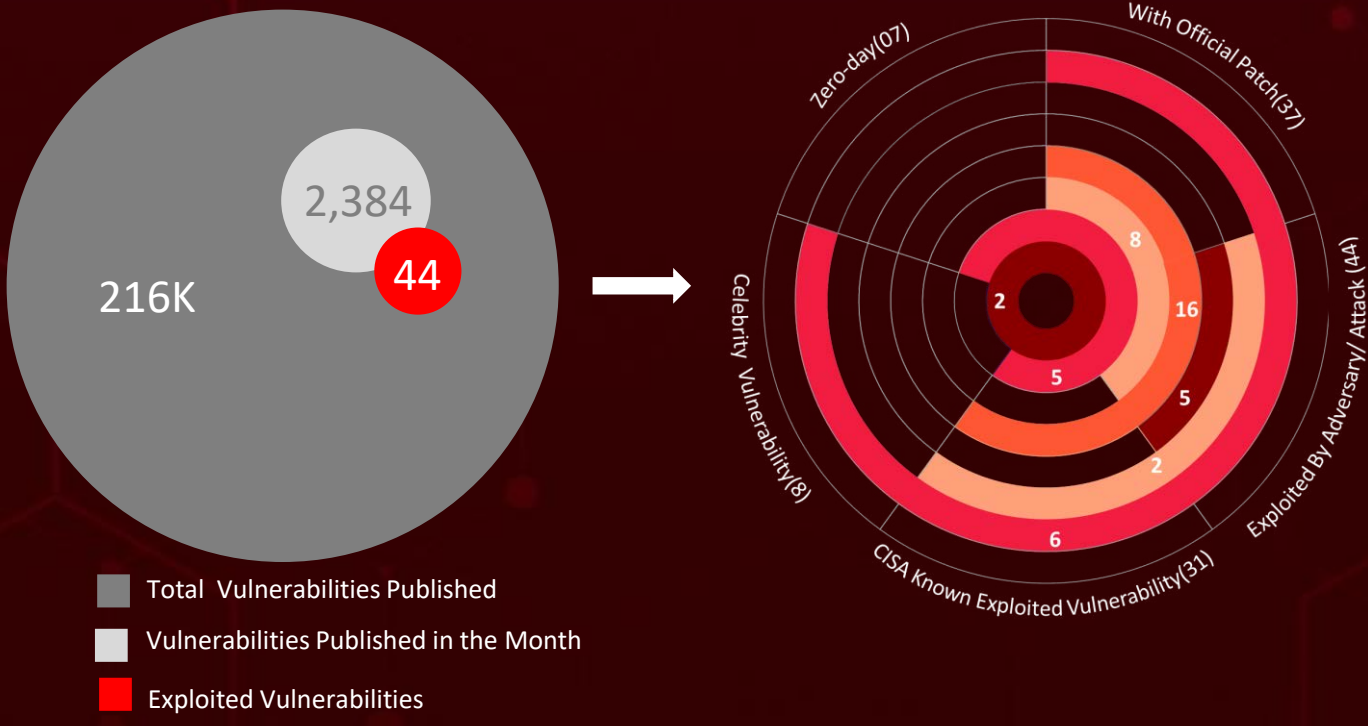
Summary

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

During the month of June, there was a resurgence of ransomware attacks, with strains like **Clop** and **LockBit** actively targeting victims. As ransomware continues to evolve and grow in sophistication, organizations must take steps to protect themselves by implementing comprehensive backup and disaster recovery strategies and training employees on how to recognize and avoid phishing attacks.

Attackers are leveraging a specific vulnerability (**CVE-2023-27997**) in FortiOS and FortiProxy SSL-VPN, enabling remote attackers to execute arbitrary code. In addition to ransomware attacks, several malware families, including **Horabot**, **WhisperGate**, **NODEBOT, AHKBOT, SunSeed,** and **Mirai Botnet** 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-2023-3079** vulnerability is a high-severity zero-day vulnerability that was exploited in attacks. It could allow attackers to execute arbitrary code, potentially leading to data theft, system compromise, and other malicious activities.



Insights

Horabot

A new botnet program targeting Spanish-speaking users in the Americas.

Volt Typhoon

Targeting United States and the U.S. island territory of Guam.

Shampoo

New ChromeLoader campaign infecting chrome and stealing data

Condi

Botnet exploiting TP-Link Archer Wi-Fi routers for DDOS attacks

Government, Technology, Financial, Manufacturing, Healthcare and were the most targeted sectors

UNC3886

Threat group has been actively exploiting the CVE-2023-20867 vulnerability

78

number of vulnerabilities were patched during Microsoft Patch Tuesday

Flea

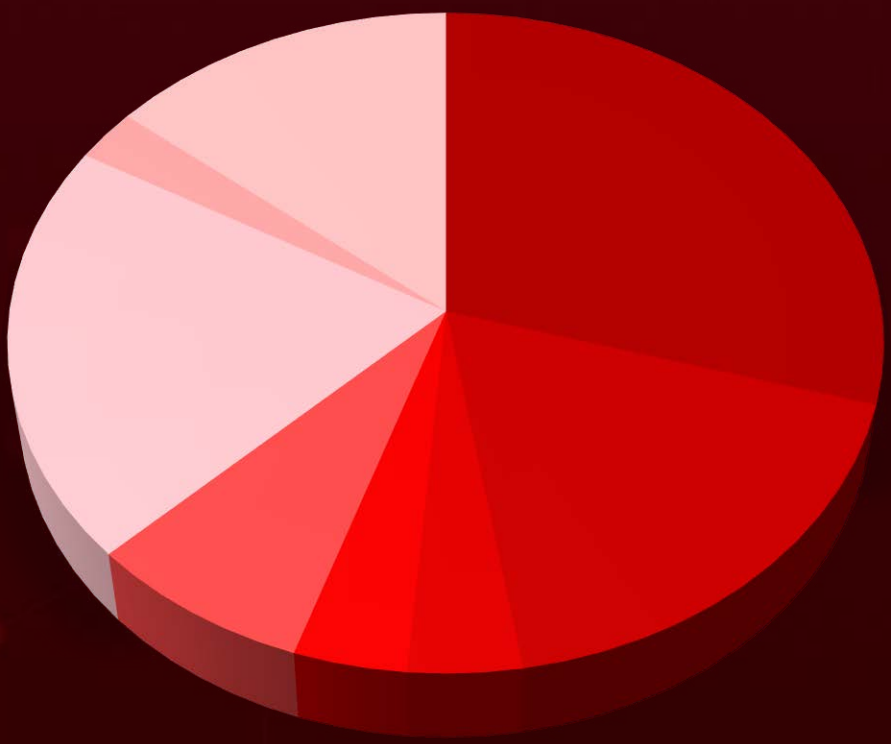
Threat group targets foreign ministries with new Backdoor.Graphican

United States, Mexico, Honduras, Paraguay, and **Nicaragua,** were the most targeted countries

CrossLock Ransomware

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

Threat Landscape



Celebrity Vulnerabilities

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Microsoft Windows	Asylum Ambuscade
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	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	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	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	LockBit Ransomware
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-2021-4034		Red Hat Polkit	Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	WhisperGate
Red Hat Polkit Out-of-Bounds Read and Write Vulnerability (PWNKIT)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-125	T1005: Data from Local System, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	https://bugzilla.redhat.com/show_bug.cgi?id=2025869

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523	✓	Microsoft Exchange Server	Cadet Blizzard (aka DEV-0586, Ruinous Ursa) & ChamelGang
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	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 (aka DEV-0586, Ruinous Ursa)
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	WhisperGate & ChamelDoH
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

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207		Microsoft Exchange Server	ChamelGang & Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**ZERO-DAY**	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	WhisperGate & ChamelDoH
Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-22	T1190:Exploit Public-Facing Application	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0708	BlueKeep	Microsoft Remote Desktop Services	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows_:-:*:*:*:*:*:*:*	LockBit Ransomware
Microsoft Remote Desktop Services Remote Code Execution Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1059:Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	MOVEit Transfer	✓	✓	✓
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	Zoho ManageEngine	✓	✓	✓
CVE-2021-27860	FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit	FatPipe WARP, IPVPN, and MPVPN software	✗	✓	✓
CVE-2023-3079	Google Chrome Type Confusion Vulnerability	Google Chrome	✓	✓	✓
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-27997	Fortinet heap-based buffer overflow Pre-Auth Vulnerability	FortiOS and FortiProxy SSL-VPN	✓	✓	✓
CVE-2023-28299	Visual Studio Spoofing Vulnerability	Visual Studio	✗	✗	✓
CVE-2023-20867	VMware Tools authentication bypass	VMware Tools	✓	✓	✓
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF/NG	✗	✓	✓
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2021-22986	F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability	F5 BIG-IP and BIG-IQ Centralized Management	✗	✓	✓
CVE-2019-0708	Microsoft Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Remote Desktop Services	✗	✓	✓
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS	✗	✓	✓
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Server and Data Center	✗	✓	✓
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓
CVE-2021-4034	Red Hat Polkit Out-of-Bounds Read and Write Vulnerability	Red Hat Polkit	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2017-12149	Red Hat JBoss Application Server Remote Code Execution Vulnerability	Red Hat JBoss Application 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-2019-18935	Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	Telerik UI for ASP.NET AJAX	✗	✓	✓
CVE-2017-9248	Progress Telerik UI for ASP.NET AJAX and Sitefinity Cryptographic Weakness Vulnerability	ASP.NET AJAX and Sitefinity	✗	✓	✓
CVE-2017-11357	Telerik UI for ASP.NET AJAX Insecure Direct Object Reference Vulnerability	Telerik User Interface (UI) for ASP.NET AJAX	✗	✓	✓
CVE-2017-11317	Telerik UI for ASP.NET AJAX Unrestricted File Upload Vulnerability	Telerik User Interface (UI) for ASP.NET AJAX	✗	✓	✓
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability	TP-Link Archer AX21 versions before 1.1.4 Build 20230219	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-27240	Tenda Command Injection Vulnerability	Tenda AX3	✗	✗	✗
CVE-2019-17621	D-Link DIR-859 Remote Command Injection Vulnerability	D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	✗	✗	✓
CVE-2019-12725	Zeroshell Remote Command Execution Vulnerability	Zeroshell	✗	✗	✓
CVE-2019-20500	D-Link Remote Command Execution Vulnerability	D-Link DWL	✗	✗	✓
CVE-2021-25296	Nagios OS Command Injection	Nagios XI	✗	✓	✗
CVE-2021-46422	Telesquare Router Command Injection Vulnerability	Telesquare Router	✗	✗	✗
CVE-2022-27002	Arris Remote Command Injection Vulnerability	Arris TR3300	✗	✓	✗
CVE-2022-29303	SolarView Compact Command Injection Vulnerability	SolarView Compact	✗	✗	✗
CVE-2022-30023	Tenda Router Command Injection Vulnerability	Tenda Router	✗	✗	✗
CVE-2022-30525	Zyxel Command Injection Vulnerability	Zyxel Multiple Firewalls	✗	✓	✗
CVE-2022-31499	Nortek Linear eMerge Command Injection Vulnerability	Nortek Linear eMerge	✗	✗	✗
CVE-2022-37061	FLIR Unauthenticated OS Command Injection Vulnerability	All FLIR AX8	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2022-40005	Intelbras Command Injection Vulnerability	Intelbras	✗	✗	✓
CVE-2022-45699	APsystems Remote Command Execution Vulnerability	APsystems Remote	✗	✗	✓
CVE-2023-25280	D-link Command injection vulnerability	D-Link DIR820LA1_FW105B03	✗	✗	✓
CVE-2021-44026	Roundcube Webmail SQL Injection Vulnerability	Roundcube: 1.3.0 - 1.4.11	✗	✓	✓
CVE-2020-12641	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube: 1.2.0 - 1.4.3	✗	✓	✓
CVE-2020-35730	Roundcube Webmail CrossSite Scripting (XSS) Vulnerability	Roundcube: 1.2.0 - 1.4.9	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Horabot	Botnet	-	-	-	Phishing emails
Clop	Ransomware	CVE-2023-34362	Progress MOVEit Transfer	✓	Phishing emails
MediaArena	Browser hijacker	-	-	-	Malvertising campaigns
NODEBOT	Loader	CVE-2022-30190	Microsoft Windows	✓	Spear-phishing emails
AHKBOT	Banking Trojan	CVE-2022-30190	Microsoft Windows	✓	Spear-phishing emails
DoubleFinger loader	Loader	-	-	-	Phishing emails
GreetingGhoul stealer	Stealer	-	-	-	DoubleFinger loader
VirtualPita backdoor	Backdoor	CVE-2023-20867	VMware Tools: 10.0.0 - 12.2.0	✓	Utilizing a zero-day vulnerability (CVE-2023-20867)
VirtualPie backdoor	Backdoor	CVE-2023-20867	VMware Tools: 10.0.0 - 12.2.0	✓	Utilizing a zero-day vulnerability (CVE-2023-20867)
SunSeed	Loader	CVE-2022-30190	Microsoft Windows	✓	Spear-phishing emails

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LockBit	Ransomware	CVE-2023-0669 CVE-2023-27350 CVE-2021-44228 CVE-2021-22986 CVE-2020-1472 CVE-2019-0708 CVE-2018-13379	Fortra GoAnywhere MFT,PaperCut MF/NG,Apache Log4j2,F5 BIG-IP and BIG-IQ Centralized Management, Microsoft Netlogon, Microsoft Remote Desktop Services, and Fortinet FortiOS	✓	Phishing
WhisperGate	Wiper	CVE-2021-26084 CVE-2020-1472 CVE-2021-4034 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server	✓	By exploiting web servers
ChamelDoH	Backdoor	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	Red Hat JBoss Application Server and Microsoft Exchange Server	✓	-
Stealth Soldier	Backdoor	-	-	-	-
Satacom (aka LegionLoader)	Loader	-	-	-	Malicious ads or links

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Mystic Stealer	InfoStealer	-	-	-	-
XMRig	Miner	-	-	-	-
Cayosin	Botnet	-	-	-	-
Shampoo	Browser extension	-	-	-	Malicious VBScript files from malicious websites
Condi	Botnet	CVE-2023-1389	TP-Link Archer AX21 versions before 1.1.4 Build 20230219	✓	-
Tsunami	Botnet	-	-	-	Exploit kits
Shellbot	Botnet	-	-	-	
FadeStealer	InfoStealer	-	-	-	Phishing emails
Mirai	Botnet	CVE-2019-12725 CVE-2019-17621 CVE-2019-20500 CVE-2021-25296 CVE-2021-46422 CVE-2022-27002 CVE-2022-29303 CVE-2022-30023 CVE-2022-30525 CVE-2022-31499 CVE-2022-37061 CVE-2022-40005 CVE-2022-45699 CVE-2023-1389 CVE-2023-25280 CVE-2023-27240	Zeroshell; D-Link DIR-859 Wi-Firouter; D-Link DWL-2600AP; TelesquareSD TCW3B11.1.0; Arris TR3300v1.0.13;SolarViewCompact; Tenda ONTGPON AC1200DualbandWiFi HG9v1.0.1; Zyxel MultipleFirewalls; Nortek LineareMerge E3-Series devicesbefore 0.32-08f; All FLIR AX8	✓	Exploiting vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
CHM malware	Unknown	-	-	-	Phishing emails
AblyGo backdoor	Backdoor	-	-	-	Phishing emails
Backdoor.Graphical	Backdoor	CVE-2020-1472	Microsoft Netlogon		Unknown
JokerSpy	Backdoor	-	-	-	Unknown
EarlyRat	Backdoor	-	Windows	-	Phishing emails
PindOS	Backdoor	-	Windows	-	Phishing emails
WarZone	Backdoor	-	Windows	-	Phishing emails

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Volt Typhoon (aka BRONZE SILHOUETTE)	Information theft and espionage	China	CVE-2021-40539 CVE-2021-27860	-	Zoho ManageEngine, FatPipe WARP, IPVPN, and MPVPN software
Asylum Ambuscade	Financial crime and espionage	Unknown	CVE-2022-30190	NODEBOT, AHKBOT, SunSeed	Microsoft Windows
UNC3886	Information theft and espionage	China	CVE-2023-20867	VirtualPita and VirtualPie backdoors	VMware Tools
ChamelGang	Information theft and espionage	China	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	ChamelDoH	Red Hat JBoss Application Server and Microsoft Exchange Server
Cadet Blizzard (aka DEV-0586, Ruinous Ursa)	Financial Crime	Russia	CVE-2021-26084 CVE-2020-1472 CVE-2021-4034 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	WhisperGate	Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server
STORM-1359 (Anonymous Sudan)	Information theft and espionage	Unknown	-	-	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Diicot (aka Mexals)	Information theft and espionage	Unknown	-	Mirai, Cayosin, XMRig	-
Flea (APT15, Playful Taurus, BackdoorDiplomacy, Vixen Panda, Ke3Chang, Playful Dragon, Bronze Palace, and NICKEL)	Information theft and espionage	China	CVE-2020-1472	Backdoor.Graphical	Microsoft Netlogon
Red Eyes (APT 37, Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	Information theft and espionage	North Korean	-	FadeStealer, CHM malware, AblyGo backdoor	-
APT28	Espionage	Russia	CVE-2020-35730 CVE-2021-44026 CVE-2020-	-	Roundcube: 1.2.0 - 1.4.11
Andariel	Information Theft, Espionage and Monetary Gains	North-Korea	-	EarlyRat	Windows

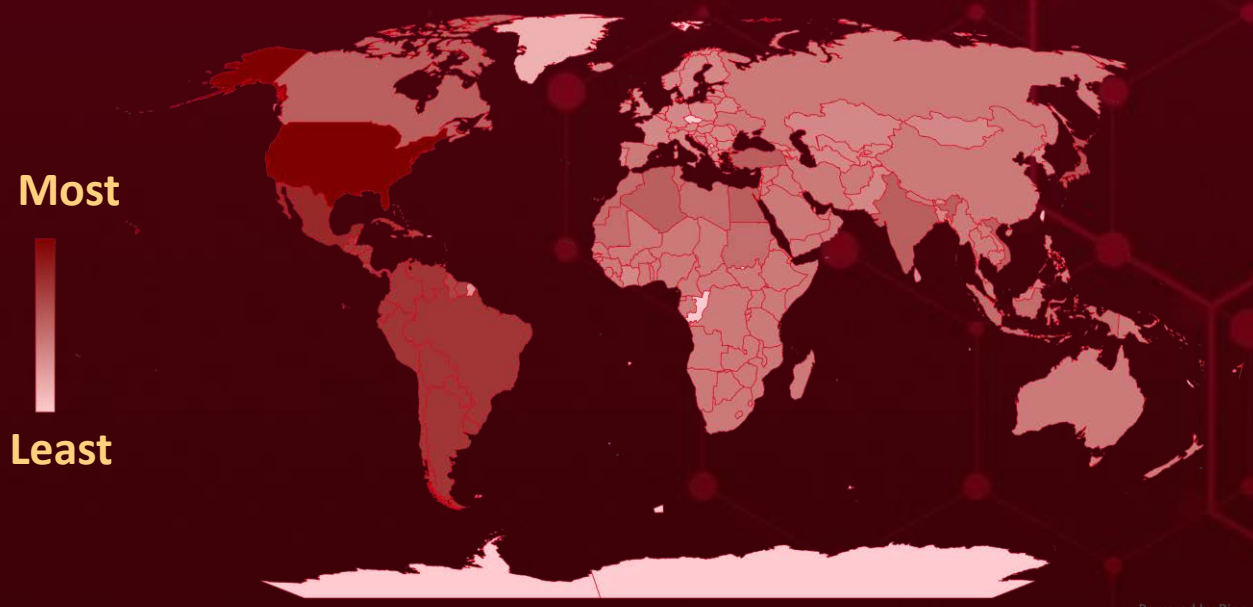
Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
ZOHO	ManageEngine	Zoho ManageEngine ADSelfService Plus: 6000 - 6113
Progress MOVEit	Managed file transfer software	MOVEit Transfer 2023.0.0(15.0),MOVEit Transfer 2022.1.x(14.1),MOVEit Transfer 2022.0.x(14.0),MOVEit Transfer 2021.1.x(13.1),MOVEit Transfer 2021.0.x(13.0),MOVEit Transfer 2020.1.x(12.1),MOVEit Transfer 2020.0.x(12.0) or older,MOVEit Cloud
FatPipe	Network product	FatPipe WARP, IPVPN, and MPVPN software
	Browser	Google Chrome: 100.0.4896.60 - 114.0.5735.91
FORTRA	File transfer	GoAnywhere MFT: 4.0.2 - 7.1.1
FORTINET	Operating System	FortiOS and FortiProxy SSL-VPN
	IDE	Visual Studio: 2017 version 15.9; 2022 version 17.4, 17.4, 17.2, 17.0; 2019 version 16.11
vmware	Application	VMware Tools: 10.0.0 - 12.2.0

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
PaperCut	PaperCut MF/NG	PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9
	Software framework	Red Hat Polkit
	Server Application	Red Hat JBoss Application Server
f5	Application Delivery and Centralized Management	F5 BIG-IP and BIG-IQ Centralized Management
Microsoft	Remote desktop	Microsoft Remote Desktop Services
	Exchange Server	Microsoft Exchange Server
ATLASSIAN	Collaboration and management tools	Atlassian Confluence Server and Data Center
Telerik by Progress	Application development tool	Telerik UI for ASP.NET AJAX
Tenda	Network product	Tenda AX3 Version: 16.03.12.11
	Router	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1
D-Link	Router	D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01
	WAP	D-Link DWL-2600AP 4.2.0.15
	Router	D-Link DIR820LA1_FW105B03

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
telesquare	Router	Telesquare SDT-CW3B1 1.1.0
ARRIS	Router	Arris TR3300 v1.0.13
SOLARVIEW	Monitoring system	SolarView Compact version: 6.00
ZYXEL	Firewalls	Zyxel Multiple Firewalls
NORTEK Lighting Lives...	Network appliance	Nortek Linear eMerge E3-Series devices before 0.32-08f
FLIR	Operating system	All FLIR AX8 version up to and including 1.46.16
intelbras	Router	Intelbras WiFiber 120AC inMesh before 1-1-220826
APsystems	ECU	APSystems ECU-R version 5203
ZEROSHELL Net Services	**Router**	Zeroshell versions: 3.9.0 - 3.9.0
Nagios	Operating system	Nagios XI version xi-5.7.5
roundcube open source webmail software	Webmail	Roundcube: 1.3.0 - 1.4.11 Roundcube: 1.2.0 - 1.4.3 Roundcube: 1.2.0 - 1.4.9

Targeted Countries



Color	Countries
	United States
	Mexico
	Honduras
	Paraguay
	Nicaragua
	Brazil
	Guatemala
	Chile
	Bolivia
	Uruguay
	Colombia
	Panama
	Cuba
	Argentina
	Peru
	Ecuador
	Venezuela
	Trinidad and Tobago
	Jamaica
	Haiti
	Costa Rica
	Saint Lucia
	Bahamas
	Guyana

Color	Countries
	Dominica
	Belize
	Dominican Republic
	Antigua and Barbuda
	El Salvador
	Suriname
	Grenada
	Barbados
	Japan
	Egypt
	Algeria
	Turkey
	Canada
	Vietnam
	India
	Saint Kitts & Nevis
	Indonesia
	Morocco
	Mauritania
	Tunisia
	St. Vincent & Grenadines

Color	Countries
	Sudan
	Libya
	Tanzania
	Ethiopia
	Papua New Guinea
	Guinea-Bissau
	South Africa
	Cambodia
	Niger
	Central African Republic
	Qatar
	Djibouti
	Seychelles
	Chad
	Fiji
	Cameroon
	Ghana
	Iran
	Oman
	Iraq
	Burkina Faso
	Israel
	Rwanda
	DR Congo

Color	Countries
	Saudi Arabia
	Bahrain
	Singapore
	Jordan
	South Sudan
	Benin
	Gambia
	China
	Timor-Leste
	Zambia
	Congo
	Lebanon
	Nigeria
	Lesotho
	Eritrea
	Afghanistan
	Brunei
	Uganda
	Philippines
	Ukraine
	Russia
	Burundi
	Eswatini
	Malawi

Color	Countries
	Sao Tome & Principe
	Malaysia
	Senegal
	Mali
	Sierra Leone
	Australia
	Somalia
	Mauritius
	South Korea
	Angola
	Spain
	Equatorial Guinea
	Gabon
	Mozambique
	Syria
	Myanmar
	Thailand
	Namibia
	Togo
	Nepal
	Comoros
	New Zealand

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1190 Exploit Public-Facing Application	**T1027** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1566** Phishing	**T1082** System Information Discovery
T1486 Data Encrypted for Impact	**T1036** Masquerading	**T1071** Application Layer Protocol	**T1083** File and Directory Discovery	**T1204** User Execution
T1134 Access Token Manipulation	**T1497** Virtualization /Sandbox Evasion	**T1095** Non-Application Layer Protocol	**T1068** Exploitation for Privilege Escalation	**T1113** Screen Capture
T1574 Hijack Execution Flow	**T1140** Deobfuscate/ Decode Files or Information	**T1102** Web Service	**T1564** Hide Artifacts	**T1055** Process Injection
T1005 Data from Local System	**T1078** Valid Accounts	**T1203** Exploitation for Client Execution	**T1016** System Network Configuration Discovery	**T1562.001** Disable or Modify Tools

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
NODEBOT	SHA1	C98061592DE61E34DA280AB179465580947890DE
Sunseed	IPV4	146[.]70[.]79[.]119
AHKBOT	SHA1	57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B 64F5AC9F0C6C12F2A48A1CB941847B0662734FBF 557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF F85B82805C6204F34DB0858E2F04DA9F620A0277 5492061DE582E71B2A5DA046536D4150F6F497F1 C554100C15ED3617EBFAAB00C983CED5FEC5DB11 AD8143DE4FC609608D8925478FD8EA3CD9A37C5D F2948C27F044FC6FB4849332657801F78C0F7D5E 7AA23E871E796F89C465537E6ECE962412CDA636 384961E19624437EB4EB22B1BF45953D7147FB8F 7FDB9A73B3F13DBD94D392132D896A5328DACA59 3E38D54CC55A48A3377A7E6A0800B09F2E281978 7F8742778FC848A6FBCFFEC9011B477402544171 29604997030752919EA42B6D6CEE8D3AE28F527E 7A78AF75841C2A8D8A5929C214F08EB92739E9CB
Stealth Soldier	IPV4	185.125.230[.]216 185.125.230[.]116 94.156.33[.]228 94.156.33[.]229 185.125.230[.]224 185.125.230[.]220
	Domains	filestoragehub[.]live customjvupdate[.]live filecloud[.]store webmailogemail[.]com loglivemail[.]com 2096[.]website
DoubleFinger loader	MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ea D9130cb36f23edf90848ffd73bd4e0e0

Attack Name	TYPE	VALUE
DoubleFinger loader	Domain	cryptohedgefund[.]us
GreetingGhoul stealer	MD5	642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e
VirtualPita backdoor	MD5	8e80b40b1298f022c7f3a96599806c43 61ab3f6401d60ec36cd3ac980a8deb75 2c28ec2d541f555b2838099ca849f965 744e2a4c1da48869776827d461c2b2ec 93d50025b81d3dbcb2e25d15cae03428 fe34b7c071d96dac498b72a4a07cb246
	SHA1	e9cbac1f64587ce1dc5b92cde9637affb3b58577 93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84 e35733db8061b57b8fcdb83ab51a90d0a8ba618c a3cc666e0764e856e65275bd4f32a56d76e51420 abff003edf67e77667f56bbcfc391e2175cb0f8a 0962e10dc34256c6b31509a5ced498f8f6a3d6b6
VirtualPie backdoor	MD5	**61ab3f6401d60ec36cd3ac980a8deb75**
	SHA1	93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84
	SHA256	4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d
LockBit Ransomware	SHA256	149d691411f10f8ec7af43f0237ccfab5b65a9ae73718acf1e0cc0dbdea36ebd
WhisperGate	MD5	3a2a2de20daa74d8f6921230416ed4e6
ChamelDoH	SHA256	34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7 4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0 6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe 70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007 92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a

Attack Name	TYPE	VALUE
Condi	SHA256	509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084 593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315 5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612 cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772 ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15 f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf
Tsunami	MD5	822b6f619e642cc76881ae90fb1f8e8e
	C2	ircx.us[.]to:53 ircxx.us[.]to:53
Backdoor.Graphical	**SHA256**	**4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5 a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8 02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5 617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd 858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253 fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476 177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf 8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286 865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48 d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30**
FadeStealer	MD5	f44bf949abead4af0966436168610bcc
CHM malware	MD5	1352abf9de97a0faf8645547211c3be7

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34362		MOVEit Transfer 2023.0.0(15.0),MOVEit Transfer 2022.1.x(14.1),MOVEit Transfer 2022.0.x(14.0),MOVEit Transfer 2021.1.x(13.1),MOVEit Transfer 2021.0.x(13.0),MOVEit Transfer 2020.1.x(12.1),MOVEit Transfer 2020.0.x(12.0) or older,MOVEit Cloud	Lace Tempest (aka FIN11, DEV-0950), TA505 (Graceful Spider, Gold Evergreen, Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo, Spandex)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	Clop Ransomware
Progress MOVEit Transfer SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40539	✗	Zoho ManageEngine ADSelfService Plus: 6000 - 6113	Volt Typhoon (aka BRONZE SILHOUETTE)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:4.5:4510:*:*:*:*:*:*	-
Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1203: Exploitation for Client Execution	https://www.manageengine.com/products/self-service-password/advisory/CVE-2021-40539.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27860	✗	FatPipe WARP, IPVPN, and MPVPN software	Volt Typhoon (aka BRONZE SILHOUETTE)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fatpipeinc:ipvpn_firmware:5.2.0:r34:*:*:*:*:*:*:*	-
FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1203: Exploitation for Client Execution	https://www.fatpipeinc.com/support/cve-list.php

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3079		Google Chrome: 100.0.4896.60 - 114.0.5735.91	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:google_chrome:-:*:*:*:*:*:*:*	-
Google Chrome Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1190: Exploit Public-Facing Application	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27997		FortiOS and FortiProxy SSL-VPN	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	-
Fortinet heap-based buffer overflow Pre-Auth Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow,T1499: Endpoint Denial of Service, T1499.004:Application or System Exploitation, T1005:Data from Local System	https://www.fortiguard.com/psirt/FG-IR-23-097

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-28299</td><td>✗</td><td rowspan="2">Visual Studio: 2017 version 15.9; 2022 version 17.4, 17.4, 17.2, 17.0; 2019 version 16.11</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:microsoft:visual_studio_2017:*:*:*:*:*:*:*:*
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:*
cpe:2.3:a:microsoft:visual_studio_2019:*:*:*:*:*:*:*:*
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:*:*:*
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:*
cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:-:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Visual Studio Spoofing Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-451</td><td>T1059: Command and Scripting Interpreter, T1005: Data from Local System,T1046: Network Service Scanning</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28299</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20867	✗	VMware Tools: 10.0.0 - 12.2.0	UNC3886
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:tools:*:*:*:*:*:*:*:*	VirtualPita and VirtualPie backdoors
VMware Tools authentication bypass	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing, T1078: Valid Accounts	https://www.vmware.com/security/advisories/VMSA-2023-0013.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0669	✗	GoAnywhere MFT: 4.0.2 - 7.1.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	LockBit Ransomware
Fortra GoAnywhere MFT Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://github.com/rapid7/metasploit-framework/pull/17607

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350		PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:* cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*	LockBit Ransomware
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1478: Install Insecure or Malicious Configuration, T1136: Create Account, T1078: Valid Accounts, T1562: Impair Defenses, T1529: System Shutdown/Reboot	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-12149		Red Hat JBoss Application Server	ChamelGang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redhat:jboss_enterprise_application_platform:-:*:*:*:*:*:*:*	ChamelDoH
Red Hat JBoss Application Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://access.redhat.com/security/cve/CVE-2017-12149

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2021-22986</td><td>  </td><td rowspan="2">F5 BIG-IP and BIG-IQ Centralized Management</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*</td><td rowspan="2">LockBit Ransomware</td></tr>
<tr><td rowspan="3">F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-918</td><td>T1059:Command and Scripting Interpreter</td><td>https://support.f5.com/csp/article/K03009991</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379	✗ ZERO-DAY	Fortinet FortiOS	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	LockBit Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1574:Hijack Execution Flow	https://fortiguard.com/advisory/FG-IR-18-384

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26084	✗ ZERO-DAY	Atlassian Confluence Server and Data Center	Cadet Blizzard (aka DEV-0586, Ruinous Ursa)
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	WhisperGate
Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1190: Exploit Public-Facing Application, T1040: Network Sniffing, T1078: Valid Accounts	https://jira.atlassian.com/browse/CONFSERVER-67940

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-18935	✗ ZERO-DAY	Telerik UI for ASP.NET AJAX	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9248	✗ ZERO-DAY	ASP.NET AJAX and Sitefinity	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:sitefinity_cms:*:*:*:*:*:*:*:* cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Progress Telerik UI for ASP.NET AJAX and Sitefinity Cryptographic Weakness Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-522	T1078:Valid Accounts, T1557:Man-in-the-Middle, T1040:Network Sniffing	http://www.telerik.com/support/kb/aspnet-ajax/details/cryptographic-weakness

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11357	✗	Telerik User Interface (UI) for ASP.NET AJAX	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Telerik UI for ASP.NET AJAX Insecure Direct Object Reference Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1046: Network Service Scanning	http://www.telerik.com/support/kb/aspnet-ajax/upload-%28async%29/details/insecure-direct-object-reference

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11317	✗	Telerik User Interface (UI) for ASP.NET AJAX	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:telerik:ui_for_asp.net_ajax:*:*:*:*:*:*:*:*	-
Telerik UI for ASP.NET AJAX Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-326	T1505.003:Server Software Component: Web Shell, T1059: (Command and Scripting Interpreter	http://www.telerik.com/support/kb/aspnet-ajax/upload-%28async%29/details/unrestricted-file-upload

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-1389	✗	TP-Link Archer AX21 versions before 1.1.4 Build 20230219	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tp-link:archer_ax21_firmware:*:*:*:*:*:*:*:*	Condi Botnet
TP-Link Archer AX-21 Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://www.tp-link.com/us/support/download/archer ax21/v3/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27240	✗	Tenda AX3 Version: 16.03.12.11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tenda:ax3_firmware:16.03.12.11:*:*:*:*:*:*:*	Mirai botnet
Tenda Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-17621	✗	D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-859_firmware:*:*:*:*:*:*:*:*	Mirai botnet
D-Link DIR-859 Remote Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1203: Exploitation for Client Exécution; T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10146; https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10147

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-12725	✗	Zeroshell versions: 3.9.0 - 3.9.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zeroshell:zeroshell:3.9.0:*:*:*:*:*:*:*	Mirai botnet
Zeroshell Remote Command Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1203: Exploitation for Client Execution	https://www.zeroshell.org/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-20500	 ZERO-DAY	D-Link DWL-2600AP 4.2.0.15	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dwl-2600ap_firmware:*:*:*:*:*:*:*:*:*	Mirai botnet
D-Link Remote Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25296	 ZERO-DAY	Nagios XI version xi-5.7.5	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:nagios:nagios_xi:5.7.5:*:*:*:*:*:*:*	Mirai botnet
Nagios OS Command Injection			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-46422		Telesquare SDT-CW3B1 1.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:telesquare:sdtcs3b1_firmware:1.1.0:*:*:*:*:*:*:*	Mirai botnet
Telesquare Router Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-27002		Arris TR3300 v1.0.13	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:commscope:arris_tr3300_firmware:1.0.13:*:*:*:*:*:*:*	Mirai botnet
Arris Remote Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-29303		SolarView Compact version: 6.00	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:contec:sv-cpt-mc310_firmware:6.00:*:*:*:*:*:*:*	Mirai botnet
SolarView Compact Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30023		Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tenda:hg9_firmware:1.0.1:*:*:*:*:*:*:*	Mirai botnet
Tenda Router Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30525	✗ ZERO-DAY	Zyxel Multiple Firewalls	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:usg_flex_100w_firmware:*:*:*:*:*:*:*:*	Mirai botnet
Zyxel Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31499	✗ ZERO-DAY	Nortek Linear eMerge E3-Series devices before 0.32-08f	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:nortekcontrol:emerge_e3_firmware:*:*:*:*:*:*:*:*	Mirai botnet
Nortek Linear eMerge Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-37061	✗ ZERO-DAY ✗	All FLIR AX8 version up to and including 1.46.16	-
NAME	**CISA KEV**	cpe:2.3:o:flir:flir_ax8_firmware:*:*:*:*:*:*:*:*	Mirai botnet
FLIR Unauthenticated OS Command Injection Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059: Command and Scripting Interpreter	https://www.flir.com/products/ax8-automation/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40005	✗ ZERO-DAY ✗	Intelbras WiFiber 120AC inMesh before 1-1-220826	-
NAME	**CISA KEV**	cpe:2.3:o:intelbras:wifiber_120ac_inmesh_firmware:*:*:*:*:*:*:*:*	Mirai botnet
Intelbras Command Injection Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059: Command and Scripting Interpreter	https://seclists.org/fulldisclosure/2022/Dec/13

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-45699	 ZERO-DAY 	APSystems ECU-R version 5203	-
NAME	CISA KEV	cpe:2.3:o:apsystems:ecur_firmware:5203:*:*:*:*:*:*:*	Mirai botnet
APsystems Remote Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://github.com/0xst4n/APSystems-ECU-R-RCE-Timezone

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-25280	 ZERO-DAY 	D-Link DIR820LA1_FW105B03	-
NAME	CISA KEV	cpe:2.3:o:dlink:dir820la1_firmware:105b03:*:*:*:*:*:*:*	Mirai botnet
D-link Command injection vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20in%20pingV4Msg

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44026		Roundcube: 1.3.0 - 1.4.11	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1505: Server Software Component, T1505.003: Web Shell, T1136: Create Account, T1190: Exploit Public-Facing Application, T1565.001: Data Manipulation	https://roundcube.net/news/2021/11/12/security-updates-1.4.12-and-1.3.17-released

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-12641		Roundcube: 1.2.0 - 1.4.3	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-35730		Roundcube: 1.2.0 - 1.4.9	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail CrossSite Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1059.007: JavaScript/JScript, T1557: Man-in-the-Browser, T1189: Drive-by Compromise, T1204: User Execution, T1204.001: Malicious Link	https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Horabot	Horabot was deployed by a threat actor since November 2020. The botnet delivers a banking trojan and spam tool to victim machines. The attacker primarily targets Spanish-speaking users in the Americas, with a focus on Mexico.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Collection of sensitive information	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clop	Clop ransomware recently has been associated with a zero-day vulnerability in the MOVEit Transfer software, allowing unauthorized access to its database. This combination poses an increased threat to organizations, leading to potential data breaches and financial losses.	Phishing emails	CVE-2023-34362
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial loss	Progress MOVEit Transfer
ASSOCIATED ACTOR			**PATCH LINK**
TA505			https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MediaArena	MediaArena is a deceptive software that hijacks browsers, redirects searches, and collects user data for malicious activities, emphasizing the importance of removal and caution.	Malvertising campaigns	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Browser hijacker		Data theft, search manipulation, and system compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NODEBOT	NODEBOT is a Node.js-based variant of AHKBOT, enabling functions like screenshot capture, password theft, and downloading of malicious plugins.	Spear-phishing emails	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Asylum Ambuscade			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AHKBOT	AHKBOT is a malware tool and it is capable of capturing screenshots, stealing passwords, and fetching additional plugins to carry out various malicious activities on compromised systems.	Spear-phishing emails	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Data Theft	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Asylum Ambuscade			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

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
DoubleFinger loader	An advanced campaign utilizes a multi-stage DoubleFinger loader to deploy GreetingGhoul malware, specially crafted for pilfering cryptocurrency credentials.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GreetingGhoul stealer	GreetingGhoul is a stealer designed to steal cryptocurrency-related credentials. It essentially consists of two major components that work together	DoubleFinger loader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VirtualPita backdoor	VIRTUALPITA is a 64-bit passive backdoor that creates a listener on a hardcoded port number on a VMware ESXi server. The backdoor often utilizes VMware service names and ports to masquerade as a legitimate service.	Utilizing a zero-day vulnerability (CVE-2023-20867)	CVE-2023-20867
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	VMware Tools: 10.0.0 - 12.2.0
ASSOCIATED ACTOR			**PATCH LINK**
UNC3886			https://www.vmware.com/security/advisories/VMSA-2023-0013.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LockBit Ransomware	LockBit ransomware has been one of the most widespread and active variants in the world, with affiliates targeting organizations across various critical infrastructure sectors. LockBit has undergone several evolutions, introducing new versions with expanded capabilities and incorporating source code from other ransomware variants.	Phishing	CVE-2023-0669 CVE-2023-27350 CVE-2021-44228 CVE-2021-22986 CVE-2020-1472 CVE-2019-0708 CVE-2018-13379
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage, Information Theft, and Financial Loss	Fortra GoAnywhere MFT,PaperCut MF/NG,Apache Log4j2,F5 BIG-IP and BIG-IQ Centralized Management, Microsoft Netlogon, Microsoft Remote Desktop Services, and Fortinet FortiOS
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/rapid7/metasploitframework/pull/17607 https://www.papercut.com/kb/Main/PO-1216-and-PO-1219 https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/ https://support.f5.com/csp/article/K03009991 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 http://www.fortiguard.com/psirt/FG-IR-20-233

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>WhisperGate</td><td rowspan="6">In the WhisperGate operation in January 2022, Cadet Blizzard is known to deploy destructive malware to select target environments to delete data and render systems inoperable.</td><td>By exploiting web servers</td><td>CVE-2021-26084
CVE-2020-1472
CVE-2021-4034
CVE-2021-34473
CVE-2021-34523
CVE-2021-31207</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Wiper</td><td rowspan="4">Data destruction and Financial Loss</td><td>Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Cadet Blizzard (aka DEV-0586, Ruinous Ursa)</td><td>https://jira.atlassian.com/browse/CONFSERVER-67940
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
https://bugzilla.redhat.com/show_bug.cgi?id=2025869
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207</td></tr>
</table>

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
ChamelDoH	A new Linux malware called 'ChamelDoH' infects Linux devices and establishes communication with the attackers' servers using DNS-over-HTTPS (DoH). The use of DoH allows the malware's communication to be encrypted and disguised as regular HTTPS traffic, making it difficult to detect.	Unknown	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Information Theft and Financial Loss	Red Hat JBoss Application Server and Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINK**
ChamelGang			https://access.redhat.com/security/cve/CVE-2017-12149 https://bugzilla.redhat.com/show_bug.cgi?id=1486220 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

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
SunSeed	SunSeed malware is a dangerous threat delivered via malicious email attachments, enabling attackers to download and execute additional payloads, posing a significant risk to compromised systems and data.	Spear-phishing emails	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		System compromise, data loss, and unauthorized access	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
Asylum Ambuscade			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Stealth Soldier	Stealth Soldier is a Custom backdoor used in targeted espionage attacks in Libya, enabling surveillance with file exfiltration, screen recording, keystroke logging, and browser data theft.	Unkown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Satacom (aka LegionLoader)	Satacom is a notorious malware that uses DNS queries to retrieve encoded URLs, delivering additional malware through malicious ads and links on third-party websites.	Malicious ads or links	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data theft, system instability, unauthorized access, and financial 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
Mystic Stealer	Mystic Stealer is an advanced information stealer malware known for its low detection rate, code manipulation techniques and is stealing sensitive data from browsers, wallets & messaging platforms, posing significant risks to individuals and organizations.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data theft, Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	XMRig is a prevalent form of malware often employed by botnets to mine cryptocurrencies such as Monero. It discreetly exploits infected systems' computing power, enabling unauthorized mining activities.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Diicot (aka Mexals)			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cayosin	Cayosin is a Mirai-based botnet agent utilized by the threat group Diicot for DDoS attacks, primarily targeting routers running OpenWrt. Its deployment showcases Diicot's expanding attack capabilities beyond cryptojacking campaigns.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		System disruption, data loss, and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Diicot (aka Mexals)			-

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
Shampoo	Shampoo malware is a variant of ChromeLoader targeting Google Chrome browsers, installing a malicious extension to collect personal information and manipulate browsing activities. It employs persistence mechanisms and encryption to evade detection, aiming to generate revenue through aggressive advertising.	Malicious VBScript files from malicious websites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Browser extension		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Condi	Condi, a recently discovered malware, utilizes a security vulnerability within TP-Link Archer Wi-Fi routers to ensnare these devices into a botnet specifically designed for launching distributed denial-of-service (DDoS) attacks.	Unknown	CVE-2023-1389
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Data Theft	TP-Link Archer AX21 versions before 1.1.4 Build 20230219
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Tsunami	Tsunami botnet is a powerful DDoS botnet known for its open-source nature and widespread usage by threat actors, causing significant disruptions on the internet.	Exploit kits	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		DDoS attacks, data theft, disruption	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Shellbot	Shellbot is a sophisticated botnet that hijacks Linux servers by exploiting vulnerabilities and installs malicious code to carry out DDoS attacks, spread malware, and engage in cryptocurrency mining	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Disruption	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FadeStealer	FadeStealer features various information theft capabilities, including screenshot capturing, keylogging, microphone wiretapping, and exfiltration from removable media devices and smartphones.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
InfoStealer		Privacy intrusion	-
ASSOCIATED ACTOR			PATCH LINK
Red Eyes			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mirai	Mirai is a notorious botnet malware that targets vulnerable Internet of Things (IoT) devices, turning them into a network of compromised devices used for launching massive DDoS attacks	Exploiting vulnerabilities	CVE-2019-12725 CVE-2019-17621 CVE-2019-20500 CVE-2021-25296 CVE-2021-46422 CVE-2022-27002 CVE-2022-29303 CVE-2022-30023 CVE-2022-30525 CVE-2022-31499 CVE-2022-37061 CVE-2022-40005 CVE-2022-45699 CVE-2023-1389 CVE-2023-25280 CVE-2023-27240
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Internet-of-Things (IoT) disruption	Zeroshell; D-Link DIR-859 Wi-Firouter; D-Link DWL-2600AP; TelesquareSDT-CW3B11.1.0; Arris TR3300v1.0.13; SolarViewCompact; Tenda ONTGPON AC1200Dual bandWiFi HG9v1.0.1; Zyxel MultipleFirewalls; Nortek LineareMerge E3-Series devicesbefore 0.32-08f; All FLIR AX8
ASSOCIATED ACTOR			
Diicot (aka Mexals)			

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

NAME	PATCH LINK
Mirai	https://www.zeroshell.org/download/; https://www.dlink.com/en/security-bulletin; https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113; https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls; https://na.niceforyou.com/solutions/access-control/; https://www.flir.com/products/ax8-automation/; https://seclists.org/fulldisclosure/2022/Dec/13; https://github.com/0xst4n/APSystems-ECU-R-RCE-Timezone; https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware; https://www.fortiguard.com/encyclopedia/ips/52742; https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20in%20pingV4Msg;
TYPE	
Botnet	
Diicot (aka Mexals)	

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CHM malware	CHM malware disguises itself as legitimate files, exploiting users' trust to execute malicious scripts and gain unauthorized access to systems.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
-		Compromised systems, Data breaches	-
ASSOCIATED ACTOR			**PATCH LINK**
Red Eyes			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AblyGo backdoor	AblyGo backdoor is a malicious tool that utilizes the Ably platform to enable real-time command and control communication with infected systems, allowing threat actors to issue commands and receive results stealthily.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Compromised systems, Data breaches	-
ASSOCIATED ACTOR			**PATCH LINK**
Red Eyes			-

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
Backdoor.Graphical	Backdoor.Graphican is a new backdoor used by the Flea APT group, leveraging the Microsoft Graph API and OneDrive for C&C communication in their recent attack campaign targeting foreign ministries in the Americas.	Unknown	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINK**
Flea APT group			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JokerSpy	JokerSpy is an advanced toolkit meticulously crafted to infiltrate macOS machines. It utilizes a combination of Python and Swift programs to gather data and execute arbitrary commands.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Disruption, Information Theft, and Financial Loss	Mac OS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EarlyRat	EarlyRat is similar to MagicRat and have a simple design. It executes given command and sends details to C2 site.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
backdoor		System Disruption, Information Theft, and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Andariel			-

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
PindOS	PindOS is a sleek JavaScript dropper designed to discreetly retrieve and deploy next stage payloads, such as Bumblebee and IcedID.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
backdoor		System Disruption, Information Theft, and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WarZone	Warzone is a remote access tool (RAT) and operates as malware as-a-service. It has no of features to harvest sensitive data and download additional malware.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
backdoor		System Disruption, Information Theft, and Financial Loss	Widnows
ASSOCIATED ACTOR			**PATCH LINK**
Confucius			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VirtualPie backdoor	VIRTUALPIE is a lightweight backdoor written in Python that spawns a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server. It supports arbitrary command line execution, file transfer capabilities, and reverse shell capabilities.	Utilizing a zero-day vulnerability (CVE-2023-20867)	CVE-2023-20867
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	VMware Tools: 10.0.0 - 12.2.0
ASSOCIATED ACTOR			**PATCH LINK**
UNC3886			https://www.vmware.com/security/advisories/VMSA-2023-0013.html

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Volt Typhoon (aka BRONZE SILHOUETTE)	China	Communications, Manufacturing, Utility, Transportation, Construction, Maritime, Government, Information Technology, and Education	United States and the U.S. island territory of Guam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-40539 CVE-2021-27860	-	Zoho ManageEngine, FatPipe WARP, IPVPN, and MPVPN software

TTPs
T1003:OS CredentialDumping; T1003.001:LSASS Memory; T1003.003:NTDS; T1016:System Network Configuration Discovery; T1033:System Owner/User Discovery; T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1059.001:PowerShell; T1059.003:Windows Command Shell; T1069:Permission Groups Discovery; T1069.001:Local Groups; T1069.002:Domain Groups; T1070: Indicator Removal; T1070.001:Clear Windows Event Logs; T1082:System Information Discovery; T1090:Proxy; T1090.002:External Proxy; T1110:Brute Force; T1110.003:Password Spraying; T1190:Exploit Public-Facing Application; T1505:Server Software Component; T1505.003:Web Shell; T1555:Credentials from Password Stores

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Asylum Ambuscade</td><td>Unknown</td><td rowspan="3">Government entities, Financial, Cryptocurrency, Small and Medium Businesses including healthcare, manufacturing, technology, retail, and education</td><td rowspan="3">North America, Europe, Asia, Africa, and South America</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2022-30190</td><td>NODEBOT, AHKBOT, SunSeed</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1583.003:Acquire Infrastructure: Virtual Private Server; T1587.001:Develop Capabilities: Malware; T1189:Drive-by Compromise; T1566.001:Phishing: Spearphishing Attachment; T1059.005:Command and Scripting Interpreter: Visual Basic; T1059.006:Command and Scripting Interpreter: Python; T1059.007:Command and Scripting Interpreter: JavaScript; T1059:Command and Scripting Interpreter; T1204.002:User Execution: Malicious File; T1547.001:Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1027.010:Obfuscated Files or Information: Command Obfuscation; T1555.003:Credentials from Password Stores: Credentials from Web Browsers; T1087.002:Account Discovery: Domain Account; T1010:Application Window Discovery; T1482:Domain Trust Discovery; T1057:Process Discovery; T1518.001:Software Discovery: Security Software Discovery; T1082:System Information Discovery; T1016:System Network Configuration Discovery; T1056.001:Input Capture: Keylogging; T1115:Clipboard Data; T1113:Screen Capture; T1071.001:Application Layer Protocol: Web Protocols; T1041:Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	Defense, Technology, and Telecommunicati on.	The US and APJ regions.
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RAN SOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-20867	VirtualPita and VirtualPie backdoors	VMware Tools: 10.0.0 - 12.2.0
TTPs			
T1560:Archive Collected Data, T1059:Command and Scripting Interpreter, T1203:Exploitation for Client:Execution, T1569:System Services, T1098:Account Manipulation, T1136:Create Account, T1543:Create or Modify System Process, T1548:Abuse Elevation Control Mechanism, T1068:Exploitation for Privilege Escalation, T1055:Process Injection, T1211:Exploitation for Defense:Evasion, T1212:Exploitation for:Credential Access, T1087:Account Discovery, T1105:Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ChamelGang	China	Energy, aviation, and government organizations	Russia, the United States, Japan, Turkey, Taiwan, Vietnam, India, Afghanistan, Lithuania, and Nepal
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RAN SOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-12149 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	ChamelDoH	Red Hat JBoss Application Server and Microsoft Exchange Server
TTPs			
T1105: Ingress Tool Transfer, T1071: Application Layer Protocol, T1189: Drive-by Compromise, T1071.004: DNS, T1059: Command and Scripting Interpreter, T1564.001: Hidden Files and Directories, T1564: Hide Artifacts, T1027: Obfuscated Files or Information, T1082: System Information Discovery, T1005: Data from Local System, T1041: Exfiltration Over C2 Channel, T1572: Protocol Tunneling			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Cadet Blizzard (aka DEV-0586, Ruinous Ursa)	Russia	Government services, Law enforcement, Non-profit/non-governmental organizations, IT service providers/consulting, and Emergency services.	Europe, Central Asia, and Latin America
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-26084 CVE-2020-1472 CVE-2021-4034 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	WhisperGate	Atlassian Confluence Server and Data Center, Microsoft Netlogon, Red Hat Polkit, and Microsoft Exchange Server
TTPs			
T1059:Command and Scripting Interpreter, T1059.001:PowerShell, T1059.005:Visual Basic, T1055:Process Injection, T1055.012:Process Hollowing, T1562:Impair Defenses, T1562.001:Disable or Modify Tools, T1132:Data Encoding, T1132.001:Standard Encoding, T1102:Web Service, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1105:Ingress Tool Transfer, T1561:Disk Wipe, T1561.002:Disk Structure Wipe, T1486:Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 STORM-1359 (Anonymous Sudan)	Unknown	Technology Companies, Government Organisation, Aviation	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1526 - Cloud Service Discovery; T1590 - Gather Victim Network Information; T1498 - Network Denial of Service; T1583 - Acquire Infrastructure; T1190 - Exploit Public-Facing Application			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Diicot (aka Mexals)	Unknown	Technology Companies, Government Organisation, Aviation	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Mirai, Cayosin, XMRig	-
TTPs			
T1027 - Obfuscated Files orInformation; T1110 - Brute Force; T1027 - Obfuscated Files or Information; T1106 - Native API; T1102 - Web Service; T1082 - System Information Discovery; T1496 - Resource Hijacking; T1059 - Command and Scripting Interpreter; T1056 - Input Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Flea (APT15, Playful Taurus, BackdoorDiplomacy, Vixen Panda, Ke3Chang, Playful Dragon, Bronze Palace, and NICKEL)	China	Foreign Affairs, Government, Diplomatic, Finance, Political, Foreign	North, Central, and South America
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2020-1472	Backdoor.Graphical	Microsoft Netlogon
TTPs			
T1550: Use Alternate Authentication Material; T1027: Obfuscated Files or Information; T1204: User Execution; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery; T1550.001: Application Access Token; T1059.001: PowerShell; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1082: System Information Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Red Eyes (APT 37, Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	North Korean	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation.	China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	FadeStealer, CHM malware, AblyGo backdoor	-
TTPs			
T1068:Exploitation for Privilege Escalation; T1204:User Execution; T1140:Deobfuscate/Decode Files or Information; T1059:Command and Scripting Interpreter; T1059.001:PowerShell; T1056:Input Capture ; T1560:Archive Collected Data; T1176:Browser Extensions; T1218:System Binary Proxy Execution; T1547:Boot or Logon Autostart Execution; T1106:Native API; T1566.001:Spearphishing Attachment; T1566:Phishing ; T1036:Masquerading ; T1218.005:Mshta; T1547.001:Registry Run Keys /Startup Folder; T1546.015:Component Object Model Hijacking; T1546:Event Triggered Execution; T1574.002:DLL Side-Loading ; T1574:Hijack Execution Flow ; T1056.001:Keylogging ; T1025:Data from Removable Media; T1027:Obfuscated Files or Information			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
 APT28	Russia	Government Institutions, Military, and Media	Ukraine
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2020-35730, CVE-2021-44026, CVE-2020-12641	-	Roundcube: 1.2.0 - 1.4.11
TTPs			
T1005: Data from Local System, T1021: Remote Services, T1027: Obfuscated Files or Information, T1048: Exfiltration Over Alternative Protocol, T1059: Command and Scripting Interpreter, T1071: Application Layer Protocol, T1078: Valid Accounts, T1114: Email Collection, T1119: Automated Collection, T1133: External Remote Services, T1203: Exploitation for Client Execution, T1204: User Execution, T1213: Data from Information Repositories, T1566: Phishing, T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
 Andariel	North-Korea	Government Agencies, Military Organizations, Financial Services	South Korea
	MOTIVE		
	Information Theft, Espionage and Monetary Gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	EarlyRat	Windows
TTPs			
TA0042: Resource Development, T1587: Develop Capabilities, T1566: Phishing, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1547: Boot or Logon Autostart Execution, T1132: Data Encoding			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.004: Credential API Hooking
	T1113: Screen Capture	
	T1114: Email Collection	T1114.003: Email Forwarding Rule
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1560: Archive Collected Data	
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.002: External Proxy
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.008: /etc/passwd and /etc/shadow
	T1056: Input Capture	T1056.001: Keylogging
		T1056.004: Credential API Hooking
	T1110: Brute Force	T1110.003: Password Spraying
	T1111: Multi-Factor Authentication Interception	
	T1212: Exploitation for Credential Access	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.005: Indicator Removal from Tools
		T1027.010: Command Obfuscation
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.012: Process Hollowing
		T1055.013: Process Doppelgänging
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
		T1070.006: Timestomp
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1548: Abuse Elevation Control Mechanism	
	T1553: Subvert Trust Controls	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.004: Dylib Hijacking
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.001: Local Groups
		T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
	T1124: System Time Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1518: Software Discovery	T1518.001: Security Software Discovery

Tactic	Technique	Sub-technique
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	
	T1204.001: User Execution: Malicious Link	
	T1204.002: User Execution: Malicious File	
	T1569: System Services	
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1531: Account Access Removal	
	T1561: Disk Wipe	T1561.002: Disk Structure Wipe
TA0001: Initial Access	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
TA0008: Lateral Movement	T1021: Remote Services	
	T1072: Software Deployment Tools	
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1098: Account Manipulation	
	T1136: Create Account	
	T1176: Browser Extensions	
	T1505: Server Software Component	T1505.003: Web Shell
	T1525: Implant Internal Image	
	T1543: Create or Modify System Process	
	T1546: Event Triggered Execution	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.004: Dylib Hijacking
TA0004: Privilege Escalation	T1055: Process Injection	T1055.002: Portable Executable Injection
		T1055.012: Process Hollowing
		T1055.013: Process Doppelgänging
	T1068: Exploitation for Privilege Escalation	
	T1543: Create or Modify System Process	
	T1546: Event Triggered Execution	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	
		T1574.002: DLL Side-Loading
TA0043: Reconnaissance	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
	T1584: Compromise Infrastructure	
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.004: Drive-by Target

Top 5 Takeaways

#1 In June, there were **seven zero-day** vulnerabilities. One of these vulnerabilities was exploited by **Clop Ransomware group**

#2 Throughout the month, various ransomware strains resurgence including Clop and LockBit were active.

#3 Attackers are leveraging a specific vulnerability (CVE-2023-27997) in FortiOS and FortiProxy SSL-VPN, enabling remote attackers to execute arbitrary code.

#4 Numerous malware families have been observed targeting victims worldwide. These include **Horabot, WhisperGate, NODEBOT, AHKBOT, SunSeed, and Mirai Botnet.**

#5 CVE-2023-3079 vulnerability is a high-severity zero-day vulnerability that was exploited in attacks

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **44 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 31 active malware,** and **176 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 (JUNE 2023)

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

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

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

Appendix

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

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

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

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

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

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Horabot	IPV4	139[.]177[.]193[.]74 185[.]45[.]195[.]226 216[.]238[.]70[.]224 51[.]38[.]235[.]152 137[.]220[.]53[.]87
Horabot	IPV4	212[.]46[.]38[.]43 191[.]101[.]2[.]101
	Domains	tributaria[.]website facturacionmarzo[.]cloud m9b4s2[.]site wiqp[.]xyz ckws[.]info amarte[.]store
	SHA256	63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064 aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252 fd932d83965d20683ea7f99244dc672e0b4187c9e7588578b626b99d67ac71a6 39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611 474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76 07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da 74a7d13289029d8439e38e0acb4d3b526c63ae863a41218a511182d8f0e6ebef 26e06886d9dde7c9ecdc9b223e5f325d0af27cc9b470179a8e493ac300bd783e 294363039bf93d4c34c8769e581b9c47f8ea210e427fc1feed128bd9bf979a4a
	URLs	hxxps[://]tributaria[.]website/ hxxps[://]tributaria[.]website/ESP/12/151222/UP/UP hxxps[://]tributaria[.]website/A/08/150822/AU/TST/INDEX[.]PHP?LIST hxxps[://]tributaria[.]website/a/09/01092022/au/tst/index[.]php?list hxxps[://]tributaria[.]website/a/08/150822/up/up hxxps[://]tributaria[.]website/esp/12/151222/up/up

Attack Name	TYPE	VALUE
Horabot	URLs	hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/adjuntos_0703[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/logs/index[.]php?CHLG hxxp[://]139[.]177[.]193[.]74/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/tst/index[.]php?list hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/09/01092022/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]htm hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]html hxxp[://]139[.]177[.]193[.]74:443/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2012[.]html hxxp[://]139[.]177[.]193[.]74/A/08/150822/AU/ADJUNTOS_2012[.]HTML hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/gm/index[.]php?CHLG hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/documento-pdf[.]html hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/index[.]php?va hxxps[://]facturacionmarzo[.]cloud/m/archivos[.]pdf[.]html hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html hxxp[://]216[.]238[.]70[.]224/20/t/e/m.zip hxxp[://]ckws[.]info/ hxxps[://]ckws[.]info/a/310122/up/up hxxps[://]ckws[.]info/a/310122/au/au hxxp[://]ckws[.]info/a/07/080722/up/up hxxp[://]ckws[.]info/a/07/080722/au/au hxxps[://]ckws[.]info/A/07/080722/UP/UP hxxps[://]ckws[.]info/a/0511/ hxxp[://]ckws[.]info/a/0511 hxxps[://]ckws[.]info/a/0511/up/up hxxp[://]ckws[.]info/a/0511/au/au hxxp[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/a1/u hxxps[://]m9b4s2[.]site/a1/u/ hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html%20%20Servicio% 20de%20Administraci%C3%B3n%20Tributaria

Attack Name	TYPE	VALUE
Horabot	URLs	hxxp[://]m9b4s2[.]site/2001525248/12457856[.]html hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html=0A= hxxps[://]m9b4s2[.]site/tst/index[.]php?list hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat hxxps[://]m9b4s2[.]site/a1/u/a/index[.]php hxxps[://]m9b4s2[.]site/a1/u/a/index[.]p[.]h[.]p hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat' hxxp[://]m9b4s2[.]site/N/I hxxp[://]m9b4s2[.]site/k/I hxxp[://]m9b4s2[.]site/A/I hxxp[://]m9b4s2[.]site/k hxxp[://]m9b4s2[.]site/a/i hxxp[://]m9b4s2[.]site/K/I hxxp[://]m9b4s2[.]site/A/I' hxxp[://]m9b4s2[.]site/k/I hxxps[://]m9b4s2[.]site/i7_5_7_3_3_2E9Uogmx/i7_5_7_3_3_2E9Uog/i7 _5_7_3_3_2E9Uogal/i7_5_7_3_3_2E9Uog hxxps[://]m9b4s2[.]site/M1S8823HSN34/?1538567474 hxxp[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/09/01092022/au/au hxxp[://]wiqp[.]xyz/09/01092022/up/up hxxps[://]amarte[.]store/ hxxps[://]amarte[.]store/a/08/150822/au/au hxxps[://]amarte[.]store/a/08/150822/up/up hxxp[://]51[.]38[.]235[.]152/20/a/m/m[.]zip hxxp[://]137[.]220[.]53[.]87/20/t/p/m[.]zip hxxp[://]212[.]46[.]38[.]43/m/1 hxxp[://]212[.]46[.]38[.]43/e/1 hxxp[://]191[.]101[.]2[.]101/m/1 hxxps[://]tributaria[.]website/a/W_/X\\W_YY/au/au hxxps[://]tributaria[.]website/a/08/150822/au/au hxxp[://]tributaria[.]website:443/ hxxps[://]tributaria[.]website/A/08/150822/AU/AU hxxps[://]tributaria[.]website/esp/12/151222/au/au hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0703[.]html
MediaArena	SHA256	5e1cec9e9011fc96638620a2ca8e08eeaeaea8a28c47fe619082abcc6794aebc e248b01e3ccde76b4d8e8077d4fcb4d0b70e5200bf4e738b45a0bd28fbc2cae6 cd2b9cf8489cca6b357bc2706a68f5a12aeb696380ce7371803d68f08e337630

Attack Name	TYPE	VALUE
MediaArena	SHA256	e9fad9727b8a66e6b593d8b416f1c60b692ffc91b72e14bb30c40a1ce9b6a260 6d37baeb841bcf6c4935a54f29df049d405df48345014cc12852b814d279d86e
	SHA1	33c02d70abb2f1f12a79cfd780d875a94e7fe8774041a7410598c46d7657ceb94b0af4ebbc7a9c0a
	Hostname	Goto[.]searchpoweronline[.]com
Satacom	MD5	0ac34b67e634e49b0f75cf2be388f2441aa7ad7efb1b48a28c6ccf7b496c9cfd 199017082159b23decdf63b22e07a7a1 a7f17ed79777f28bf9c9cebaa01c8d70
	Domains	dns-beast[.]com don-dns[.]com die-dns[.]com hit-mee[.]com noname-domain[.]com don-die[.]com old-big[.]com tchk-1[.]com you-rabbit[.]com web-lox[.]com ht-specialize[.]xyz ht-input[.]cfd ht-queen[.]cfd ht-dilemma[.]xyz ht-input[.]cfd io-strength[.]cfd fbs-university[.]xyz io-previous[.]xyz io-band[.]cfd io-strength[.]cfd io-band[.]cfd can-nothing[.]cfd scope-chat[.]xyz stroke-chat[.]click icl-surprise[.]xyz new-high[.]click shrimp-clock[.]click oo-knowledge[.]xyz oo-station[.]xyz oo-blue[.]click oo-strategy[.]xyz oo-clearly[.]click economy-h[.]xyz

Attack Name	TYPE	VALUE
Satacom	Domains	church-h[.]clickclose-h[.]xyz thousand-h[.]click risk-h[.]xyz current-h[.]click fire-h[.]xyz future-h[.]click moment-are[.]xyz himself-are[.]click air-are[.]xyz teacher-are[.]click force-are[.]xyz enough-are[.]xyz education-are[.]click across-are[.]xyz although-are[.]click punishment-chat[.]click rjjy-easily[.]xyz guy-seventh[.]cfd back-may[.]com post-make[.]com medical-h[.]click hospital-h[.]xyz filesend[.]live soft-kind[.]com ee-softs[.]com big-loads[.]com el-softs[.]com
NODEBOT	SHA1	C98061592DE61E34DA280AB179465580947890DE
Sunseed	IPV4	146[.]70[.]79[.]119
AHKBOT	SHA1	57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B 64F5AC9F0C6C12F2A48A1CB941847B0662734FBF 557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF F85B82805C6204F34DB0858E2F04DA9F620A0277 5492061DE582E71B2A5DA046536D4150F6F497F1 C554100C15ED3617EBFAAB00C983CED5FEC5DB11 AD8143DE4FC609608D8925478FD8EA3CD9A37C5D F2948C27F044FC6FB4849332657801F78C0F7D5E 7AA23E871E796F89C465537E6ECE962412CDA636 384961E19624437EB4EB22B1BF45953D7147FB8F 7FDB9A73B3F13DBD94D392132D896A5328DACA59 3E38D54CC55A48A3377A7E6A0800B09F2E281978 7F8742778FC848A6FBCFFEC9011B477402544171 29604997030752919EA42B6D6CEE8D3AE28F527E 7A78AF75841C2A8D8A5929C214F08EB92739E9CB

Attack Name	TYPE	VALUE
AHKBOT	SHA1	441369397D0F8DB755282739A05CB4CF52113C40 117ECFA95BE19D5CF135A27AED786C98EC8CE50B D24A9C8A57C08D668F7D4A5B96FB7B5BA89D74C3 95EDC096000C5B8DA7C8F93867F736928EA32575 62FA77DAEF21772D599F2DC17DBBA0906B51F2D9 A9E3ACFE029E3A80372C0BB6B7C500531D09EDBE EE1CFEDD75CBA9028904C759740725E855AA46B5
	IPV4	5.39.222[.]150 5.44.42[.]27 5.230.68[.]137 5.230.71[.]166 5.230.72[.]38 5.230.72[.]148 5.230.73[.]57 5.230.73[.]63 5.230.73[.]241 5.230.73[.]247 5.230.73[.]248 5.230.73[.]250 5.252.118[.]132 5.252.118[.]204 5.255.88[.]222 23.106.123[.]119 31.192.105[.]28 45.76.211[.]131 45.77.185[.]151 45.132.1[.]238 45.147.229[.]20 46.17.98[.]190 46.151.24[.]197 46.151.24[.]226 46.151.25[.]15 46.151.25[.]49 46.151.28[.]18 51.83.182[.]153 51.83.189[.]185 62.84.99[.]195 62.204.41[.]171 77.83.197[.]138 79.137.196[.]121 79.137.197[.]187 80.66.88[.]155 84.32.188[.]29 84.32.188[.]96 85.192.49[.]106 85.192.63[.]13

Attack Name	TYPE	VALUE
AHKBOT	IPV4	85.192.63[.]126 85.239.60[.]40 88.210.10[.]62 89.41.182[.]94 89.107.10[.]7 89.208.105[.]255 91.245.253[.]112 94.103.83[.]46 94.140.114[.]133 94.140.114[.]230 94.140.115[.]44 94.232.41[.]96 94.232.41[.]108 94.232.43[.]214 98.142.251[.]26 98.142.251[.]226 104.234.118[.]163 104.248.149[.]122 109.107.173[.]72 116.203.252[.]67 128.199.82[.]141 139.162.116[.]148 141.105.64[.]121 146.0.77[.]15 146.70.79[.]117 157.254.194[.]225 157.254.194[.]238 172.64.80[.]1 172.86.75[.]49 172.104.94[.]104 172.105.235[.]94 172.105.253[.]139 176.124.214[.]229 176.124.217[.]20 185.70.184[.]44 185.82.126[.]133 185.123.53[.]49 185.150.117[.]122 185.163.45[.]221 193.109.69[.]52 193.142.59[.]152 193.142.59[.]169 194.180.174[.]51 195.2.81[.]70 195.133.196[.]230 212.113.106[.]27 212.113.116[.]147

Attack Name	TYPE	VALUE
Stealth Soldier	IPV4	185.125.230[.]216 185.125.230[.]116 94.156.33[.]228 94.156.33[.]229 185.125.230[.]224 185.125.230[.]220
	Domains	filestoragehub[.]live customjvupdate[.]live filecloud[.]store webmailogemail[.]com loglivemail[.]com 2096[.]website
Stealth Soldier	SHA256	2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb 05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f 8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946 df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4 e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974 c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6 cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885 b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723 7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd
DoubleFinger loader	MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ea D9130cb36f23edf90848ffd73bd4e0e0

Attack Name	TYPE	VALUE
DoubleFinger loader	Domain	cryptohedgefund[.]us
GreetingGhoul stealer	MD5	642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e
VirtualPita backdoor	MD5	8e80b40b1298f022c7f3a96599806c43 61ab3f6401d60ec36cd3ac980a8deb75 2c28ec2d541f555b2838099ca849f965 744e2a4c1da48869776827d461c2b2ec 93d50025b81d3dbcb2e25d15cae03428 fe34b7c071d96dac498b72a4a07cb246
	SHA1	e9cbac1f64587ce1dc5b92cde9637affb3b58577 93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84 e35733db8061b57b8fcdb83ab51a90d0a8ba618c a3cc666e0764e856e65275bd4f32a56d76e51420 abff003edf67e77667f56bbcfc391e2175cb0f8a 0962e10dc34256c6b31509a5ced498f8f6a3d6b6
	FullPath	/bin/rdt /usr/lib/vmware/weasel/consoleui/rhttpproxy-io /usr/libexec/setconf/ksmd /usr/bin/ksmd
	SHA256	c2ef08af063f6d416233a4b2b2e991c177fc72d70a76c24bca9 080521d41040f 4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b2 64ae0d1e15e70d 505eb3b90cd107cf7e2c20189889afdff813b2fbb98bbdeab65 cde520893b168 4a6f559426493abc0d056665f23457e2779abd3482434623e1 f61f4cd5b41843 13f11c81331bdce711139f985e6c525915a72dc5443fbbfe99c 8ec1dd7ad2209 5731d988781c9a1d2941f7333615f6292fb359f6d48498f32c2 9878b5bedf00f
VirtualPie backdoor	MD5	61ab3f6401d60ec36cd3ac980a8deb75
	SHA1	93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84
	SHA256	4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b2 64ae0d1e15e70d
LockBit Ransomware	SHA256	149d691411f10f8ec7af43f0237ccfab5b65a9ae73718acf1e0c c0dbdea36ebd

Attack Name	TYPE	VALUE
LockBit Ransomware	SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae40876 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db cb83eb6f5fd42f59b1c1a34826df48e5a5882c45e4a7f34c80c0830c26cb30dd 4d4bc9d78db93c25548a679de06e267363a31a400e2e37caf9d1fce91b65fe8d b9872ad6ec82d3f2f9a8c6af7e5838f91712e52ece265cd04f4452378bd5bcfd a8939a43feb8cc258507ffd0be564d56a2874c220729e00da8ad204c3b4012c5 fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 fef1f9664fde9b23754c691b15a05fdc35a51a0ceb8a18fb9a5a0166e6377c69 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309 E47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d

Attack Name	TYPE	VALUE
LockBit Ransomware	SHA256	9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194 a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a a9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390 b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122 f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9 1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716 ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9 6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7 cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662

Attack Name	TYPE	VALUE
WhisperGate	MD5	3a2a2de20daa74d8f6921230416ed4e6
ChamelDoH	SHA256	34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7 4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0 6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe 70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007 92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9 e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72
Mystic Stealer	SHA256	7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc 5c0987d0ee43f2d149a38fc7320d9ffd02542b2b71ac6b5ea5975f907f9b9bf8 8592e7e7b89cac6bf4fd675f10cc9ba319abd4aa6eaa00fb0b1c42fb645d3410 45d29afc212f2d0be4e198759c3c152bb8d0730ba20d46764a08503eab0b454f ce56e45ad63065bf16bf736dccb452c48327803b434e20d58a6fed04f1ce2da9 fc4aa58229b6b2b948325f6630fe640c2527345ecb0e675592885a5fa6d26f03
XMRig	MD5	0014403121eeaebaeede796e4b6e5dbe 125951260a0cb473ce9b7acc406e83e1
Condi	SHA256	091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f 291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144 449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190 4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a

Attack Name	TYPE	VALUE
Condi	SHA256	509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084 593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315 5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612 cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772 ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15 f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf
Tsunami	MD5	822b6f619e642cc76881ae90fb1f8e8e
	C2	ircx.us[.]to:53 ircxx.us[.]to:53
Mirai	SHA256	b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3 366ddbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6 413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2 2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599 4cb8c90d1e1b2d725c2c1366700f11584f5697c9ef50d79e00f7dd2008e989a0 461f59a84ccb4805c4bbd37093df6e8791cdf1151b2746c46678dfe9f89ac79d aed078d3e65b5ff4dd4067ae30da5f3a96c87ec23ec5be44fc85b543c179b777 0d404a27c2f511ea7f4adb8aa150f787b2b1ff36c1b67923d6d1c90179033915 eca42235a41dbd60615d91d564c91933b9903af2ef3f8356ec4cfff2880a2f19 3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d aaf446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b

Attack Name	TYPE	VALUE
Shellbot	URLs	ddoser[.]org/logo ddoser[.]org/siwen/bot
	MD5	c5142b41947f5d1853785020d9350de4 2cd8157ba0171ca5d8b50499f4440d96
Backdoor.Graphical	SHA256	4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5 a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8 02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5 617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd 858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253 fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476 177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf 8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286 865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48 d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30
FadeStealer	MD5	f44bf949abead4af0966436168610bcc
CHM malware	MD5	1352abf9de97a0faf8645547211c3be7
AblyGo backdoor	MD5	3277e0232ed6715f2bae526686232e063c475d80f5f6272234da821cc418a6f7
	URL	hxxp://172.93.181[.]249/file/
DoubleFinger loader	Domain	cryptohedgefund[.]us
	MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ead9130cb36f23edf90848ffd73bd4e0e0
GreetingGhoul stealer	MD5	642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e

Attack Name	TYPE	VALUE
JockerSpy Backdoor	Domain	app.influmarket[.]org hxxps://www.git-hub.me/view.php
	SHA1	937a9811b3e5482eb8f96832454723d59229f945 c7d6ede0f6ac9f060ae53bb1db40a4fbe96f9ceb bd8626420ecfd1ab5f4576d83be35edecd8fa70e 370a0bb4177eeebb2a75651a8addb0477b7d610b 1ed2c5ee95ab77f8e1c1f5e2bd246589526c6362 76b790eb3bed4a625250b961a5dda86ca5cd3a11
	SHA256	d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6e f8c5c9bd3487d8, 8ca86f78f0c73a46f31be366538423ea0ec58089f3880e04154 3d08ce11fa626, aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b 8737558a08dc1
PindOS dropper	URL	hxxps://qaswrahc.com/wp-content/out/mn[.]php hxxp://tusaceitesesenciales.com/mn[.]php hxxp://carwashdenham.com/mn[.]php hxxps://intellectproactive.com/dist/out/mn[.]php hxxps://masar-alulaedu.com/wp- content/woocommerce/out/berr[.]php hxxps://egyfruitcorner.com/wp-content/tareq/out/berr[.]php hxxps://tech21africa.com/wp- content/uploads/out/berr[.]php hxxps://www.posao-austrija.at/images/out/lim[.]php hxxps://logisticavirtual.org/wp-content/out/lim[.]php hxxps://adecoco.us/wp-content/out/lim[.]php hxxps://acsdxb.net/wp-content/out/lim[.]php
	SHA256	bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22 efd1f8974d1ca91, 07d2cb0dc0cd353fb210b065733743078e79c4a27c42872cd5 16a6b1fb1f00d1, 00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e 50ad80b2212b0, 15da5b0a65dd8135273124da0c6e52e017e3b54642f87571e 82d2314aae97eec, 180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca 587b5cc3f5e7a, 24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff6 5e4065cb18359, 76c9780256e195901e1c09cb8a37fb5967f9f5b36564e380e7c f2558652f875b,

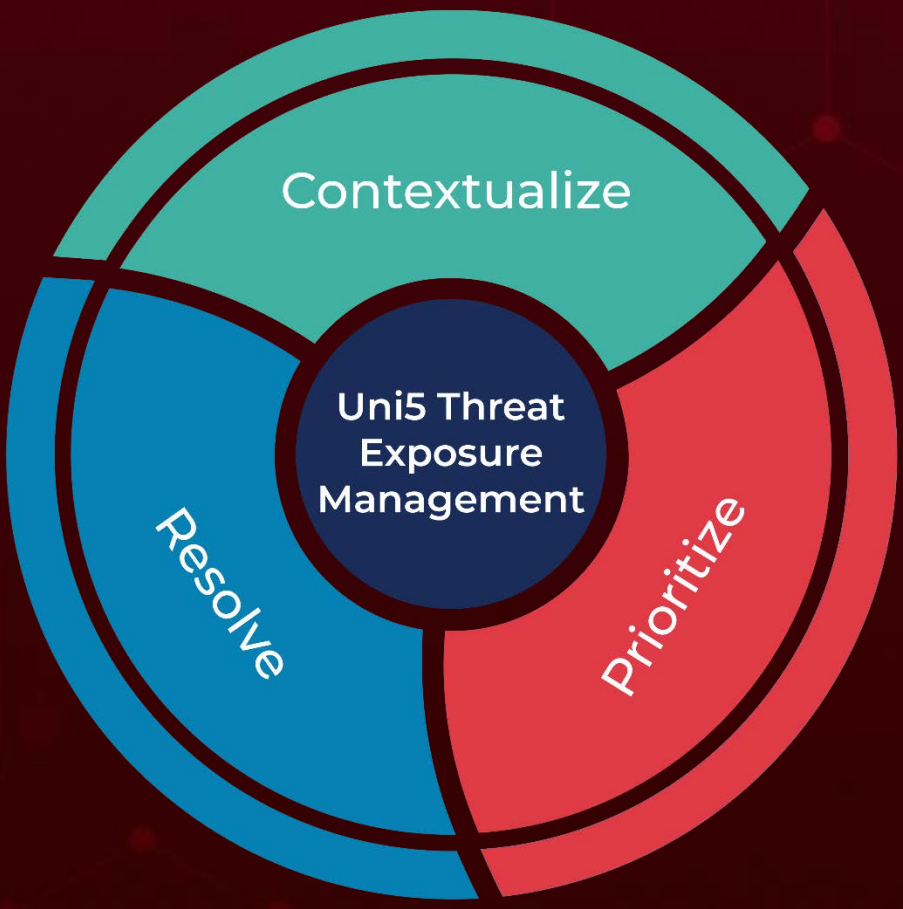
Attack Name	TYPE	VALUE
PindOS dropper	SHA256	28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523, ac261ac26221505798c65c61a207f3951cc7dce2e1014409d8a765d85bfd91d4, 92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b, c84c84387f0b9e7bc575a008f36919448b4e6645e1f5d054e20b59be726ee814, 7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6, 8f40ff286419eb4b0c4d15710dc552afb2c2a227a180f4b4f520d09b05724151, 9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226, 4f0c9c6fc1287ef16f4683db90dd677054a1f834594494d61d765fa3f2e1352c, cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c, 361b0157ef63d362fdd4399288f5f6a0e1536633dfb49c808a3590718c4d8f10, e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c, 8ae3be9f09f5fc64ec898a4d6467b2f6e50eaaa26fc460a4f1a9b9566e97a9a7
EarlyRat Backdoor	IPv4	226.132.219[.]125 74.124.228[.]148
WarZone backdoor	URL	hxxps://lo3kcg.bl.files.1drv[.]com/y4mtafF_tQM7vAFHxOASpTWOq0M5qmXCnd8FhdFvHvKOxYaA1h-ocJsybIp-r0iMVcK8UH6WP-fFspS6l-aP6uTlpsy11crZ_p_HfMxTI4yymzBqVkLX-v4nQLrn2Ty0-ilIRzICAbtwbooanM9U97qPmTgUNxhC9ab_4VfNvcmiWFeami9lwl35D8Eb7UiF7TCJTo_0XyAatlemjaXw9zAlw/REQUEST.zip?download&psid=1 -- redirects to -- hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D!152&authkey=AErksvWpjzpD_Ag hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21151&authkey=AGCMruhQJESxca4 hxxps://onedrive.live[.]com/download?cid=D09BFD4EBDA21A3D&resid=D09BFD4EBDA21A3D%21148&authkey=ADY1aqOba7HnNZs&em=2

Attack Name	TYPE	VALUE
WarZone backdoor	URL	hxxps://onedrive.live[.]com/download?cid=4A89E2A4EA0448C0&resid=4A89E2A4EA0448C0%21130&authkey=ABwx94zEGC3SmxA 134[.]19.179.147:38046/dominion46.ddns[.]net 134[.]19.179.147:29185/dominion46.ddns[.]net
	SHA256	8674817912be90a09c5a0840cd2dff2606027fe8843eb868929fc33935f5511e, 3783acc6600b0555dec5ee8d3cc4d59e07b5078dd33082c5da279a240e7c0e79, 18C876A24913EE8FC89A146EC6A6350CDC4F081AC93C0477FF8FC054CC507B75, 31960A45B069D62E951729E519E14DE9D7AF29CB4BB4FB8FEAD627174A07B425, 02212f763b2d19e96651613d88338c933ddfd18be4cb7e721b2fb57f55887d64, 5A11C5641C476891AA30E7ECFA57C2639F6827D8640061F73E9AFEC0ADBBD7D2, 30951DB8BFC21640645AA9144CFEAA294BB7C6980EF236D28552B6F4F3F92A96, 37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E, F9130B4FC7052138A0E4DBAAEC385EF5FAE57522B5D61CB887B0327965CCC02A, 0E799B2F64CD9D10A4DFED1109394AC7B4CCC317A3C17A95D4B3565943213257, 455ED920D79F9270E8E236F14B13ED4E8DB8DD493D4DABB05756C867547D8BC7, 9C14375FBBCE08BCF3DC7F2F1100316B2FB745FA2C510F5503E07DB57499BFC8
WarZone backdoor	SHA256	**B452A2BA481E881D10A9741A452A3F092DFB87BA42D530484D7C3B475E04DA11, AB0212F8790678E3F76ED90FBA5A455AC23FBB935CF99CABC2515A1D7277676F, 4A834B03E7FAFFEF929A2932D8E5A1839190DF4D5282CEF35DA4019FE84B19A5, 11408368F4C25509C24017B9B68B19CE5278681F6F12CE7DB992D3C6124B0A23**

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

July 04, 2023 . 09:30 AM

More at www.hivepro.com