Date of Publication
November 2, 2023

Hive Pro®

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Actors, and Attacks

OCTOBER 2023

Table Of Contents

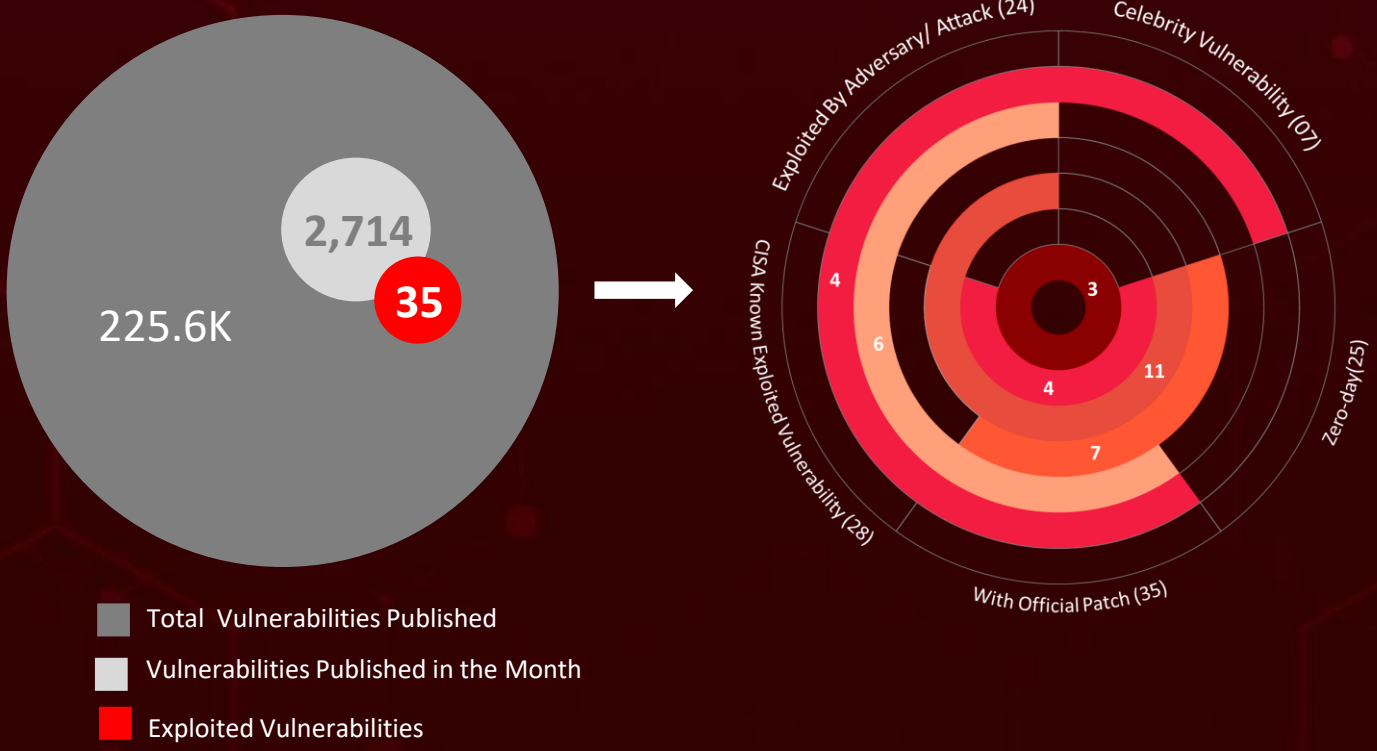
Summary

In **October**, the discovery of **twenty-five zero-day** vulnerabilities drew significant attention from the cybersecurity community. One of these vulnerabilities was exploited by the **Storm-0062 group**, leading to a sense of urgency among security teams to patch their systems.

October saw a rise in ransomware attacks, with various strains such as **Ransom Knight**, **Clop** , **LostTrust**, **Phobos**, **BlackCat** and **AvosLocker** 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.

Furthermore, nine adversaries were active and involved in various campaigns. **Grayling APT's** exploited a four year old vulnerability (**CVE-2019-0803**) in Microsoft Win32k, targeting a government entity in the Asia-Pacific region.

Lastly, the **CVE-2023-44487**, a critical zero-day is causing widespread impact as attackers exploit a flaw within the HTTP/2 protocol, resulting in a denial of service (DoS) attack.



Insights

ToddyCat

Chinese Group targets specific countries in Asia, focusing Telecom and Government industries

Balada Injector

A large scale malware campaign exploited over 17,000 WordPress websites

AvosLocker

Ransomware targets critical infrastructure organizations, primarily in the US

ShellBot

Malware updated its evasion detection technique to use Hexadecimal IP Addresses

Government, Technology, Financial, Manufacturing, and **Defence** were the most targeted sectors

103

vulnerabilities were patched during October Microsoft Patch Tuesday, in addition to 2 non Microsoft flaws

CVE-2023-20198

Critical Zero-Day Vulnerability Actively Exploited in Cisco IOS XE Software

DarkGate

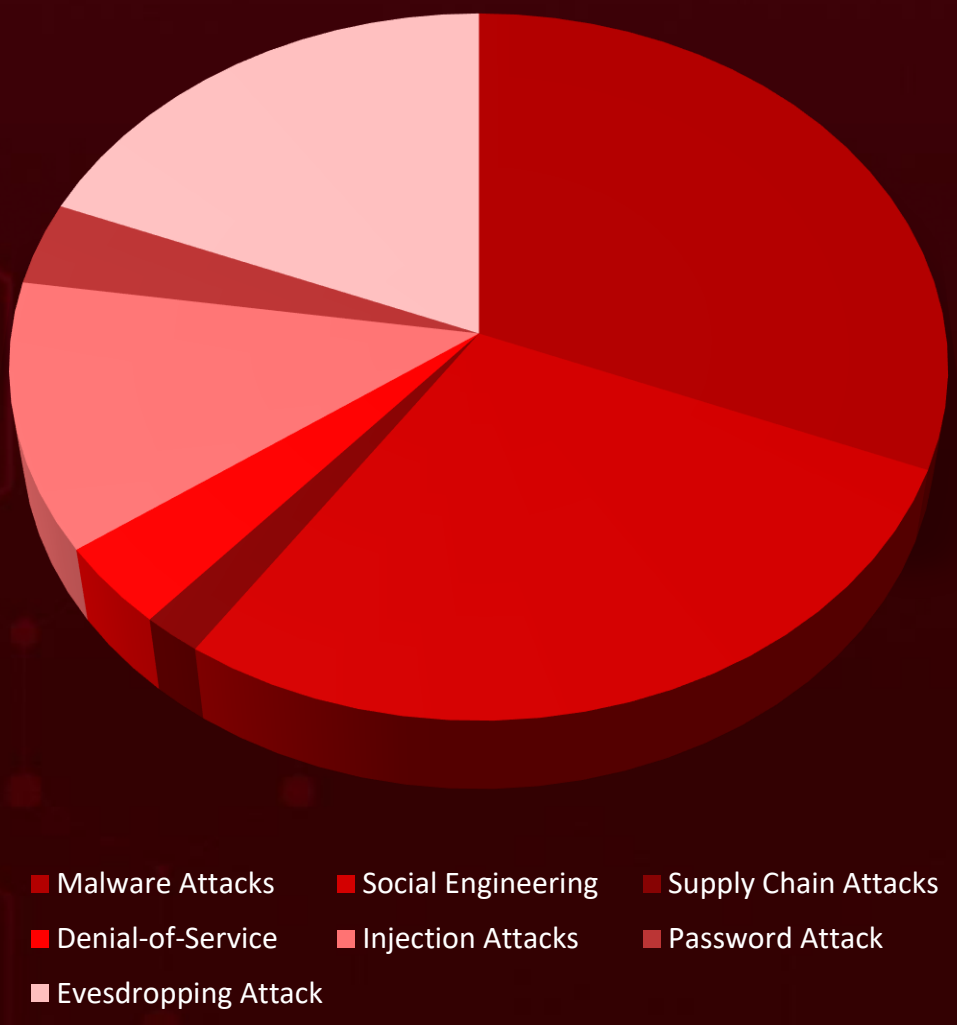
Malware campaign spreading across multiple continents

United Arab Emirates, United States, Turkey, Syria, and **South Korea,** were the most targeted countries

Storm-0978

Utilized a new PEAPOD backdoor, to target attendees of the Women Political Leaders Summit in Brussels

Threat Landscape



Celebrity Vulnerabilities

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

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

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-1675		Windows: 7 - 10 S, Windows Server: 2008 - 2019 2004	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675

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

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228		Apache Log4j2	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:*:*	AvosLocker ransomware
Apache Log4j2 Remote Code Execution Vulnerability (Log4j)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917 CWE-502 CWE-400 CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34527		Windows: 7 - 10 S, Windows Server: 2008 - 2019 2004	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	ZERO-DAY	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

CVE ID	CISA KEV	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	✓	Microsoft Exchange Server: 2013 Cumulative Update 1 15.00.0712.024 - 2019 RTM 15.02.0221.012	-
		AFFECTED CPE	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**ZERO-DAY**	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_21:*:*:*:*:*:*:*	AvosLocker ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability (ProxyLogon)	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-918	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-42114	Exim Information Disclosure Vulnerability	Exim	✓	✗	✓
CVE-2023-42115	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42116	Exim Buffer Overflow Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42117	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42118	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42119	Exim Information Disclosure Vulnerability	Exim	✓	✗	✓
CVE-2023-22515	Atlassian Confluence Privilege Escalation Vulnerability	Atlassian Confluence Data Center and Server	✓	✓	✓
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✓	✓	✓
CVE-2017-17215	Huawei HG532 Remote Code Execution Vulnerability	Huawei HG532	✓	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2017-11882	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✓	✓
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability	Microsoft IIS, Apache Tomcat, Netty, Jetty	✓	✓	✓
CVE-2023-41763	Microsoft Skype for Business Privilege Escalation Vulnerability	Skype for Business Server	✓	✓	✓
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability	Microsoft WordPad	✓	✓	✓
CVE-2019-0803	Microsoft Win32k Privilege Escalation Vulnerability	Windows	✓	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✓	✓	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-40539	Zoho ADSelfService Plus Remote code execution Vulnerability	Zoho ManageEngine ADSelfService Plus	✓	✓	✓
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2018-19320	GIGABYTE Multiple Products Unspecified Vulnerability	GIGABYTE Multiple Products	✗	✓	✓
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE	✓	✓	✓
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	WinRAR	✓	✓	✓
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	JetBrains TeamCity	✗	✓	✓
CVE-2021-34527	Microsoft Windows Print Spooler Remote Code Execution Vulnerability	Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-1675	Microsoft Windows Print Spooler Remote Code Execution Vulnerability	Windows	✗	✓	✓
CVE-2017-0213	Microsoft Windows Privilege Escalation Vulnerability	Windows	✗	✓	✓
CVE-2021-40449	Microsoft Windows Win32k Privilege Escalation Vulnerability	Windows	✓	✓	✓
CVE-2021-26411	Microsoft Internet Explorer Memory Corruption Vulnerability	Microsoft Internet Explorer	✓	✓	✓
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco IOS XE	✓	✓	✓
CVE-2023-34051	VMware Aria Operations for Logs Authentication Bypass Vulnerability	VMware Aria Operations for Logs	✗	✗	✓
CVE-2023-5631	Roundcube Cross Site Scripting Vulnerability	Roundcube	✓	✓	✓
CVE-2023-34048	VMware vCenter Out-of-Bounds Write Vulnerability	VMware vCenter	✗	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
EvilProxy	Phishing-as-a-service kit	-	-	-	Phishing
BunnyLoader	Loader	-	-	-	-
DinodasRAT	RAT	-	-	-	Phishing
Qakbot	Trojan	-	-	-	Phishing
Ransom Knight	Ransomware				Phishing
Remcos	Backdoor				Phishing
Clop	Ransomware	CVE-2023-34362	Progress MOVEit Transfer	✓	Phishing
LostTrust	Ransomware	-	Windows	-	Phishing
SFile	Ransomware	-	Windows	-	Phishing
Mindware	Ransomware	-	Windows	-	Social engineering
MetaEncryptor	Ransomware	-	Windows	-	Phishing
HyperBro	RAT	-	Windows	-	Social engineering
Cobalt Strike	-	-	Windows	-	Phishing
ChargeWeapon	Backdoor	-	-	-	Social engineering
Mirai	Botnet	CVE-2017-17215	Linux	✓	-
HailBot		CVE-2017-11882	IoT platforms		Exploiting vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
KiraiBot	Botnet	-	IoT platforms	-	-
catDDoS	Botnet	-	IoT platforms	-	-
Lu0Bot	Botnet	-	Windows	-	Phishing emails
CurKeep	Backdoor	CVE-2022-23748	-	✓	Phishing Emails
CurLu	Downloader	CVE-2022-23748	-	✓	Phishing Emails
CurLog	Loader	-	-	-	Social engineering
Balada	Injector	CVE-2023-3169	-	✓	Phishing emails and exploit vulnerabilities
ShellBot	Botnet	-	Linux SSH servers	-	Phishing emails
DarkGate	Loader	-	-	-	Phishing emails
SeroXen RAT	RAT	-	-	-	Social engineering
PEAPOD	Backdoor	-	-	-	Spear-phishing emails and malvertising
XorDDoS	Trojan	-	Linux	-	Exploiting vulnerabilities
Volgmer	Backdoor	-	-	-	Spear phishing and supply chain attacks

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
AvosLocker	Ransomware	CVE-2021-31206, CVE-2021-31207, CVE-2021-34473, CVE-2021-34523, CVE-2021-26855, CVE-2021-40539, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-26134, CVE-2018-19320	Windows, Linux, and VMware ESXi	✓	Compromised RDP/VPN credentials or by exploiting vulnerabilities
Scout	Downloader	-	-	-	Spear phishing and supply chain attacks
BbyStealer	Information Stealer	-	Windows	-	Phishing
SmokeLoader	Loader	CVE-2023-38831	RARLAB WinRAR	✓	Phishing
NanoCore	RAT	CVE-2023-38831	RARLAB WinRAR	✓	Phishing
Crimson	RAT	CVE-2023-38831	RARLAB WinRAR	✓	Phishing
AgentTesla	RAT	CVE-2023-38831	RARLAB WinRAR	✓	Phishing
HazyLoad	Loader	CVE-2023-42793	TeamCity servers	✓	Exploiting Vulnerability
Rhadamanthys	Information Stealer	CVE-2023-38831	RARLAB WinRAR	✓	Phishing
xRAT	RAT	-	-	-	Spear-phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BabyShark	Backdoor	-	-	-	Spear-phishing
RevClient	RAT	-	-	-	Spear-phishing
TinyNuke	Banking Trojan	-	-	-	Spear-phishing
ForestTiger	Backdoor	CVE-2023-42793	TeamCity servers	✓	Exploiting Vulnerabilities
FeedLoad	Loader	CVE-2023-42793	TeamCity servers	✓	DLL search order hijacking
Phobos	Ransomware	CVE-2021-34527 CVE-2021-1675 CVE-2017-0213	Microsoft Windows Print Spooler	✓	Phishing emails
MATA	Backdoor	CVE-2021-40449 CVE-2021-26411	Microsoft Internet Explorer & Windows	✓	Spear-phishing
PowerExchange	Backdoor	-	-	-	Phishing emails
Clipog	Information Stealer	-	-	-	Phishing emails
Munchkin	Dropper	-	-	-	Unknown
BlackCat	Ransomware	-	-	-	Unknown
SIGNBT	Loader	-	-	-	Unknown
LPEClient	Downloder	-	-	-	Phishing
BiBi-Linux	Wiper	-	-	-	Phishing
GHOSTPULSE	Loader	-	-	-	Unknown

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Grayling APT	Information theft and espionage	Unknown	CVE-2019-0803	-	-
ToddyCat	Information theft and espionage	China	CVE-2022-23748	CurKeep, CurLu, CurLog	Windows
Storm-0978	Information theft and espionage, Financial gain	Russia	-	PEAPOD (aka ROMCOM 4.0)	-
OilRig	Information theft and espionage	Iran	-	PowerExchange, Clipog	-
Lazarus Group	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2023-42793	Volgmer, Scout, ForestTige, FeedLoad, RollSling, and HazyLoad	TeamCity
Kimsuky	Information theft and espionage	North Korea	-	xRAT, BabyShark, RevClient, TinyNuke	-
Andariel	Information theft and espionage	North Korea	CVE-2023-42793	Volgmer, Scout, ForestTiger, FeedLoad, RollSling, and HazyLoad	TeamCity

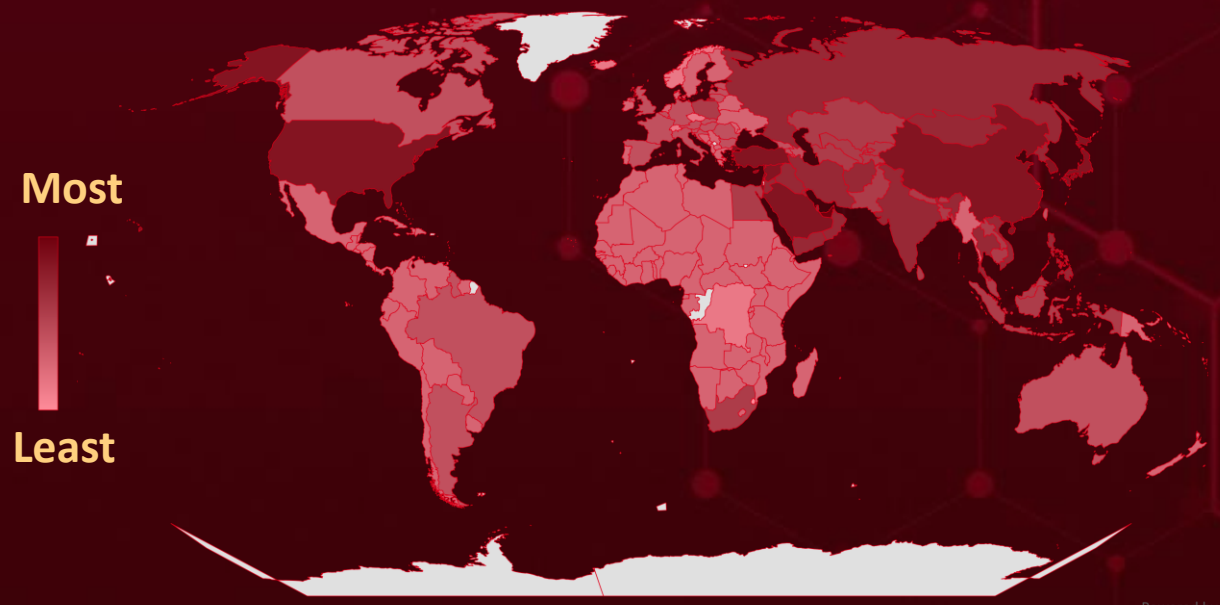
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
YoroTrooper	Information theft and espionage	Unknown	-	-	-
Winter Vivern	Information theft and espionage	Unknown	CVE-2023-5631	-	Roundcube

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Exim	Exim	Exim: 4.96 or earlier versions
ATLASSIAN	Data Center and Server	Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1
Progress MOVEit	Managed file transfer	Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1)
HUAWEI	Router	Huawei HG532: All versions
Microsoft	Applications	Microsoft Office: 2007 - 2016
		Skype for Business Server: before 7.0.246.530
	Operating System	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2
	Browser	Microsoft Internet Explorer: 9 - 11
ZOHO	ManageEngine	Zoho ManageEngine ADSelfService Plus: 6000 - 6113

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
GIGABYTE	Applications	GIGABYTE APP Center: 1.05.21 AORUS GRAPHICS ENGINE: 1.0 - 1.33 XTREME GAMING ENGINE: 1.22 - 1.25 OC GURU: 2.08
CISCO	Security Appliances	Cisco IOS XE- All versions
	Application	WinRAR: 3.20 - 6.23 beta 1
CITRIX	Applications	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300
TC	Server	TeamCity: 2023.05 - 2023.05.3
vmware	Application	Vmware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12
	Server	vCenter Server: 7.0-7.0U3n 8.0- 8.0UIc, VMware Cloud Foundation 5.x, 4.x

Targeted Countries



Color	Countries
	United Arab Emirates
	United States
	Turkey
	Syria
	South Korea
	Saudi Arabia
	Lebanon
	Japan
	Israel
	Cyprus
	China
	Yemen
	Vietnam
	Thailand
	Singapore
	Russia
	Qatar
	Philippines
	Oman
	North Korea
	Mongolia
	Kuwait
	Jordan

Color	Countries
	Iraq
	Iran
	India
	Bahrain
	Afghanistan
	Uzbekistan
	Turkmenistan
	Timor-Leste
	Tajikistan
	Sri Lanka
	South Africa
	Poland
	Pakistan
	Nepal
	Maldives
	Malaysia
	Laos
	Kyrgyzstan
	Kazakhstan
	Indonesia
	Egypt
	Cambodia
	Brunei
	Bhutan
	Bangladesh

Color	Countries
	United Kingdom
	Taiwan
	Spain
	Slovenia
	Slovakia
	Romania
	Lithuania
	Latvia
	Italy
	Hungary
	Guyana
	Germany
	Georgia
	France
	Estonia
	Croatia
	Canada
	Bulgaria
	Brazil
	Belgium
	Azerbaijan
	Austria
	Australia
	Armenia
	Argentina

Color	Countries
	Zimbabwe
	Zambia
	Venezuela
	Vanuatu
	Uruguay
	Ukraine
	Uganda
	Tuvalu
	Tunisia
	Trinidad and Tobago
	Tonga
	Togo
	Tanzania
	Sweden
	Suriname
	Sudan
	South Sudan
	Somalia
	Solomon Islands
	Sierra Leone
	Seychelles
	Serbia

Color	Countries
	Senegal
	Samoa
	Saint Vincent and the Grenadines
	Saint Lucia
	Saint Kitts and Nevis
	Rwanda
	Portugal
	Peru
	Paraguay
	Papua New Guinea
	Panama
	Palestine
	Palau
	North Macedonia
	Nigeria
	Niger
	Nicaragua
	New Zealand
	Netherlands
	Nauru
	Namibia

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1574.002** DLL Side-Loading	**T1203** Exploitation for Client Execution
T1082 System Information Discovery	**T1068** Exploitation for Privilege Escalation	**T1566** Phishing	**T1083** File and Directory Discovery	**T1027** Obfuscated Files or Information
T1486 Data Encrypted for Impact	**T1547** Boot or Logon Autostart Execution	**T1562** Impair Defenses	**T1055** Process Injection	**T1547.001** Registry Run Keys / Startup Folder
T1588.005 Exploits	**T1071** Application Layer Protocol	**T1059.001** PowerShell	**T1574** Hijack Execution Flow	**T1036** Masquerading
T1057 Process Discovery	**T1105** Ingress Tool Transfer	**T1005** Data from Local System	**T1562.001** Disable or Modify Tools	**T1573** Encrypted Channel

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
BunnyLoader	MD5	Dbf727e1effc3631ae634d95a0d88bf3, Bbf53c2f20ac95a3bc18ea7575f2344b, 59ac3eacd67228850d5478fd3f18df78
	IPv4	37[.]139[.]129[.]145
Sfile	MD5	ae8c22cc7542b4a3dc92cca88897048f, fdc8e99745554b1138a431c15168364d, 575934448f3a30696336644d6c379db9, 0493958b9915e5799927716aa5b82191, 1875e9d8031876674d4d236ffab6b826, 4f44f3a05d014ee1a4e85f67436abcb9, 38ca7e711977058ae3ae702b2ea676b0, c83874d9e1f6531a05c61d40ebe9b82a, a1e880b1bf079e1c9ac9a9238c68e674
	SHA1	0f20e5ccdbbed4cc3668577286ca66039c410f95, 14e4557ea8d69d289c2432066d860b60a6698548, 28f73b38ace67b48e525d165e7a16f3b51cec0c0, 5ffac9dff916d69cd66e91ec6228d8d92c5e6b37, 665572b84702c4c77f59868c5fe4d0b621f2e62a, 6960beedbf4c927b75747ba08fe4e2fa418d4d9b, 8c507d26c2fec90707320ffb721ae626139bbf11, a67686b5ce1d970a7920b47097d20dee927f0a4d, bdb0c0282b303843e971fbcd6d2888d834da204c
	SHA256	e82606b7c179cd39d0e68d9f61723c4b2c909c44e2630c69d7038cd0f1bcb595, 451c4ff0a4313c98b519179eb276914d18d01eb1d6b1a28d6af15fda1693ec34, 8396728b5267a9ff823db2ab600e3ef1d131fc36596d24747ac494e8cdfe877c, 26b7c7079cfea22cd9335b788db32453a727c81aec313a3637391a9763434f0a, 92c24d0c2075133e91f1be803c00478c733ee5be5610564efc48dd160cf2c632, 97d679f364b1d0c6e3896574f1338801a0d707c137e4d220d2c974ae40fbe708, 7195995c6ea6afc08bdfa51f7227ee3398aec95f242e992c900f14eb644dd838

Attack Name	TYPE	VALUE
Qakbot	SHA256	006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b
HyperBro	MD5	af43e0c21ddf7e4e087cdab2ac8d2948, 7d75561cb378e54c5711f077858a4a48, 4109ac08bdc8591c7b46348eb1bca85d, b35c698732f49f998f6e6b6b83cfa9dd, b5cb7044a189f8752ecdbc799f25ce06
	SHA1	b8d9bba99d9777c43b96f338f5bc3a08201fa05c, 692b407893846cdd5d3e75110402fe1e7bf5515e, 6423d1c324522bfd2b65108b554847ac4ab02479, 13e334a4857b8bee0283e5e193fa7983d5c0ee06, 9e08fdd7eaeffbbf6e441060e02dc29b0f66b118
	SHA256	12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df, 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b, df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348, 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5, df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9
	URL	http://38[.]54[.]119[.]239:443/jquery-3.3.1.min.js ,
ChargeWeapon	MD5	44ee43adc8f423db4a461fc99731cdb9
	SHA1	0fd8c9ed43d66022a08cc8ed7e78c4a6216cf26c
	SHA256	3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135
	IPv4	45[.]77[.]37[.]145:8443
hailBot	IPv4	34.147.16[.]24, 34.165.70[.]211, 34.176.112[.]249, 34.64.52[.]239, 34.69.75[.]60, 34.92.28[.]223, 35.188.240[.]127, 5.181.80[.]115, 5.181.80[.]120, 5.181.80[.]70, 5.181.80[.]71
	MD5	f30a468b56c5761e346f3e709fd098e

Attack Name	TYPE	VALUE
DarkGate	SHA1	4ed69ed4282f5641b5425a9fca4374a17aecb160, 549cb39cea44cf8ca7d781cd4588e9258bdff2a1, e108fe723265d885a51e9b6125d151b32e23a949, a85664a8b304904e7cd1c407d012d3575eeb2354, 924b60bd15df000296fc2b9f179df9635ae5bfed, cec7429d24c306ba5ae8344be831770dfe680da4, d9a2ae9f5cffba0d969ef8edbbf59dc50586df00, 381bf78b64fcdf4e21e6e927edd924ba01fdf03d, 4c24d0fc57633d2befaac9ac5706cbc163df747c, 9253eed158079b5323d6f030e925d35d47756c10, 0e7b5d0797c369dd1185612f92991f41b1a7bfa2, 7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc, e47086abe1346c40f58d58343367fd72165ddecd, 42fe509513cd0c026559d3daf491a99914fcc45b, 93cb5837a145d688982b95fab297ebdb9f3016bc, f7b9569a536514e70b6640d74268121162326065, d40c7afee0dd9877bbe894bc9f357b50e002b7e2, 1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc, 3229a36f803346c513dbb5d6fe911d4cb2f4dab1, 6585e15d53501c7f713010a0621b99e9097064ff, 001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2, ad1667eaf03d3989e5044faa83f6bb95a023e269, a3516b2bb5c60b23b4b41f64e32d57b5b4c33574, e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f, 3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1, f3a740ea4e04d970c37d82617f05b0f209f72789, e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10, 45a89d03016695ad87304a0dfd04648e8dfeac8f
	Domains	msteamseyeappstore[.]com, Drkgatevservicceoffice[.]net, reactervnamnat[.]com, coocooncookiedpo[.]com, wmnwserviceadsmark[.]com, onlysportsfitnessam[.]com, marketisportsstumi[.]win
	IPv4:Port	5.188.87[.]58[:]2351
	URl	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin
PEAPOD	Domains	budgetnews[.]org, wirelessvezion[.]com, redditanalytics[.]pm, netstaticsinformation[.]com
	URL	hXXps://onedrive[.]live[.]com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317
	SHA256	83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c
	File Name	pcmf-installer-23.0.5.exe

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42114	✗	Exim: 4.96 or earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1082: System Information Discovery	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42115	✗	Exim: 4.96 or earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42116		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Buffer Overflow Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42117		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42118		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-191	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42119		Exim: 4.96 or earlier versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*:*	-
Exim Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-125	T1082: System Information Discovery	https://exim.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22515		Confluence Data Center and Confluence Server Versions- 8.0.x, 8.1.x, 8.2.x, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*:*:*:*	-
Atlassian Confluence Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34362		Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:moveit_cloud:*:*:*:*:*:*:*:*	Clop Ransomware
Progress MOVEit Transfer SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-89	T1055: Process Injection	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-17215		Huawei HG532: All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:huawei:hg532:-:*:*:*:*:*:*:*	HailBot
Huawei HG532 Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882		Microsoft Office: 2007 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	HailBot
Microsoft Office Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-44487</td><td>  </td><td rowspan="2">Microsoft IIS: 10.0, Apache Tomcat: 8.5.0 - 11.0.0-M11, Netty: 4.0.0 - 4.1.99, Jetty: 9.0.0.v20130308 - 12.0.1</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>cpe:2.3:o:microsoft:IIS:10.0:*:*:*:*:*:*:*cpe:2.3:a:apache_foundation:apache_tomcat:11.0.0-M11:*:*:*:*:*:*:*cpe:2.3:a:netty:netty:4.1.99:*:*:*:*:*:*:*cpe:2.3:a:eclipse:jetty:9.4.53.v20230927:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td rowspan="3">HTTP/2 Rapid Reset Attack Vulnerability</td><td>  </td><td></td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-400</td><td>T1498: Network Denial of Service; T1584.005: Compromise Infrastructure:Botnet</td><td>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-44487; https://netty.io/downloads.html; https://mvnrepository.com/artifact/org.eclipse.jetty/jetty-servlets/9.4.53.v20231009</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41763	✗	Skype for Business Server: before 7.0.246.530	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:skype_for_business_server:*:*:*:*:*:*:*:*	-
Microsoft Skype for Business Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-41763

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36563	✗	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	-
Microsoft WordPad Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36563

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0803	 ZERO-DAY	Windows: 7 - 10 1809 Windows Server: 2008 - 2019 1803	Grayling APT
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
Microsoft Win32k Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134	 ZERO-DAY	Confluence Server and Confluence Data Center	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	AvosLocker ransomware
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40539	✗	Zoho ManageEngine ADSelfService Plus: 6000 - 6113	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:*:*:*:*:*:*:*	AvosLocker ransomware
Zoho ADSelfService Plus Remote code execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-706	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20273	✗	Cisco IOS XE- All versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios_xe:*	-
Cisco IOS XE Web UI Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20198	✗	Cisco IOS XE- All versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios_xe:*	-
Cisco IOS XE Web UI Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z#REC

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR: 3.20 - 6.23 beta 1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	SmokeLoader, Nanocore RAT, Crimson RAT, AgentTesla, BOXRAT and Rhadamanthys info stealer
WinRAR Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://www.winrar.com/singlenewsview.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-4966</td><td>  </td><td rowspan="2">NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300</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:citrix:netscaler_application_delivery_controller:*:*:*:*:*:-:*:*:*
cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*:*
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:fips:*:*:*
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:ndcpp:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-119</td><td>T1574: Hijack Execution Flow; T1499.004: Application or System Exploitation; T1563: Remote Service Session Hijacking; T1548.002: Bypass User Account Control; T1210: Exploitation of Remote Services</td><td>https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42793	✗	TeamCity: 2023.05 - 2023.05.3	Lazarus Group & Andariel
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	ForestTiger, FeedLoad, RollSling, HazyLoad
JetBrains TeamCity Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application; T1040: Network Sniffing	https://www.jetbrains.com/teamcity/download/other.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0213	✗	Windows: 7 – 10, Windows Server: 2008 - 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation; T1204: User Execution;	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40449	✗ ZERO-DAY	Windows: 7 - 11 21H2 Windows Server: 2008 - 2019 2004	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	MATA Backdoor
Microsoft Windows Win32k Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation; T1204: User Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26411	✗ ZERO-DAY	Microsoft Internet Explorer: 9 - 11	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:edge:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:*	MATA Backdoor
Microsoft Internet Explorer Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1005: Data from Local System; T1499: Endpoint Denial of Service; T1211: Exploitation for Defense Evasion; T1212: Exploitation for Credential Access	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34051	✗	Vmware Aria Operations for Logs (formerly vRealize Log Insight): 8.0.0 - 8.12	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vreaalize_log_insight:8.12:*:*:*:*:*:*:*	-
VMware Aria Operations for Logs Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application	https://www.vmware.com/security/advisories/VMSA-2023-0021.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-5631	✗	Roundcube: 1.0.0 - 1.6.3	Winter Vivern
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Cross Site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application	https://roundcube.net/download/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2018-19320</td><td>  </td><td rowspan="2">GIGABYTE APP Center: 1.05.21
AORUS GRAPHICS ENGINE: 1.0 - 1.33
XTREME GAMING ENGINE: 1.22 - 1.25
OC GURU: 2.08</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:gigabyte:aorus_graphics_engine:*:*:*:*:*:*:*:*</td><td rowspan="2">AvosLocker ransomware</td></tr>
<tr><td rowspan="3">GIGABYTE Multiple Products Unspecified Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-782</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://www.gigabyte.com/Support/Security/1801</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34048	✗	vCenter Server: 7.0-7.0U3n 8.0- 8.0UIc, VMware Cloud Foundation 5.x, 4.x	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:vcenter-server:8.0:U1c:*:*:*:*:*:*:*	-
VMware vCenter Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U2&productId=1345&rPId=110105 , https://customerconnect.vmware.com/downloads/details?downloadGroup=VC80U1D&productId=1345&rPId=112378 , https://customerconnect.vmware.com/downloads/details?downloadGroup=VC70U3O&productId=974&rPId=110262,https://kb.vmware.com/s/article/88287

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EvilProxy	EvilProxy is a phishing-as-a-service platform that employs reverse proxies to simplify communication and transfer user information between the target, and the malicious actors orchestrating the phishing campaign.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Phishing-as-a-service kit		Unauthorised Access	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BunnyLoader	BunnyLoader is a type of malware that is openly available for purchase on various online forums. This malicious software provides cybercriminals with a wide range of features and functionalities, including the ability to download and execute a second-stage payload, as well as harvest browser credentials and system information from infected machines. It is often marketed at a price of $250.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information Disclosure	-
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
DinodasRAT	DinodasRAT is a remote access trojan developed in C++ with various capabilities that allow an attacker to spy on and collect sensitive information from a victim's computer.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote access trojan (RAT)		Exfiltrate files, manipulate Windows registry keys, and execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Qakbot (aka QBot, QuackBot, and Pinkslipbot)	Qakbot is a modular second-stage malware with backdoor capabilities, initially purposed as a credential stealer. Qakbot steals sensitive data and attempts to self-propagate to other systems on the network. Qakbot also provides RCE capabilities, allowing attackers to perform manual attacks to achieve secondary objectives such as scanning the compromised network or injecting ransomware.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Deliver payloads, including ransomware	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Ransom Knight ransomware (aka Cyclops)	Knight ransomware is the rebrand of Cyclops. It is designed to encrypt files and demand ransoms for their decryption.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information stealing	-
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos backdoor	Remcos is a sophisticated remote access Trojan (RAT) that can be used to fully control and monitor any Windows computer from XP and onwards.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft	-
Backdoor			
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.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Clop Ransomware</td><td rowspan="6">Clop is a type of ransomware that is known for encrypting a victim's files and appending the ".clop" extension to them. One distinctive feature of Clop ransomware is the string "Dont Worry C|0P" that is often included in the ransom notes left behind for the victim. Clop is known to attempt to disable Windows Defender and remove Microsoft Security Essentials from the infected system, aiming to evade detection by security software running in the user space.</td><td>Phishing</td><td>CVE-2023-34362
CVE-2023-35036
CVE-2023-35708
CVE-2023-36934
CVE-2023-36932
CVE-2023-36933</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Unauthorized access and data breaches</td><td>Progress MOVEit Transfer</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 , https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023 , https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023 , https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023</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
LostTrust	LostTrust ransomware, emerged in September 2023, is a multi-extortion threat related to SFile and Mindware, employing techniques reminiscent of MetaEncryptor, encrypting files and demanding ransoms. It presents a serious cybersecurity concern due to its similarities to other ransomware families.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Compromised systems, and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SFile	SFile aka SFile2, Escal malware is a ransomware that encrypts files on a victim's computer and demands a ransom payment in exchange for the decryption key. First appearing in 2021. SFile is known to be particularly difficult to detect and remove, as it uses a variety of evasion techniques.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Financial loss and Compromised systems	Windows
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
Mindware	Mindware malware is a ransomware that targets the human mind. It is designed to exploit human psychology and manipulate people into making mistakes or taking actions that they would not otherwise take.	Social engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Financial loss and Compromised systems	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MetaEncryptor	MetaEncryptor is a ransomware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. It was first discovered in early 2023 and has since been used in a number of high-profile attacks.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data theft, Financial loss and Compromised systems	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HyperBro	HyperBro is a sophisticated RAT that can be used to take control of a victim's computer, steal data, and perform other malicious activities. . It was first discovered in 2017 and has since been utilized by the APT27 threat group	Social engineering	APT27
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Stealing sensitive information	Windows
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
Cobalt Strike	Cobalt Strike (aka Agentemis, BEACON, CobaltStrike, cobeacon) is a commercial penetration testing tool that is also used by threat actors to launch attacks against organizations. It is a powerful tool that can be used to perform a variety of malicious activities	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
-		Gaining unauthorized access, Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ChargeWeapon	ChargeWeapon is a malicious software designed to establish remote access and transmit device and network data from a compromised host to a command-and-control (C2) server under the control of an attacker	Social engineering	
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mirai	Mirai is a malware that infects IoT devices and turns them into bots that can be used to launch distributed denial-of-service (DDoS) attacks. Since its first appearance in 2016, Mirai has evolved into multiple variants, each with its own unique features.	-	CVE-2017-17215 CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

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
HailBot	HAILBOT is a new variant of the Mirai botnet that was discovered in 2023. It is known to exploit vulnerabilities in Huawei HG532 routers and to target financial and trade institutions, as well as IoT platforms.	Exploiting vulnerabilities	CVE-2017-17215 CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks	IoT platforms
ASSOCIATED ACTOR			**PATCH LINK**
-			http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KiraiBot	kiraiBot is a new variant of the Mirai botnet that was discovered in 2023. It is known to exploit vulnerabilities in a variety of devices, including routers, cameras, and NAS devices. kiraiBot is also known to target financial and trade institutions, as well as IoT platforms	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	IoT platforms
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
catDDoS	CatDDoS is a new variant of the Mirai botnet that was discovered in 2023 and is exploits vulnerabilities in IoT devices to turn them into bots that can be used to launch distributed denial-of-service (DDoS) attacks.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	IoT platforms
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
Lu0Bot	Lu0Bot Malware, a Node.js-based threat, surfaced in February 2021 as a secondary payload in GCleaner attacks. This malware acts as a bot, responding to C2 server commands and transmitting encrypted system data while employing intricate obfuscation techniques for stealth.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CurKeep	CurKeep malware that is used in the Stayin' Alive targeted attack campaign. It is a small, lightweight malware that is difficult to detect. Once CurKeep is installed on a system, it establishes persistence by creating a scheduled task and copying itself to the %APPDATA% folder. CurKeep then collects information about the infected system	Phishing Emails	CVE-2022-23748
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748

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
CurLu	CurLu malware is a malicious downloader that is used in the Stayin' Alive targeted attack campaign. It is a small, lightweight malware that is difficult to detect.	Phishing emails	CVE-2022-23748
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CurLog	CurLog malware is a sophisticated and relatively new threat that is used in the Stayin' Alive targeted attack campaign. It is a lightweight and cross-platform downloader malware that is written in the Golang programming language.	Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Stealing sensitive information	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Balada Injector	Balada Injector is a malware that is used to inject malicious code into websites, typically WordPress websites. It is a sophisticated malware that is difficult to detect and remove. Balada Injector is used to deliver a variety of malware, including backdoors, Trojans, and ransomware.	Phishing emails and exploit vulnerabilities	CVE-2023-3169
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Injector		Information Theft	WordPress
ASSOCIATED ACTOR			**PATCH LINK**
-			https://wpscan.com/vulnerability/e6d8216d-ace4-48ba-afca-74da0dc5abb5/

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>AvosLocker</td><td rowspan="7">AvosLocker, also known as Avos, was first detected on July 4, 2021, and operates as a ransomware-as-a-service (RaaS), using a double extortion technique. It has compromised organizations in various critical infrastructure sectors primarily in the United States.</td><td>Compromised RDP/VPN credentials or by exploiting vulnerabilities</td><td>CVE-2021-31206, CVE-2021-31207, CVE-2021-34473, CVE-2021-34523, CVE-2021-26855, CVE-2021-40539, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-26134, CVE-2018-19320,</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Gaining unauthorized access, Data Theft and Financial loss</td><td>Windows, Linux, and VMware ESXi</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855; https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html; https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/; https://logging.apache.org/log4j/2.x/security.html; https://issues.apache.org/jira/browse/LOG4J2-3293; https://jira.atlassian.com/browse/CONFSERVER-79016</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
ShellBot	ShellBot malware, targeting poorly managed Linux SSH servers, now employs hexadecimal IP addresses in its download URLs to evade detection.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Launch DDoS attacks And Data Theft	Linux SSH servers
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkGate	DarkGate is a commodity malware that is used in a variety of cyber attacks, including targeted attacks and mass attacks. DarkGate is a versatile malware that can be used to steal data, install additional malware, launch denial-of-service attacks, and take control of infected systems.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Launch DDoS attacks And Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SeroXen RAT	SeroXen is a recently surfaced Remote Access Trojan (RAT) that is deceptively promoted as a legitimate tool. It is conveniently accessible and deployable through a dedicated website, making it appealing even to users with limited technical expertise.	Social engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Launch DDoS attacks, Install other malware And Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PEAPOD (aka ROMCOM 4.0)	The latest version of RomCom, known as PEAPOD, has been simplified to include core features, allowing it to execute commands, manage files, collect system data, and even remove itself from compromised systems.	Spear-phishing emails and malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Extortion of data	-
ASSOCIATED ACTOR			**PATH LINK**
Storm-0978			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XorDDoS	The XorDDoS Trojan, a Linux-based malware, encrypts its data using an XOR encryption key. It collects essential information about the compromised device and uses CRC codes for error detection during network communication.	Exploiting vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Denial of Service, Data Theft, and compromised systems	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Volgmer (aka FALLCHILL, Manuscrypt)	Volgmer, a DLL-type backdoor, has been discreetly installed to masquerade as a legitimate file. Volgmer exhibits a unique characteristic of employing specific logic to randomly generate strings for the name of the Volgmer DLL file.	Spear phishing and supply chain attacks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Scout	Scout Downloader, once activated, displays a graphical user interface (GUI), setting it apart from typical malware behaviors. Scout employs a file name-based lookup of the registry value housing encrypted configuration data.	Spear phishing and supply chain attacks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BbyStealer	The BbyStealer malware duplicates itself, placing the copy in the startup folder to ensure persistence. Subsequently, it terminates web browser processes and proceeds to extract valuable information from the compromised system. This is achieved by creating duplicates of the user data folder and appending the ".bby" extension.	Phishing domains	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft and Espionage	Windows
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SmokeLoader (aka Dofoil, Sharik, Smoke)	SmokeLoader can be used to drop other malware on infected systems, but operators can choose additional modules that allow for information-stealing capabilities.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.winrar.com/singlenewsview.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
Nanocore (aka Nancrat, NanoCore)	NanoCore is a modular remote access tool developed in .NET that can be used to spy on victims and steal information.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crimson (aka SEEDOOR, Scarimson)	Crimson RAT has the ability to exfiltrate files and system info and send it to its C2 server using non-web channels. The RAT is designed to capture the screen and terminate any ongoing processes.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AgentTesla (aka Negasteal)	Agent Tesla is a.NET framework-based spyware Trojan. The malware can collect keystrokes, access the host's clipboard, and search the disk for credentials or other useful data. It can send data back to its command and control over HTTP(S), SMTP, FTP, or Telegram channels.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.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
HazyLoad	The HazyLoad proxy tool facilitates a persistent connection between the compromised server and Andariel's servers. Regardless of the specific techniques used, the attackers ultimately extract credentials from the LSASS memory.	Exploiting Vulnerability	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys	Rhadamanthys is a stealer that is meant to steal information from affected computers. Rhadamanthys is downloaded alongside the actual software, reducing user suspicion. These sites were promoted using Google advertisements, which took precedence over legitimate Google search results.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
xRAT (aka QuasarRAT)	xRAT, now known as QuasarRAT in newer versions, is a remote access tool whose source code is openly available on GitHub. Because of this, anyone may easily clone and compile the project and is actively maintained.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-

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
BabyShark	BabyShark is a malware family that uses Microsoft Visual Basic (VB) scripts. Since the malware is launched from a remote site, it can be supplied via a variety of file types, including PE files and malicious documents. It sends system information to the C2 server and maintains persistent access to the system.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RevClient	RevClient is an RDP-related malware that operates by accepting commands from the command-and-control server. It can conduct user account-related tasks or port forwarding, depending on the instructions provided.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TinyNuke (aka NukeBot, Nuclear Bot, MicroBankingTrojan)	TinyNuke can steal credentials with form-grabbing and web-inject capabilities for Firefox, Internet Explorer, and Chrome, and it can also install extra payloads.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-

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
ForestTiger	ForestTiger malware serves as a backdoor, allowing threat actors to execute commands on the infected system. The ForestTiger conducts scheduled tasks on compromised systems as well as credentials and utilizes them to dump credentials via the LSASS memory.	Exploiting Vulnerability	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FeedLoad	FeedLoad's primary function is to install a RAT, providing the threat actors with remote control and access to the affected server. Following a successful compromise.	DLL search order hijacking	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GHOSTPULSE	GHOSTPULSE malware is a new type of malware that was discovered in October 2023. It operates as a multi-stage loader, decrypting its payload and deploying various types of malware while employing advanced defense evasion techniques.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
loader		Executes other malware	-
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
Phobos	Phobos actors tend to prioritize targeting servers rather than end-user computers, and it exclusively affects Windows operating systems. Phobos ransomware is known for being a double extortion ransomware, where it first exfiltrates data and then encrypts files using the AES encryption method.	Phishing emails	CVE-2021-34527 CVE-2021-1675 CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage, Data Extortion and compromised system	Microsoft Windows Print Spooler
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MATA (aka Dacls)	The MATA malware is a backdoor framework that is written in C++ and the updated version is harder to detect and remove. MATA backdoor allowed the attackers to remotely control the victim's computer, steal data, and deploy additional malware. This multi-faceted attack campaign highlights the MATA cluster's advanced tactics and their ability to adapt and evolve their malware.	Spear-phishing	CVE-2021-40449 CVE-2021-26411
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Compromising financial software servers, Exfiltration of data and Financial Loss	Microsoft Internet Explorer & Windows
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449 https://potal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerExchange	PowerExchange, a PowerShell-based malware, has the capability to access an Exchange Server using hardcoded credentials and monitor emails sent by the attackers. It utilizes the Exchange Server as a command and control (C&C) center.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
OilRig			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clipog	Clipog is an information-stealing malware with the ability to copy clipboard data, capture keystrokes, and record the processes of the entered keystrokes.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
OilRig			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Munchkin	Munchkin allows threat operators to run BlackCat on remote machines, as well as to deploy it for the purpose of encrypting remote SMB and CIFS network shares. Munchkin runs on a customized version of Alpine Linux and is delivered in the form of an ISO file.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackCat (aka AlphaV, AlphaVM, ALPHV-ng, or Noberus)	BlackCat ransomware drew attention due to its use of the Rust programming language and its Ransomware-as-a-Service (RaaS) business model. BlackCat is extremely customizable and can be tailored to create targeted Executables.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Quasar RAT (aka xRAT, CinaRAT, Yggdrasil)	Quasar RAT is an open-source remote administration tool developed in C#. It comes with a variety of features, including the ability to gather system information, list running applications, retrieve files, log keystrokes, capture screenshots, and execute arbitrary shell commands on the compromised host.	DLL side-loading	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Deploying and executing malicious payloads	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Netrunner	Netrunner is a custom Go-based backdoor that performs data theft, likely aiding espionage operations. The backdoor is distinguished primarily by its command-and-control server configurations.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Dmcserv	Dmcserv is a custom Go-based backdoor that performs data theft, likely aiding espionage operations. The backdoor is distinguished primarily by its command-and-control server configurations.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ExelaStealer	Exela Stealer is a Python-based tool designed to discreetly extract sensitive data, including credentials, tokens, sessions, cookies, and more. It accomplishes this covert data exfiltration solely through Discord webhook URLs.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Gather sensitive data, including passwords, credit card information, cookies, sessions, and keystrokes.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoPIX	GoPIX is a typical clipboard stealer malware that steals PIX “transactions” used to identify payment requests and replaces them with a malicious one which is retrieved from the C2. The malware also supports substituting Bitcoin and Ethereum wallet addresses.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal PIX transactions, financial and personal information.	-
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
StripedFly	StripedFly is a complex modular malware, enabling attackers to establish network persistence, gain a comprehensive insight into network activities, and exfiltrate credentials. It boasts advanced features such as TOR-based traffic obscuring methods for communication with command servers, automated update and delivery capabilities.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Inject Shellcode	-
Modular			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ThunderCrypt	ThunderCrypt is a ransomware-type virus distributed via fake Adobe Flash Player updates. Once infiltrated, ThunderCrypt encrypts various data using RSA-2048 cryptography. It opens a pop-up window containing a ransom-demand message	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Demand Ransom	-
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SIGNBT	SIGNBT malware is a loader, which means that it is used to load other malware onto a victim's system. It can load a variety of different types of malware, such as backdoors, ransomware, and data stealers. It has been attributed to the North Korean Lazarus Group.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Inject Shellcode	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LPEClient	LPEClient malware is an HTTP(S) downloader that is used to download and execute other malware on a victim's system. It is often used to download and execute backdoors, ransomware, and other types of malware that can be used to steal data, disrupt operations, or gain control of systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Executes other malware, stealing data	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BiBi-Linux	BiBi-Linux malware is a new Linux wiper malware that has been used to target Israeli organizations. It was first discovered in October 2023, and it is believed to be used by a pro-Hamas hacktivist group.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Data loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Grayling APT	Unknown	Government, Manufacturing, IT, and Biomedical	Taiwan, Vietnam, U.S, and Asia-Pacific region
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2019-0803	-	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, T1070: Indicator Removal, T1083: File and Directory Discovery, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1562: Impair Defenses			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ToddyCat	China	Telecommunication, Government	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-23748	CurKeep, CurLu, CurLog	Windows
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, T1083: File and Directory Discovery, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1562: Impair Defenses, T1071: Application Layer Protocol, T1566.001: Spearphishing Attachment, T1566: Phishing, T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Winter Vivern (aka UAC-0114, TA473)	Unknown	Defense and Government	India, Lithuania, Poland, Slovakia, Ukraine, USA and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-5631	-	Roundcube
TTPs			
T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1587: Develop Capabilities; T1587.004: Exploits; T1190: Exploit Public-Facing Application; T1566: Phishing; T1203: Exploitation for Client Exécution; T1087: Account Discovery; T1087.003: Email Account; T1114: Email Collection; T1114.002: Remote Email Collection; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0978 (aka Tropical Scorpius, RomCom, Void Rabisu, DEV-0978)	Russia	Construction, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Shipping and Logistics, Transportation.	European Union
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PEAPOD (aka ROMCOM 4.0)	-
TTPs			
T1566: Phishing;T1566.002: Spearphishing Link;T1608: Stage Capabilities;T1608.001: Upload Malware;T1574: Hijack Execution Flow;T1574.002: DLL Side-Loading;T1587: Develop Capabilities;T1587.002: Code Signing Certificates;T1071: Application Layer Protocol;T1071.001: Web Protocols;T1204: User Execution;T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 OilRig (aka Crambus, Helix Kitten, APT 34, Twisted Kitten, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, EUROPIUM, Hazel Sandstorm)	Iran	Government	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PowerExchange, Clipog	-
TTPs			
T1566: Phishing;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1003: OS Credential Dumping;T1016: System Network Configuration Discovery;T1021.001: Remote Desktop Protocol;T1005: Data from Local System;T1041: Exfiltration Over C2 Channel;T1105: Ingress Tool Transfer;T1056.001: Keylogging;T1113: Screen Capture			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 

Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</td><td>North Korea</td><td rowspan="3">Satellite, Software, Media, Defense, Manufacturing, ICT, And Financial Sectors.</td><td rowspan="3">Korea</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2023-42793</td><td>Volgmer, Scout, ForestTiger, FeedLoad, RollSling, HazyLoad, SIGNBT, LPEClient</td><td>TeamCity</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing;T1195: Supply Chain Compromise;T1204: User Execution;T1047: Windows Management Instrumentation;T1543: Create or Modify System Process;T1574.002: DLL Side-Loading;T1070: Indicator Removal;T1573: Encrypted Channel;T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)	North Korea	Defense, Diplomatic, Education, Media industries, Energy, Government, Healthcare, Manufacturing, Think Tanks	France, Japan, Russia, South Africa, South Korea, United Kingdom, United States, Thailand, Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	xRAT, BabyShark, RevClient, TinyNuke	-
TTPs			
T1047: Windows Management Instrumentation;T1055: Process Injection;T1087: Account Discovery;T1140: Deobfuscate/Decode Files or Information;T1016: System Network Configuration Discovery;T1497: Virtualization/Sandbox Evasion;T1566: Phishing;T1566.001: Spearphishing Attachment;T1021: Remote Services;T1056: Input Capture;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1059.003: Windows Command Shell;T1059.005: Visual Basic;T1204: User Execution;T1204.002: Malicious File;T1204.001: Malicious Link;T1105: Ingress Tool Transfer;T1104: Multi-Stage Channels;T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)	North Korea	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-42793	ForestTiger, FeedLoad, RollSling, HazyLoad	TeamCity
TTPs			
T1588: Obtain Capabilities;T1588.006: Vulnerabilities;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1574: Hijack Execution Flow;T1574.001: DLL Search Order Hijacking;T1105: Ingress Tool Transfer;T1136: Create Account;T1021: Remote Services;T1021.001: Remote Desktop Protocol;T1003: OS Credential Dumping;T1003.001: LSASS Memory;T1007: System Service Discovery			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
YoroTrooper</td><td>Unknown</td><td rowspan="3">Energy and Government</td><td rowspan="3">Azerbaijan, Kyrgyzstan, Tajikistan, Turkey, Turkmenistan and Europe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1595: Active Scanning; T1590: Gather Victim Network Information; T1588.006: Vulnerabilities; T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1548: Abuse Elevation Control Mechanism; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1046: Network Service Discovery; T1105: Ingress Tool Transfer; T1041 Exfiltration Over C2 Channel</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1598: Phishing for Information	
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
		T1588.001: Malware
		T1588.002: Tool
	T1584: Compromise Infrastructure	T1584.004: Server
	T1583: Acquire Infrastructure	T1583.001: Domains
	T1586: Compromise Accounts	
	T1584: Compromise Infrastructure	T1584.005: Botnet
		T1584.004: Server
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
		T1587.003: Digital Certificates
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.006: SEO Poisoning
TA0001: Initial Access	T1133: External Remote Services	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003:Spearphishing via Service
	T1189: Drive-by Compromise	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1190: Exploit Public-Facing Application	
TA0002: Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.007: JavaScript
		T1059.005: Visual Basic
		T1059.008: Network Device CLI
		T1059.006: Python
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1204: User Execution	T1204.002: Malicious File
	T1047: Windows Management Instrumentation	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	

Tactic	Technique	Sub-technique
TA0002: Execution	T1106: Native API	
	T1204: User Execution	T1204.001: Malicious Link
	T1559: Inter-Process Communication	T1559.001: Component Object Model
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	T1547.009: Shortcut Modification
		T1547.001: Registry Run Keys / Startup Folder
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1133: External Remote Services	
	T1543: Create or Modify System Process	T1543.001: Launch Agent
	T1556: Modify Authentication Process	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1547: Boot or Logon Autostart Execution	T1547.008: LSASS Driver
	T1546: Event Triggered Execution	T1546.008: Accessibility Features
	T1098: Account Manipulation	
	T1136: Create Account	
	T1136: Create Account	T1136.001: Local Account
TA0004: Privilege Escalation	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
	T1055: Process Injection	T1055.013: Process Doppelgänging
		T1055.001: Dynamic-link Library Injection
		T1055.011: Extra Window Memory Injection
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1546: Event Triggered Execution	T1546.008: Accessibility Features
	T1055: Process Injection	T1055.012: Process Hollowing
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.001: Invalid Code Signature
		T1036.006: Space after Filename
		T1036.007: Double File Extension
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.006: Timestomp
		T1070.004: File Deletion
	T1484: Domain Policy Modification	T1484.002: Domain Trust Modification
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.009: Embedded Payloads
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
	T1127: Trusted Developer Utilities Proxy Execution	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1014: Rootkit	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1140: Deobfuscate/Decode Files or Information	
	T1006: Direct Volume Access	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1211: Exploitation for Defense Evasion	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1112: Modify Registry	
	T1202: Indirect Command Execution	
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
		T1497.002: User Activity Based Checks
		T1497.001: System Checks
	T1218: System Binary Proxy Execution	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1620: Reflective Code Loading	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts

Tactic	Technique	Sub-technique
TA0007: Discovery	T1057: Process Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1217: Browser Information Discovery	
	T1012: Query Registry	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1010: Application Window Discovery	
	T1018: Remote System Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1040: Network Sniffing	
	T1033: System Owner/User Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.002: User Activity Based Checks
		T1497.003: Time Based Evasion
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.004: SSH
	T1570: Lateral Tool Transfer	
	T1072: Software Deployment Tools	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
TA0009: Collection	T1005: Data from Local System	
	T1115: Clipboard Data	
	T1113: Screen Capture	
	T1530: Data from Cloud Storage	
	T1056: Input Capture	T1056.001: Keylogging
	T1560: Archive Collected Data	
TA0011: Command and Control	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1572: Protocol Tunneling	
	T1105: Ingress Tool Transfer	
	T1571: Non-Standard Port	
	T1132: Data Encoding	T1132.001: Standard Encoding
		T1132.002: Non-Standard Encoding
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1095: Non-Application Layer Protocol	
	T1205: Traffic Signaling	T1205.001: Port Knocking
	T1219: Remote Access Software	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1041: Exfiltration Over C2 Channel	
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1498: Network Denial of Service	
	T1496: Resource Hijacking	
	T1529: System Shutdown/Reboot	
TA0006: Credential Access	T1110: Brute Force	T1110.003: Password Spraying
	T1212: Exploitation for Credential Access	
	T1539: Steal Web Session Cookie	
	T1040: Network Sniffing	
	T1606: Forge Web Credentials	T1606.001: Web Cookies
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1621: Multi-Factor Authentication Request Generation	
	T1556: Modify Authentication Process	T1556.004: Network Device Authentication
	T1552: Unsecured Credentials	T1552.002: Credentials in Registry
	T1056: Input Capture	T1056.001: Keylogging

Top 5 Takeaways

#1 In October, there were **twenty-five zero-day** vulnerabilities, among them seven were celebrity vulnerabilities. One of these vulnerabilities was exploited by **Storm-0062 group.**

#2 Throughout the month, various ransomware strains including Ransom Knight, Clop, LostTrust, Phobos, BlackCat and AvosLocker actively targeting victims.

#3 There were a total of 9 active adversaries identified across multiple campaigns. Their focus was directed toward the following key industries: Government, Technology, Financial, Manufacturing, and Defence.

#4 Numerous malware families have been observed targeting victims worldwide. These include **ShellBot, DarkGate, SeroXen RAT, PowerExchange, DinodasRAT, Qakbot, Mirai Botnet, hailBot, kiraiBot, and catDDoS**.

#5 Finally, the critical zero-day vulnerability identified as **CVE-2023-44487** exploited within the HTTP/2 protocol and enables remote attackers to carry out a denial of service (DoS) attacks.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **35 significant vulnerabilities** and block the indicators related to the **9 active threat actors, 61 active malware,** and **212 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 (OCTOBER 2023)

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

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

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

Appendix

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

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information. This is also known 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
EvilProxy	Domains	lmo[.]roxylvfuco[.]com[.]au, lmo[.]bartmfil[.]com, lmo[.]triperlid[.]com, roxylvfuco[.]com[.]au, earthscigrovp[.]com[.]au, mscr.earthscigrovp[.]com[.]au, vfuco.com[.]au, catalogsumut[.]com, ivonnesart[.]com, sheridanwyolibrary[.]org
	IPv4	199.204.248[.]121, 193.239.85[.]29, 212.224.107[.]74, 206.189.190[.]128, 116.90.49[.]27, 85.187.128[.]19, 202.139.238[.]230
BunnyLoader	MD5	Dbf727e1effc3631ae634d95a0d88bf3, Bbf53c2f20ac95a3bc18ea7575f2344b, 59ac3eacd67228850d5478fd3f18df78
	IPv4	37[.]139[.]129[.]145
Ransom Knight ransomware (aka Cyclops)	SHA256	7b4d227fddcc4e93ea0cdf017026ff2dad6efd6bc7de71b689dc0595a2a4fb4d, a2c654357d790d7c4cec619de951649db31ecdb63935f38b11bb37f983ff58de, C42ad519510936f14ab46fbad53606db8132ea52a11e3fc8d111fbccc7d9ab5a
Remcos Backdoor	SHA256	34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437, 597541041b49043bd2abd482b3bf4dd233a0dbb47d5ef704ea9ee28705d2764b, 86e96d3d22ead8f41f6a29f7bfe4b35c0d4ae5bd8da046ff0d01d9c6ea678dc2

Attack Name	TYPE	VALUE
DinodasRAT	SHA1	599EA9B26581EBC7B4BDFC02E6C792B6588B751E, 8BDC8FA3E398733F50F8572D04172CD4B9765BBC, 9C660AC9E32AD853CAAA995F5FC112E281D8520A, 6022383243927CAFC74D8DC937423DBED2A170B8, B2B86DDA48A109EDD932B460649F60F505D5D71C, EFD1387BB272FFE75EC9BF5C1DD614356B6D40B5, 9343E9716933382DA172124803F5463A8454E347, C92DAC928D70EDED7D52CB1347850AA422CEA817, FFBA119D86688AFC098109E08811F67A6E5DECDA, 9A6E803A28D27462D2DF47B52E34120FB2CF814B, 33065850B30A7C797A9F1E5B219388C6991674DB, 6129E37412AFEAFEE47ECEB4C52094EE185E6768, 010451191D8556DCF65C7187BE9579E99323F74D
	IPv4	23.106.122[.]5, 23.106.122[.]46, 23.106.123[.]166, 42.119.111[.]97, 115.126.98[.]204, 118.99.6[.]202, 199.231.211[.]19
	Filenames	President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.doc.exe, client.exe, tools.exe, Client.exe, windowsupdate.exe, people.zip, lass.exe, 2.dll, 1.dll, President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.exe, 114.exe, hh.hsnx, COTED_Att. I to Sav. 230 (Draft Agenda).docx.exe
	Domains	`fta.moit.gov[.]vn, update.microsoft-settings[.]com
Qakbot	SHA256	006e0b5f47462c4d755b3f84e22b90f09fb6b369032a3ca72f39180e5395ed17, 25cc64a072861840df9dfa7b2449165e4c37d57c542da8ec4ea4fffa10f1be39, 6e0062ccdfa7a117a8b76d4056ac144fdf91f3a2811b32d5a3b7f31ac326181b
Clop Ransomware	SHA256	c73388f2ae31cab1a62b18006c634a06e34d42cdd9129efc3de2d095700810d2, ac978f6aaf36d1d90c35e6dc7ae010a19082794d3391ea0111112aed7507f708, 198d3affc04ac9e18cd6fb84f06f809a53ea7b96ad61fd622188abaa11e9328d

Attack Name	TYPE	VALUE
LostTrust Ransomware	MD5	4ae8efc6c80fe086aa27117619718fc2
	SHA1	09170b8fd03258b0deaa7b881c46180818b88381
	SHA256	25a906877af7aed44c21b4c947a34666c3480629a929a227b67b273245ee3708
Mindware	MD5	0d5bbc80bdc3bd5c148995dbd7f97f4a, 78d6ca966b7a7129c729e985a539ebb6, 760ea87bd570c2ea938dd55ae684ff37, 86fb4bc1f17511f7b5d14bde84272a58, 7883e7d9c4165e09afb25ab0c731fcb2
	SHA1	46ca0c5ad4911d125a245adb059dc0103f93019d, 9bc1972a75bb88501d92901efc9970824e6ee3f5, Ae974e5c37936ac8f25cfea0225850be61666874, E9b52a4934b4a7194bcbbe27ddc5b723113f11fe, F91d3c1c2b85727bd4d1b249cd93a30897c44caa
	SHA256	d1a0a2dc26603b2e764ee9ab90f3f55a2f11a43e402dd72f4a32a19b0ac414b5, 32c818f61944d9f44605c17ca8ba3ff4bd3b2799ed31222975b3c812f9d1126c, c306254b44d825e008babbafbe7b07e20de638045f1089f2405bf24e7ce9c0dc, 00309d22ab53011bd74f4b20e144aa00bf8bb243799a2b48f9f515971c3c5a92, 81828762ebe7ea99b672c8ac07dc3c311487a5a246db494c7643915f6c673562
SeroXen RAT	SHA256	4c6e90e178396d000b5dd5c5bb2b9ae5bbbca5986f26ffad2a6bd0845b6b2c83, 050efb70d521f74a42dcd63c703900433b03cf138fcfa1812705c8cb37deb1ea, a840fb6ea2354c5bdd1b531aa548620ed7c962a4241e4a384b03939eca8345b8, 5bcebf01c55b24ba2097f86c5074898ff8f04aca40064903d3afc2ca0593dde2, 0f0e9dfbe8a36d5a2447c1a0ae3af05779088329e7a796d17aba97fd233c3592, 9936d687086d0adfd38efa1304ad52f1007fb57027ebcfa2ca243cab7ff77ee8, 969a635bd8d14fffb3ee8767eb411e4178e4a2df8289d030d54126e3a11b409b, e7dc6a2f0c65a2c6f3d7cc2a11c3fd2acb4e23af1e55a8769366766ee22278c3, 8bf56c92865fade8d06d4a57e1d049bccd3041842b2a1c71503a29729a71073d, 075acd923103e731e91140e663756699e7379a7f63ea31487434ce04cca02b02

Attack Name	TYPE	VALUE
Sfile	MD5	ae8c22cc7542b4a3dc92cca88897048f, fdc8e99745554b1138a431c15168364d, 575934448f3a30696336644d6c379db9, 0493958b9915e5799927716aa5b82191, 1875e9d8031876674d4d236ffab6b826, 4f44f3a05d014ee1a4e85f67436abcb9, 38ca7e711977058ae3ae702b2ea676b0, c83874d9e1f6531a05c61d40ebe9b82a, a1e880b1bf079e1c9ac9a9238c68e674
	SHA1	0f20e5ccdbbed4cc3668577286ca66039c410f95, 14e4557ea8d69d289c2432066d860b60a6698548, 28f73b38ace67b48e525d165e7a16f3b51cec0c0, 5ffac9dff916d69cd66e91ec6228d8d92c5e6b37, 665572b84702c4c77f59868c5fe4d0b621f2e62a, 6960beedbf4c927b75747ba08fe4e2fa418d4d9b, 8c507d26c2fec90707320ffb721ae626139bbf11, a67686b5ce1d970a7920b47097d20dee927f0a4d, bdb0c0282b303843e971fbcd6d2888d834da204c
	SHA256	e82606b7c179cd39d0e68d9f61723c4b2c909c44e2630c69d7038cd0f1bcb595, 451c4ff0a4313c98b519179eb276914d18d01eb1d6b1a28d6af15fda1693ec34, 8396728b5267a9ff823db2ab600e3ef1d131fc36596d24747ac494e8cdfe877c, 26b7c7079cfea22cd9335b788db32453a727c81aec313a3637391a9763434f0a, 92c24d0c2075133e91f1be803c00478c733ee5be5610564efc48dd160cf2c632, 97d679f364b1d0c6e3896574f1338801a0d707c137e4d220d2c974ae40fbe708, 7195995c6ea6afc08bdfa51f7227ee3398aec95f242e992c900f14eb644dd838, feddee093d72838ac1f13ea9bbfc0473e2f3df1495432d6f95d6fe8ddf7ff09b, 4576fd0e13e13c9d490bd84ff83d2f3b602272cdea5f6c54c74f75d067ac5505
MetaEncryptor	MD5	e471f1f13de4cd91e3d4139c98c045d4
	SHA1	e04760f670fab000c5ff01da39d4f4994011e581
	SHA256	40ec6eb75af3bf1c8406a121cbdeb4145c70f71e0523c1ffcc12265805d5441b

Attack Name	TYPE	VALUE
HyperBro	MD5	af43e0c21ddf7e4e087cdab2ac8d2948, 7d75561cb378e54c5711f077858a4a48, 4109ac08bdc8591c7b46348eb1bca85d, b35c698732f49f998f6e6b6b83cfa9dd, b5cb7044a189f8752ecdbc799f25ce06
	SHA1	b8d9bba99d9777c43b96f338f5bc3a08201fa05c, 692b407893846cdd5d3e75110402fe1e7bf5515e, 6423d1c324522bfd2b65108b554847ac4ab02479, 13e334a4857b8bee0283e5e193fa7983d5c0ee06, 9e08fdd7eaeffbbf6e441060e02dc29b0f66b118
	SHA256	12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df, 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b, df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348, 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5, df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9
	URL	http://38[.]54[.]119[.]239:443/jquery-3.3.1.min.js ,
ChargeWeapon	MD5	44ee43adc8f423db4a461fc99731cdb9
	SHA1	0fd8c9ed43d66022a08cc8ed7e78c4a6216cf26c
	SHA256	3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135
	IPv4	45[.]77[.]37[.]145:8443
Cobalt Strike	SHA256	0e9f26b9a92ba13916a6e98de924397ec3adc68507a1447a0472d1b4e4d8b2df, 923bb69535e27f3493f6253abd93a1c0a9bd08bcf18dbc27d4d8d381a9220bed, 46725598f6c781f6fd178d6f1bce8c93bb21a6a27d6daebc9ff57878a1a301ad, 092188d15ff480ad9ca89f2c65984d8e3d1e7c1e7a8aa91fbd5ceb02461071b8, dc1a58694467305a98f62b7d4b6b6945398e43f0f982a0e13c2a8982ef8bb84a, 69458febe1c88d03d6b5f0a83b516481f9dcbedfb97c8720170e4d0c75c1c880, 7fa4e361cf073d65ccbc49dc937a622965977ef995a0c199a4b4aa5fddd57d17
Mirai	SHA256	c6e55d1c5e4fbf79337819efa366433840bc743e8830454b06cac72723bf1687, 3dd1607d6c78a16784049978459e4a07cd1188c5419af699724b2b99c0187822, 40dcf03076a4e4114d628dcb7931d7d766b0ef0a17210e97bc6cae70089db080,

Attack Name	TYPE	VALUE
Mirai	SHA256	2a63ebb23958cac89eb7404fb328774031f875ac563affdf5c67abe4d2d78a4d, 516967063c380a26e75ff2b0f529913366b492efa236a8f641686bfb17443cb0
hailBot	IPv4	34.147.16[.]24, 34.165.70[.]211, 34.176.112[.]249, 34.64.52[.]239, 34.69.75[.]60, 34.92.28[.]223, 35.188.240[.]127, 5.181.80[.]115, 5.181.80[.]120, 5.181.80[.]70, 5.181.80[.]71
	MD5	f30a468b56c5761e346f3e709fd098e
kiraiBot	MD5	33ea03c6fdb4bcd826f99ca7ae8b5907
	SHA1	5e0f04554264dfc3eb0ed6a22a53ff8ae26a4162
	SHA256	d619cefad993a0df9ad0ddb631159c50995f76dfd0f14b3fb334b04fce8095cd
	IPv4	179.43.155[.]231
catDDoS	MD5	12fe77575c11b698501e2068810823a4
	SHA1	3a3f37333e298c3c6f2be18da4f5473454820d2d
	SHA256	259b0c0c65f6836cc2ee8aa22da007415404231e178aabfbb4bfc11c7786f441
	IPv4	139.177.197[.]168, 212.118.43[.]167, 77.105.138[.]202, 84.54.47[.]93, 88.218.62[.]22, 88.218.62[.]221
Lu0Bot	MD5	6181206d06ce28c1bcdb887e547193fe
	SHA1	8eb65b4895a90d343f23f9228e0d53af62de3dab
	SHA256	169b23f45787a0213143bdbb4125658b4bee18e74cb9899c09c29233807bcd21, 4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799, e6bf861332a771e037a76546d095dd752db63ba0e9fec254a69e0864ae248921, 31fa43d98ac742905cf04735033e154fd103bc67c255cec63a7448ad138df0cf, ca09a22afb6d9a1853fe4fc4d36089900d24d7178642ec7ca86789cd0dbc5c67, 8ee274b430932f7e8068229a7f32c2bbaead31bf6c18dd13194a1126f5cbfb33, 3a1f00f2d35eb2fbab05c0543eaf32d29b12b856c64809393c873474a4a27083, 95fad71ca5df4eb7e390f6795d4a02d117524e9432d118a5213a484e211e1480, 7b4055eb9d72b5e5cd10c846497cb538bc366f8993198b680d195c98987d74e6, e2c630adb97cc041c5ce1835add03841493ae95223d43c9e415e26e6c4c418e2, fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428, f4b15f591e0138a46f1f5fd157f31a78b360624d72a18136a5269a05ba8b987c, 22b643071879895cd947cf37c75c71b23af5fe4228f36b49571b1a47df137d06, 28eb3941dee1a78351ee18596be6445d4fb10332d002f85aee675f672cf2fd1c, ea596ff0c0802b85cc304447799c91907ae1016283152ba5ba5dc4cb50ca8712, 9837727bf67f4a49655b5f2230fa7dad235b025c9af377e559df6fab0f4ff36a, a4a0e26bb4aa352f66952902cc9704d130593adacb46017c0b2a1be2b7a9269d, 863c612734f5ff0ff0ea3fed7fd790dfb43c47eecdc1417bcd82c0ad866419af, 9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa, f17694550f57c6605f37588e37f55898bbc969c1f24b18f0be8ce416c95ab91c, 0296a426d47abf467c431db1e126b8763eac7d062e731193eccd15a51c52da7c, 149ca091b02aafdeff15610c639b442a61e0dfcd461d9bec7f8c38998a390575, 6f7ab51e9f0d382c650743cb3c06b42708cd06d64170a458864e89ad6480a237, fd746c51486e5ccb2bd801f4cffbeefaf77e7844ef1dd5d211a4c183ec26f52d, cb96ceb0b26fc150baaa7fe1cc2a65af42c7db902f54839578b3235a7d12d25c, bfc050b80ad15c6bf86ea0dce49089c56ed9ffccf5dae2b8e3b78b59dd36e0bb,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	956610a72b5e5aaf220b861aec44e08dda7b6a97ccae3d2fea0181e3a6b37228, 09a2d8ab4c255b6f78ca7534e3105014a21613cd3c6b07cbb92eb2c82b553483, 24c0997ec70f23963598b59df453f28ffcc1e8b356898d5ddc4b2cbf06f6f2ac, 0718b209bd95315b8347d3f006b7da387f9807153ebe8b2788285296e19b5973, 0739718c03bd39daad459142116b886d6138cfe887d30b02942e01b9d238dd13, b13633b31e8704b63d977921d1c9a4284bfd4780c3f35a5bee372816d7beb005, 242467ea19694c0e6cd76dcff901f5af6a309c2c999971b1dc4cd9bad253ea19, f5f8716486cab2d9b866a1e19e4f25d64d070262ce32d2ff79db283ac7fd1b05, 0bdaa27e390c5e15c3b27ae4f4168fbf97693f5d03fa0f70487c63c13030ffd8, 5920894ae997b61f27b53c9f6e598df5f928acb11a5dc09f4fa0627747f1312d, 6d265ec945dfd70f60e5a016ec26276f3d460076e9320a3c11c7a76b638da9ab, 5a2283a997ab6a9680b69f9318315df3c9e634b3c4dd4a46f8bc5df35fc81284, 742eb714457c3646f7f5dee44aaf0d57d5fa076ee294de6755818132402b06f5, 70657b04b2da77f8019be49fa3043898874bebb385317a6c91246f9e3858bf16, 858bafe27080124fc1560894b00cf8c0c672df0bd0a66dbd08cf28b4cf9e1ee5, 7374cce760bf018df8c602b12e475a66114747d96848168cb939f27afafb29e0, d5069d544f3ff1efe1851688b9625cd44fe45c6f1a9792b30f5f28c74af1d6d6, 5de7148d727fec09a0597b5f64cf1719968372a21c6ded90c51cae3f42b4c26d, 0f2c35b80a36f70ab923b56c495ea6fe9ebdd48b3d5a4ff404fec3b99ff010d9, d189c35ecd1b9665741e7e08f9d9029c307e07870cf57832426d8bfce1c48fa6, 8264e723a411381a9d837458ec39cbb36c8d582bcba14f7ed7fc45f8154c479d, 4547dab867404fa6e5cebc5794ae58c4d365355372d26e6bcd01c1aea0f91e1b, 45964a7afb9d41eb319161c26215c5bea0334b388ecfb1520b83bb2d6984ad5e, 02e4898e0a4cc85c406996e5e60274082746eb45d77a18a24eb545074a56ab3c,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	f186c2ac1ba8c2b9ab9b99c61ad3c831a6676728948ba6a7ab8345121baeaa92, 5a2264e42206d968cbcfff583853a0e0d4250f078a5e59b77b8def16a6902e3f, c88e27f257faa0a092652e42ac433892c445fc25dd445f3c25a4354283f6cdbf, 2d721df670fdb63c643b3de2dcdd46311b8d94d2753b47ad0035392644dee77a, 4c31eccb460bef397e6100e1ecd85c3a2b823b893a9a9add4bb83fde8f9b122b, 0297bbb0f00b3f591894ebcf042f2c6b0ed52e6662def1a9dbca0f8d20133cee, cb23aeac6382ff99608a71e3b416c1ca22f5f301474840239e4c319db31cef25, 9db5c02ac4e161369160fe13719a212e55377dd57ffc9f98b7141bce3b9df26c, 4c99457625e752a03693aab64e2b5129eff89872c649194e81bd87809ed1ae13, 22934e006b3f1b8225c51a93ce0acaa1874c4f1dc895fa1664bdf16b0065d2e7, 7c37b8dd32365d41856692584f4c8e943610cda04c16fe06b47ed2d1e5c6415e, 418a860f2f7f5d415ffa2c7b2662c6fde7c35e2bdafd45e378bdf7c95579fde8, fce3d69b9c65945dcfbb74155f2186626f2ab404e38117f2222762361d7af6e2
CurLu	SHA256	6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746, 78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd, 4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6, da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9, 93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347, 12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc, 4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d, a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9, 7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e

Attack Name	TYPE	VALUE
CurKeep	SHA256	295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719, 462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a, 437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a, 482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651, 877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697, a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172, 36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652, caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1, d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30, 1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6, d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4, 2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782, 1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a
CurLog	SHA256	409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c, c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac, c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0, 2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed, 778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e
ShellBot	IPv4	123[.]6[.]5[.]229, 124[.]222[.]211[.]66, 135[.]125[.]240[.]201, 175[.]178[.]157[.]198, 31[.]145[.]142[.]206, 39[.]107[.]61[.]230, 39[.]165[.]53[.]17, 61[.]242[.]178[.]220, 94[.]250[.]254[.]43
	MD5	7bc4c22b0f34ef28b69d83a23a6c88c5, 8853bb0aef4a3dfe69b7393ac19ddf7f, a92559ddace1f9fa159232c1d72096b2

Attack Name	TYPE	VALUE
ShellBot	SHA1	5daf348ae3ca2c13ff7983c5771e9436ca540695, 620a4ef784f6bbc8c9fd08c7590b691de546049f, a10262346ce669b28914570415a223ec09c234c8
	SHA256	8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a, 9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97, c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140
DarkGate	SHA1	4ed69ed4282f5641b5425a9fca4374a17aecb160, 549cb39cea44cf8ca7d781cd4588e9258bdff2a1, e108fe723265d885a51e9b6125d151b32e23a949, a85664a8b304904e7cd1c407d012d3575eeb2354, 924b60bd15df000296fc2b9f179df9635ae5bfed, cec7429d24c306ba5ae8344be831770dfe680da4, d9a2ae9f5cffba0d969ef8edbbf59dc50586df00, 381bf78b64fcdf4e21e6e927edd924ba01fdf03d, 4c24d0fc57633d2befaac9ac5706cbc163df747c, 9253eed158079b5323d6f030e925d35d47756c10, 0e7b5d0797c369dd1185612f92991f41b1a7bfa2, 7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc, e47086abe1346c40f58d58343367fd72165ddecd, 42fe509513cd0c026559d3daf491a99914fcc45b, 93cb5837a145d688982b95fab297ebdb9f3016bc, f7b9569a536514e70b6640d74268121162326065, d40c7afee0dd9877bbe894bc9f357b50e002b7e2, 1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc, 3229a36f803346c513dbb5d6fe911d4cb2f4dab1, 6585e15d53501c7f713010a0621b99e9097064ff, 001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2, ad1667eaf03d3989e5044faa83f6bb95a023e269, a3516b2bb5c60b23b4b41f64e32d57b5b4c33574, e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f, 3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1, f3a740ea4e04d970c37d82617f05b0f209f72789, e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10, 45a89d03016695ad87304a0dfd04648e8dfeac8f
	Domains	msteamseyeappstore[.]com, Drkgatevservicceoffice[.]net, reactervnamnat[.]com, coocooncookiedpo[.]com, wmnwserviceadsmark[.]com, onlysportsfitnessam[.]com, marketisportsstumi[.]win
	IPv4:Port	5.188.87[.]58[:]2351
	URl	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin

Attack Name	TYPE	VALUE
Balada Injector	IPv4	2.59.222.113, 2.59.222.119, 2.59.222.121, 2.59.222.122, 2.59.222.158, 185.39.206.158, 185.39.206.159, 185.39.206.160, 185.39.206.161, 80.66.79.252, 80.66.79.253, 88.151.192.253, 88.151.192.254, 89.23.103.32, 89.23.103.246
	Domains	decentralappps[.]com, statisticscripts[.]com, dataofpages[.]com, listwithstats[.]com, promsmotion[.]com, stablelightway[.]com, specialtaskevents[.]com, getmygateway[.]com, stratosbody[.]com, specialnewspaper[.]com
AvosLocker ransomware	MD5	5cb3f10db11e1795c49ec6273c52b5f1, 122ea6581a36f14ab5ab65475370107e, c82d7be7afdc9f3a0e474f019fb7b0f7, 825d6049ba8600ee5fefd817ac5444b4
	Email Address	keishagrey994@outlook[.]com
	Virtual Currency Wallets	a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee, bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92, 418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd, bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn
	Tor Address	hxxp[:]//avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad[.]onion, hxxp[:]//avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad[.]onion

Attack Name	TYPE	VALUE
AvosLocker ransomware	SHA256	6cc510a772d7718c95216eb56a84a96201241b264755f28875e685f06e95e1a2, 1198fb9117776809b11a19000161377384957bee846f7b25a610fc8ca082eb37, 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81, bff12a83b1fc2e0ad0000ad9b68abc8eada559bb1094caaf5b9f52887df23705, 91ecad5a2010a6d8b6b738a88a1e3db30bd0e4fbc647cd49ecadebdf0a357643, fe23d4b7a9db3c937523afecdbe14969987c27f35b9bb9c90f656bcd897bcb87, df480deb191b335dcbc3d4fc5d59594cb38caee2aaef8d877fbbc573de741301, 01792043e07a0db52664c5878b253531b293754dc6fd6a8426899c1a66ddd61f, e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721, c0a42741eef72991d9d0ee8b6c0531fc19151457a8b59bdcf7b6373d1fe56e02, 29910ea42c8e2abb22d5a88053e1725c93a104e61560a2f8d88716d619bcaa08, 27cd3e759ec4858adaea63050ad1fc22e4850c1e157d88c0943c2589fa39b5a4, 373a791f058539d72983e38ebe68e98132fcf996d04e9a181145f22a96689386, bd88d415032eb24091c352fc0732b31116f44a78d9333037bd7608289608d3cd, e62c0bdf69b88a5bd95872cbcf4da4de4eef226bc9ef0452ee652eeee519b15a, fb544e1f74ce02937c3a3657be8d125d5953996115f65697b7d39e237020706f, 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856, 10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4, 7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1, 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6, a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749, e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f, ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7, 48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731, 1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff,

Attack Name	TYPE	VALUE
AvosLocker ransomware	SHA256	05ba2df0033e3cd5b987d66b6de545df439d338a20165c0ba96cde8a74e463e5 7731a9e1e5fff9d912b1d238dcd92c2ba671a5ea55441bb7f14b05ed40039ce1 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81 a58864dd006f0528f890c9e000e660f65ffe041ebd2bcb45903fb0228321cfb2 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856 a5ad3355f55e1a15baefea83ce81d038531af516f47716018b1dedf04f081f15 05ba2df0033e3cd5b987d66b6de545df439d338a20165c0ba96cde8a74e463e5 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 e81a8f8ad804c4d83869d7806a303ff04f31cce376c5df8aada2e9db2c1eeb98 ddcb0e99f27e79d3536a15e0d51f7f33c38b2ae48677570f36f5e92863db5a96 14f0c4ce32821a7d25ea5e016ea26067d6615e3336c3baa854ea37a290a462a8
	SHA1	9c8f5c136590a08a3103ba3e988073cfd5779519, 05c63ce49129f768d31c4bdb62ef5fb53eb41b54, dab33aaf01322e88f79ffddcbc95d1ad9ad97374, 6f110f251860a7f6757853181417e19c28841eb4, 67f0c8d81aefcfc5943b31d695972194ac15e9f2, 2d1ce0231cf8ff967c36bbfc931f3807ddba765c, 2f3273e5b6739b844fe33f7310476afb971956dd
	MD5	f659d1d15d2e0f3bd87379f8e88c6b42, e09183041930f37a38d0a776a63aa673, 31f8eedc2d82f69ccc726e012416ce33, d3cafcd46dea26c39dec17ca132e5138, 504bd1695de326bc533fde29b8a69319, eb45ff7ea2ccdcceb2e7e14f9cc01397, 829f2233a1cd77e9ec7de98596cd8165, 6ebd7d7473f0ace3f52c483389cab93f, 10ef090d2f4c8001faadb0a833d60089, 8227af68552198a2d42de51cded2ce60, 9d0b3796d1d174080cdfdbd4064bea3a, af31b5a572b3208f81dbf42f6c143f99, 1892bd45671f17e9f7f63d3ed15e348e, cc68eaf36cb90c08308ad0ca3abc17c1, 646dc0b7335cffb671ae3dfd1ebefe47, 609a925fd253e82c80262bad31637f19, c6a667619fff6cf44f447868d8edd681, 3222c60b10e5a7c3158fd1cb3f513640, 90ce10d9aca909a8d2524bc265ef2fa4, 44a3561fb9e877a2841de36a3698abc0

Attack Name	TYPE	VALUE
PEAPOD	Domains	budgetnews[.]org, wirelessvezion[.]com, redditanalytics[.]pm, netstaticsinformation[.]com
	URL	hXXps://onedrive[.]live[.]com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317
	SHA256	83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c
	File Name	pcmf-installer-23.0.5.exe
XorDDoS	SHA256	b8c4d68755d09e9ad47e0fa14737b3d2d5ad1246de5ef1b3c794b1339d8fe9f8, 265a38c6dee58f912ff82a4e7ce3a32b2a3216bffd8c971a7414432c5f66ef11, 1e823ae1e8d2689f1090b09dc15dc1953fa0d3f703aec682214750b9ef8795f1, 989a371948b2c50b1d45dac9b3375cbbf832623b30e41d2e04d13d2bcf76e56b, 20f202d4a42096588c6a498ddb1e92f5b7531cb108fca45498ac7cd9d46b6448, 9c5fc75a453276dcd479601d13593420fc53c80ad6bd911aaeb57d8da693da43, ce0268e14b9095e186d5d4fe0b3d7ced0c1cc5bd9c4823b3dfa89853ba83c94f, aeb29dc28699b899a89c990eab32c7697679f764f9f33de7d2e2dc28ea8300f5
BlackCat	SHA256	b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2, e69a13add1245bc1b7b6337e64eee9b53395b9574f2b85d32f891680c7165ff5, aa236a7ae9949fa1bc6111e6613f2a2e05f33b95c28d19c1f0fd5417736ecbe0, 3a7866a23339baf6997fe08d7e7dac97d3f8754af552acee3457c3604abaf4c5, f5f645ae6dfa3f957412eb44a5d251e93b37678862baf16b08dc8e142da6f998, 53c62e81c89160f56647bc526e11923842187f557ae42669cc0cfa9f7f1e7203, 841424257c677da6b679f6ce45ee141d05b99deb4a694d0480549b747c1ec6b4, 841424257c677da6b679f6ce45ee141d05b99deb4a694d0480549b747c1ec6b4, d7657ff830673017fb420bc90249c4f1ecbaa778e032a3b203b10d8866741bd4, 3a7866a23339baf6997fe08d7e7dac97d3f8754af552acee3457c3604abaf4c5

Attack Name	TYPE	VALUE
Volgmer	Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-5903-ed41-902f-e93a29dafef5"
	MD5	35f9cfe5110471a82e330d904c97466a, 5dd1ccc8fb2a5615bf5656721339efed, 9a5fa5c5f3915b2297a1c379be9979f0, a545f548b09fdf61405f5cc07e4a7fa1, eb9db98914207815d763e2e5cfbe96b9, fe32303e69b201f9934248cc06b32ef8, 64965a88e819fb93dbabafc4e3ad7b6c, 6da7d8aec65436e1350f1c0dfc4016b7, e3d03829cbec1a8cca56c6ae730ba9a8, 0171c4a0a53188fe6f9c3dfcc5722be6, 17eacf4b4ae2ca4b07672dcc12e4d66d, 1e2acecce7b5e9045b07d65e9e8afe1f, 226cc1f17c4625837b37b5976acbd68e, 3e6119ebfacd1d88acbd2ca460c70b49, 4753679cef5162000233d69330208420, 5473fa2c5823fbab2b94e8d5c44bc7b4, 570a4253ae80ee8c2b6b23386e273f3a, 5c87373eef090bed525b80aef398ee8a, 693afaedf740492df2a09dfcc08a3dff, 6e21cc6669ada41e48b369b64ec5f37b, 72756e6ebb8274d9352d8d1e7e505906, 8b3ec4b9c7ad20af418e89ca6066a3ad, 947124467bd04b7624d9b31e02b5ee7f, 9a87f19609f28d7f7d76f9759864bd08, b1225fa644eebafba07f0f5e404bd4fd, cf2ff5b59c638a06d8b81159b9a435ea, d52b5d8c20964333f79ff1bce3385d0b, e273803ae6724a714b970dd86ca1acd0, ea5d322648ff108b1c9cbdd1ef4a5959
Scout	Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-2790-10f2-dd2a-d92f482d094f”
	MD5	05bb1d8b7e62f4305d97042f07c64679, 0b78347acf76d4bb66212bf9a41b9fb9, 0ed86587124f08325cd8f3d3d2556292, 35943aa640e122fcb127b2bfd6e29816, 394b05394ebb9b239a063a6b5839edb9, 5496adcd712d4378950ba62ad4c2423b, 64cac69ab1e9108e0035f9ce38b47db7, 695e5b8dc9615ec603fe2cbb7326a50f, c07e04d388fb394ac190aace51c03c33, c41eb1ea59fab31147c5b107cc1c5a51, cc5a8a15d5808002e62d5daf2d4f31b3, 0b746394c9d23654577f4c0f2a39a543, 225cdc9b452b6d5a3f7616dcc9333d7d, 43f218d3a4b2199468b00a0b43f51c79, 4b1f1db4f169ca6b57015b313d665045,

Attack Name	TYPE	VALUE
Scout	MD5	80d34f9ca10b0e8b49c02139e4615b7a, 855e26d530e69ddc77bb19561fb19d90, 9ec3a4257564658f651896abc608680e, a76624578ed42cceba81c76660977562, b517e7ad07d1182feb4b8f61549ff233, fa868a38ceeb46ee9cf8bd441a67ae27, 1f1a3fe0a31bd0b17bc63967de0ccc29, fa3e49c877a95f37fd25dbd62f9e274c, 202a7eec39951e1c0b1c9d0a2e24a4c4, b457e8e9d92a1b31a4e2197037711783, 8543667917a318001d0e331aeae3fb9b, c16a6178a4910c6f3263a01929f306b9, 1c89fb4aee20020bfd75713264df97cd, 76f02ab112b8e077544d0c0a6e0c428a, 7ba37d662f19bef27c3da2fd2cee0e3a, 7f0e773397808b4328ad11d6948a683f, bf5d815597018fe7f3dfb52d4f7e1f65
BbyStealer	MD5	2cf6efb8104b5d4606fb1698ae97e4f5, 3cf9c1d65d59b63d479ec26e9fd98b57, f1da9126a48197897644a62135c0df46, 352ba438532e9a7a9941875f3824c1cd, 71e0b2a2372398776297cee13c8efa55, bbc3364d8040296b910cf61280cd6ad7, 0d2071be3f76d4b25f19b54d56ff6cb7, 1f8eda53714be873e2280d494c9eacbf, bcd419817ebb4d2ec7e21fbdaf61dd3b, 4ee5a9ffd40f8c0970e53e832bfb9acd
	SHA1	effb88250fcb89bbab77f46c1022f3c9c0aad37e, eab9cf1e969b5d9a3fda7714c6ae2796aaf44fd0, 8fcbf76cccb573d3007032a2148da458f81ffbb1, d72c3e3b1fdaa271629676d7d0215cc396a106c4, c9fd398ed07a2daeeaf526ab094634adbd851934, bdd5dec13109f9cfe992ce325f746c0d3bad6c72, 8a7fab41932aa2dbe8da17697926d69b15dc6c63, aae16faf79be993b27791fb7a6a3663320067876, 61fd361edcfaecb87dbf3711ecb1dd448d6a2ab2, 0ee35e1992b93dbeb7adcd2ccdfcafcb3a1dfdae
	SHA256	55a6a784d4acb7e9761a99fb38eb441519cdcd2943bfdf1a1558fe8513690c97, e97b03c98056d7c88bad83b7422767d51ac75fe959e7d1582cc645d6a2bae84b, 7a27aca062c7b4b180190452afbc6ba4026a13ca8c9503372459a5b214b68ff9, 50ab07bd922546f90d2d62565a3618ba7251459c8aaf007945feb3e7c9f29458, f46017c2c5c98d89a1d35510ed8eeae263a3f8f60092df2bb13db6918d691a32, 833ba04dfe7c93f397117690bf656bdf1cf2768b216f40f525bb0c7527897b9a,

Attack Name	TYPE	VALUE
BbyStealer	SHA256	8b93ed446668642a0d3b8dc45b794d76ce71ebd7552de8437975da2b228df9c7, a26a2a95b6ad1449bf4fe5814533b408cdcc67ad5c234c900b6e0b31300018b0, ae4ea904741b95f044edf0e16ce244dc5a4015050dd9ecf23f2f831435e1ccbc, 058caf0c1750391e8a625ee3310c804e1a0034ce890aef4773ef6cfff3ccCed5
SmokeLoader	SHA256	184f4f60f0d0438a975309e33078ec976111425f890d43799f09c0b492962d9c, 2f1e77b4703bbe3131c73b9904653f1175b6f6ec485bcdd1e517173df807d46f, 5f2256cb5470ffc8c81545b7ad9ba361adbe8b7883249412ca2ee38a1acf34aa, 0602c6de331d5133a1213be5ac970898f74d8630a7ff273eda97b1cee73a08bc, c75011e37825e51e7d884caa4c01e43e0b3fc76d31b92624d83f64aebfbab134, cdbdd07a270d1d907798fabe6c680b677f98f119cd93987de5b6a2db7597d5b4, 2769d9ba9625f530819789fd7750ede220f53e3e5c8612a7994abd124e93966b, 0145682b82083b4c90ab5adc2e31ace000d27c89ebf867f1bab5538ecb0e847c, 30a492bdeae90d129df25f025dcd1e014a371461d35be9239673e36a2d7e1718, aa8fd2c68d244547148a554400661572879c9a9916a6651f27bd703fae2a2cc8
Nanocore	SHA256	3326240e9bddfc66fc85528944900d2afa9be59837f8e80537f3dd4cb105ec40, 85ba99319f22cde0abd25e839a7a230a730f1d52e546754873e479be88e65da1, 4eaf86877e9160a7bcb9105039f90acefec1ad130979335ff093344fed31ca22, 8b44d972bbe20975a47391ee41e7a6179a00510c6a023eadfe06fe2bd965e860, fd3b84b15d3079c8dfa2e386de838bf9406841f2eec7454ba642497f3bd524f5, f72da1620877b354290e9152bd9389fa8e8ea18d292a06e93d82641987a3e678, 9b56deee6d3d191f4cb38a3771bf1d818baed58ab18dd968341f2016a8a5cf50, 73142b5f2ad334785424e3c6f8ca97b3796b9a0d6c8c13c52866f988b6f9650d, 93e080fc54f12414da2606f38855227f8e90bb50345a3bbd082395ee359bfc4d, d77804f10b391fb2dc77a749ab27cbf71e2effc0a149888f4962112f1ad61575

Attack Name	TYPE	VALUE
Crimson	SHA256	3198fb63145c3a354d7915a4bd1e41cb8d45396f85d179393cf744817f82196a, e38c39e302de158d22e8d0ba9cd6cc9368817bc611418a5777d00b90a9341404, ce556d55e07bf6b57e3e086e57e9c52552ac7f00adf4a7c9f99bbc21a5ac26c2, a833dbdc5c2113da51bf778351834682bc6220461394050e04592cd9096e0aba, 2110af4e9c7a4f7a39948cdd696fcd8b4cdbb7a6a5bf5c5a277b779cc1bf8577, e38c39e302de158d22e8d0ba9cd6cc9368817bc611418a5777d00b90a9341404, 2110af4e9c7a4f7a39948cdd696fcd8b4cdbb7a6a5bf5c5a277b779cc1bf8577, a833dbdc5c2113da51bf778351834682bc6220461394050e04592cd9096e0aba, ce556d55e07bf6b57e3e086e57e9c52552ac7f00adf4a7c9f99bbc21a5ac26c2, 7df319a67e11d9b5196f9da64e8413f8448c6f2f1319be4f48dfbb3a045ed645
AgentTesla	SHA256	b2733739ec7e122deeed490926f1e9b50a3ac83ce3d87dd407fc3983cc1b35e4, c6e890fe05afe481cb4d8d4460424276a29566a9d15e145f13413b0d1a158d8d, 4ab7caf841130dd3052e383e4bcf300a79d284bd0f35c777ca25c823c97f5ea5, c34e81fe62af4f81b2bf0d42095b27a0e70db3dc28d0399e1c3477ad9bdf6764, c4ab03eb1096d5643db922730824168efa45ba7f308c3336c47558360fa8b44b, c7728266367cb088e58dd7c5207e86c2c00a36a45e7267732bb5322af0fc82b2, ca399dc8b5bd33a6536454774e350400d0693b4ceef2738d06b8cb73a9e262e6, cabf5777651e17c1d64384cefbf5f7ce2fc7abedff68901c96174dd16612caf1, cbd2e33daf09934c60b689bb54205a2072ae6ae9f748eec21f3508a5cbfb532b, ce2bdcc4087d372411c30e4d003a90c7794accf14004a5200fab1948b0c94659
Rhadamanthys	SHA256	ebad5799999c845b30f52f65cdf7ca9da64b5406d875770b854eeffcbcc42253, 0a2c9d63381141a3d3ba914626f5e08f027e644dff07009582e7ef85aaf4928a, 2cf0c41523a67a1112db28e85d7694ebf02b0e94b4b3e684e82b299d2d448a75,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	c77a99aebc91775a48fcbc85c0b062bb0338818860facc160cd005a3ed5801e9, 62600a3d570dd2096f9eb8bb18b7d4b4844e9c603182529dadad8831f8a067a7, 74a434ab27dee2234cc149fa8d34c6d5af5beaa0060ffad7523fde8ec923f983, 8ba72f675acf5bc12805d4fff0bda437ea419d15e4237c916554a7f7df1b0b36, b45536b641815e8e230c3519ee7b9dcb4bf186ed2f4dc73b4be00066550731aa, b76d7c7450892b61891be2cbcfdb364e7b6f3c39a30ea1a3727d57b5683cd237, c46f2fcce113e720cfd68123663b96ea24203591c40caafa70cb518fa9e31fac
xRAT	SHA256	b1e9a85c03068ca865cd3b4951c83e43548acf7daf137e59b0ba92b6050170bb, 14d25750cb84c1c8d0fba9797ede0e3589e661ea8aeb5e357aa6c9c69cbb3b73, 69205ea8da1443cee48059eebe27c4046bcb7efac024b2d26b618544cb6d4996, b60a6257b257b668dbe48686e6ec953a4ecc13158702a8cfb37043101da105e8, d2b3682c2a7a847400cb42f338d41b054d5f0ccd63e9338903a6a11c67cfe62d, 37b810b19d1cd5c18e78d0b2e24a58e79a023ad95350d4fcfef53364ab61cda2, 5aca307743008434d993c21b5291ae0fbbcba0b31f91276010dc7f184fe234d7, 06d532b874eb678faa3b9d14cd9b2a10c401a241e05e2c1aea6947ae31857b79, bfdf4add1fdb2daf0c4a3f5102130461f437347a2221a7370e17e157ba895ede, 3c5d54bafaa699f1aa27dfa437569ab284051ab8947dde26bd9743da9139f011
BabyShark	MD5	ad9a3e893abdac7549a7d66ca32142e8, 116a71365b83cc38211ccfc8059b363e, c8d589ac5c872b12e502ec1fc2fee0c7, 0d6717c3fa713c5f5f5cb0539b94b84f
	URLs	hxxps://onessearth[.]online/up/upload_dotm.php, hxxps://powsecme[.]co/up/upload_dotm.php
RevClient	MD5	be2f73a637258aa872bdf548daf55336, 02804d632675b2a3711e19ef217a2877
	IPv4:PORT	5.61.59[.]53:2086

Attack Name	TYPE	VALUE
TinyNuke	SHA256	db2027cd8687abdce3e6df39420b34494788301b9c5d892c470e975e67c65d09, 08b0b9fff5f719e1ff863c0ff2505122b4ee7e075956199ecc7b59769f719abe, 29e7bed50c7a5738ce2e69b48e94d532133491d9a99b613dc962e270cae61049, a74e7edcc211be78093e8516f8013db6f2f0c7e950cc680c2c50ab8f3f71ec8d, 5ea23633beb89010185047a47f84fa500278ba442f408f3901946ac6c5fb4cee, c59a7541b0c51a0bc912971f1fc729240c5d27398eef580484b956818cde06e2, 47b5e55165a20b834e42bbd13c304ae73107e65bb902798cfa2de61ce75fc1cb, 795d99db27ef00d4e8c53bb1e97aeb6f7bcb0693b1e0fd5eb4d700847011b3b9, fdea22e1aebe4daa925455dd4015518fe681562c350a994720be7abe606cd444, 81b308fe77fc1b3539e6b859f2aadbe6f7944964cea8ed0e63f54505fa5eeabd
ForestTiger	File Path	C:\ProgramData\Forest64.exe, C:\ProgramData\4800-84DC-063A6A41C5C
	SHA256	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795, 0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa
	URLs	hxxp://www.bandarpowder[.]com/public/assets/img/user64.png, hxxps://www.bandarpowder[.]com/public/assets/img/user64.png, hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/user64.png
FeedLoad	File Path	C:\ProgramData\Version.dll, C:\ProgramData\readme.md
	SHA256	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486, fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6
	URLs	hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feed.zip, hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feedmd.zip

Attack Name	TYPE	VALUE
HazyLoad	File Path	C:\Windows\Temp\temp.exe, C:\Windows\ADFS\bg\inetmgr.exe
	URLs	hxxp://147.78.149[.]201:9090/imgr.ico, hxxp://162.19.71[.]175:7443/bottom.gif
	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
Phobos	SHA256	d0604a3864899ac9bf0a07e47330b62a3e76b61335d6dac2e9b5a796b9fcc164, 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c, fd59543a425d2159dfadba8efd4d40178b609ef123a8bc5cf00fe3afef95623d, 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52, 2a50a42d3c44e6e3890a53228cb84f6fdb17e38b31422c68b8634a06d36cc324, 78732997a6c9d975b97da85fc511533d44083a9f9da60dae8393274a59b7bfce, 8f60d17bbaefd66fe94d34ea3262a1e94b0f8f0702c437d19d3e292c72f1cedc, 698b2a9cf9ce16f1cb5cff4576e902888cb14db7414b8e6ac4eb728f8c87d209, aedbddbf7494baaaf759a720d9cd17540d3c171b9cc52a02e0ef9a592bd9cd63, f595f91a9966808cc85d11981e66e98043af9aeaaaa3893ef058b9a79c474f17, d4cb20dba15d88c38c35be69fe04538b4f9bb0a12edb51ff23c0171b584edf08, 7e18ff461e3fc159c9b6634c9250600ea4c62da604885697c95d9bac794109b8, b0b7a65f4821d5c9e8c782ee5ccca1c1a6a05236c27a4a136eb370302db2b35e, f709d1f84e4f0a845ebb4a9fb1500aa2a9fd600e97cbea32ffc3e49c1084f467, ab3985e07195465b9a9d8c5a9959e783e2a30f6d6e7fdda3ab153de4d7fc6fe6, f5d99d4548470b4699b215453e9be29e48aa20616d45f704c335bd3bbe3e0a4f, 8e5f99b92349381fd772b1bdb18cce2c6595181fcad0f68de25593276d61620f, d7cb8a2d60e1818d0638a4c38cd6fae475dc83ab7b2bde9827ecc4e4a7ce6ed7, 32c9c069c7fe9ffdd9086b957e45c03993863730cd1eed4815e226dc1b7b436e, 691eaa4c48666b69ca180b9aae1a4035fefb29cef1f0a3cfbc91c020b0b09f40, fe025cd046edabab5a07d058bfcbb884c144511581d5206681064355fb2834bc,

Attack Name	TYPE	VALUE
Phobos	SHA256	9f40b69060a52731107baec84a0c0f8a1bfc1a62e8471b9cd69509aade9cb7f1, 97a4d094f86b757b3fb0e189f2843a7af8d0ec43f9805214e89992528e83b5d7, 795b951e16aa4aa0557c24eedad4897e457864838393fcf66220da85ad8be9d8, 1c1eed8f9b2c44bb7290690521cc5f4e02929d5eeb3cc8fc2bf042cf3b789b8e, 681f180735ec833997bea4eb26c58f9c2e39980cd0a351e0b5cd99c502b33ae8, ebbbc1d293ce864c83cf874c3f8051dd636bd1303f013d3fa0cc97eada3266ac, 667F88E8DCD4A15529ED02BB20DA6AE2E5B195717EB630B20B9732C8573C4E83, 6E9C9B72D1BDB993184C7AA05D961E706A57B3BECF151CA4F883A80A07FDD955, 31dba1a23db70ffb952f0e597acf95d16ab60423018a83d0ccb4f57ce0471793, 56bd92cb5c9800338f01a5c8d6fdda4d602717d7a279ec499d15b8a2df36ec92, 62d67fe5548da330b0074f8fd162833e2675f8973899ae5778c10ef33a3f06af, 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6, 94e5a07113b228991a294f9b972d2727695ecd68520f56741ae4ad649d5d529b, 52507e8ce8151bd4fa072949245a50f002ed7973b322968b9690927d061d506f, 703cb9286dd4c0219dcb85fc960d0d662a784b5d9bf3ab78b379ac195fc72595, a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2, 596f40f23a1284b4e844e4159f07b92d0bdcfdc7ce00180a2b70af4f6843bed4, 25dce15057f3e9f904ea28e039fe0d2945308d7f41ea5386e99af4840c2e6762, c918ba4319356db7b86b34849baba40eb2fdc96b05c5ead8bf7375373ced3bcd, e443920a2306dd8b0182dedadc7c1254bd9c43e576c4876a1970886d06b1cccf, ffbafce6dc32dd8e1dc28d5de250f08f2f32d12b061c3ad5d7ee8125298bfc07, 61f5fcb639e3ad7b671a16e243bf0731e1759dcffde00eb14df56415856edbdb, 02db45a4a6821114adc7aad6eb875ff0db66f0ce1e63387dd02fd499e9a0b745, e30169690074a26afb368ec33e8195a89bd33a48f879913a100a67a960d033bb, 43f846c12c24a078ebe33f71e8ea3b4f75107aeb275e2c3cd9dc61617c9757fc,

Attack Name	TYPE	VALUE
Phobos	SHA256	9ab71ecc8338329b63410ba744c564c014eb5628eeed774302ef99bcc4e44d00, 9d298673b975048819034f7e746f9a2f4e011ae47ba87b48b9375e151326e7b1, 69e479f062e247568bb995ee0eed042d5cf1e37f4f41843981b52c55c10f6c7a, 409ef3b1cf30687fde062ac12af5ceebe5f91dd261f515231d172a4c0687ce72, 97e4ffdb8be8d108e5c81af0d8edda6e3bed9f37e170a05221199742f4de309c, a394878332e9c10950a04d9d735d23dc65e8d102fbfd04b790af7db40b60c5d5, 88d3bdfba7c8f0a49e6a296662e4d5ac13440ab38235602d75dbff3342cd2642, 55135de67a5816c6622ae671c934d5a2bfac1b8f3f09083f64a3ae5997bfbfdf, b4965b7fb169577c87cc40e303a002e497fb4812a1376b73e9ba85813917c733, 3b272c1e76e72bf4acc236b2305dd1c6b12dae729620e6c82f25b74a38b73044, 6575de46c36289308b49fa67bce7cf2c964d5367893391427487900069948bef7, 35920652147ca2dc1150f8605ed50036a8c50d869f328dc9912628a33db40b3a, f6b60839de0ac933f0788bc1e12dee859950010f938a05544ad51c424954b9a6, 7f8f8c82fec8acbb0947a192dd5cbe8b95ffdba4e252b582eae127f1c062399b, 2cadd0ff146e1cdf1270894be4fb1523bfdcc7a31760e0ca5cfd9d8e6b525c21, 4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e, cfc5fb8385f662b109c6cf866ff70e598964dd37dc3498d5bd45ad2c8f4c7d59, b93fcbafc42d24b88abeb354defad342110bb3928e7e24de4315b905dc74dd86, f0aec57001a184ea82122a59c6e5be48042f75d6f11a40125995ba9531aab718, ccc167391bb396f08e365eec5421786ccf1578ba8d3250debb9321767d33dff2, 4ce04ba4acc3645c66c9da89eb05e7708408e4463b5a901fc15be2479b9bdaf5, 2eff58738b5a7717a3fcdf7a4171c6fa18492bc200eddc26bf608fa35d28466e, F17D535192C421BF7C587C11190AE3BA6CC7EEE392DCCD86AD981D3547868D49, 883162246c3d0a2c10e5c35a2a43ff444a24dbcf9e64dc5cc09009b9cd0ab48e, 0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81,

Attack Name	TYPE	VALUE
Phobos	SHA256	527918fbd218787f202dcfb20024375238aca2dc64c1661bdc71f8833240e7f8, f0d6846da6d45180a695201888edc4f9c512fb0d11ed56394aae9daa874ba88c, fab5850b79de211ba1d789f80a4684657b3a79c849d46761decb2de95931162b, 51220927e71a1b8c5cc0ca85c454dc93f3aaae25bb3ec0dc3a9837236687d45f, f97cc59b803e60dcca4461975ecd5e6fc4c64dc31db89e187e5874503af1eb4d, 9f67b6057e5b5dc4b2ec3b370ca3062e0bed91a934b227911af2a3de17164ee5
	MD5	aaa058858261d7c0e73fa1b8264a9a3d, 1a75878dea8f5580c25e0b9f1c734949, 25674f5426c59051960f0d00f06f0b77, 9de437c0a1f9e633186f5f631d32af8a, 792b27b961ee8ae67855b952859053c7, 86e50a7bd09c2a5fc2eac716c29ea6c7, 6ad6c98f75c3133b94026c2fdd06a6f1, d62a9ae1380402cc467cced405ba4aa0, 840d99c89f366505d06259a89273f8b1, 4f25e57d4f754f0cea4f30d9da4156fd, 373a7a21c65d50861b0f7fa81d998165, 90bfa1d3b743c1546a053a206e49cac6, 4942b6f7a7b009cf5bb1ef7d31270b98, 733035ba7c294dd365d2a9601b900b4a, 471cb7869b9c4078717156e809e24001, 719000d0db27119867daf91dd1e8a20b, 2ec9ad510241a00a53f3090af9899250
	Emails	cadillac[.]407@aol[.]com, OttoZimmerman@protonmail[.]ch, ofizducwe111988@aol[.]com, FobosAmerika@protonmail[.]ch, posiccimen1982@aol[.]com, kipp[.]swindlehurst@aol[.]com, lachneyorlachb@aol[.]com, abbott_wearing@aol[.]com, decryptyourfiles@firemail[.]cc, 1decryption1@protonmail[.]com[.]
	IPv4	104[.]26[.]5[.]223, 185[.]112[.]82[.]235, 185[.]112[.]82[.]236, 185[.]112[.]82[.]237
	URLs	https://paste[.]ee/r/1q1gD, https://paste[.]ee/r/OwAyf, https://www[.]patreon[.]com/ccatss, hxxp://178[.]62[.]19[.]66/campo/v/v,

Attack Name	TYPE	VALUE
Phobos	File Paths	%LocalAppData%\horsemoney[.]exe, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\horsemoney[.]exe, %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\StartUp\horsemoney[.]exe
	Registry Keys	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney, HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney
MATA	MD5	2bf250d64e72a14f05ee190148291564, 9672437e1dc219ca8a4ee847bed25d0d, 01b3c7b2ff7e5158f80f593c09232e04, 996013c565b1f0ae68418d09d712d72b, 5f619927b586a6f776eb582f661ed55c, 91014e9b43ad489535e62e1b048feb59, 289b0d0b626b0be26ee81ed84fb94ec1
PowerExchange	SHA256	d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae
Clipog	SHA256	75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372
	SHA1	56df507f945d6149a1f0090a19c71254cc08c84e
	MD5	576a1d9e79bf32120d74eabae45f17ab
Munchkin	SHA256	1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d
Netrunner	MD5	6086673A65B85B3463B551BA611EE6E6
Dmcserv	MD5	16074C7518B2E5A3335CCF5AAA469470
ExelaStealer	SHA256	b9bc445af6729a95599f1a39e37f559f3ca18dbbc8ae4e60263af565ef4f4db3, 882484b56ad4418786852f401b1b81f31030bec8566b6b07c9798d4ea3033516, ccb1337383351bb6889eb8478c18c0142cb99cbb523acc85d0d626d323f5d7ad, d8488f93b8c096838b3d9b335091216667ce4ffc7ae2cf3c8925271f0f190c11, b6ca47065e68aebb007657ff0e6b0dfa0fc4e19823f336ab73f42b25dd5cfc22, 206278545b897a7e2ebb1ec4687e6ec31d7ca8f1828792a34f4fca745db8e3d4, 53b1b3c6f73312cdae7be69d16a42d298fae0cb3721c7fc11252f65b10f5a323, 2db54628a877ab40463a128496cb94523ccae6186d1648c6f372c719f6ed8152

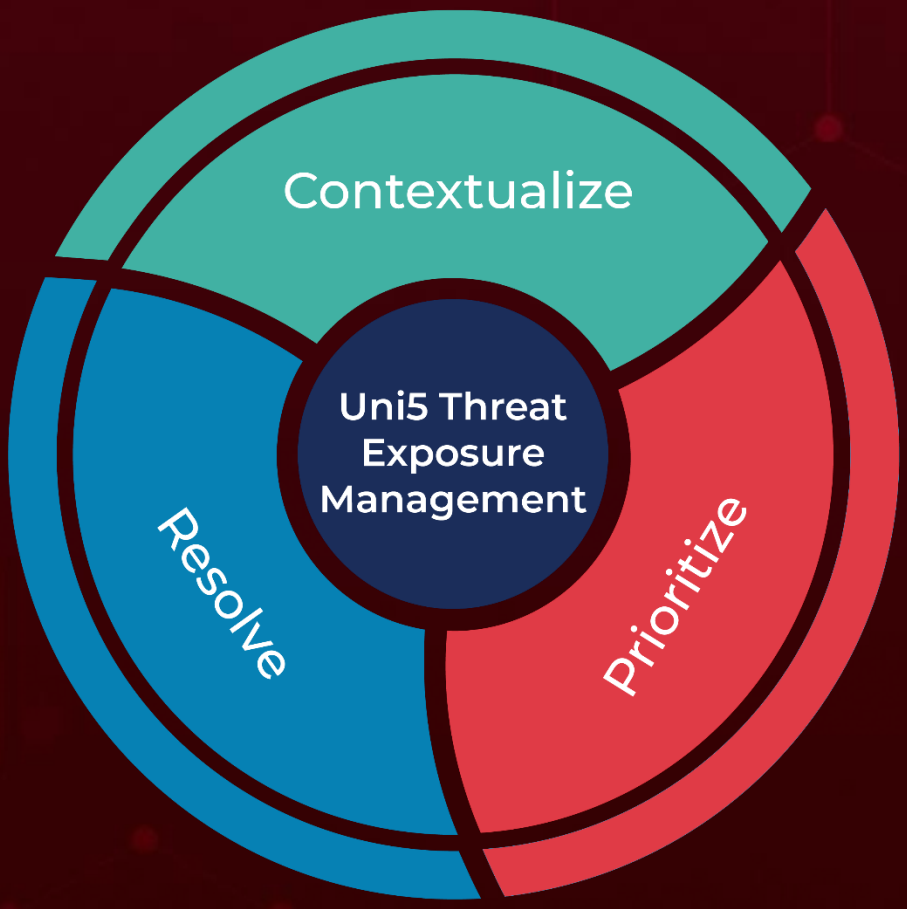
Attack Name	TYPE	VALUE
Quasar RAT	SHA256	5e3e65909b68d631913056a90e3da3e86c5378719f6d910d55989600d2a36cd1, 17ef487d5567c1fa318ae31b821746d6071dc21490de778359095e014127dff5, 8bd0ac703bd20a29a588599e2a3ee59d21e53cb356eea4a624ae859eaa23a381, f5e916891cb6585fb06e655518a64223aae96691f77e768398b32bfd7d9a90e0, b55588176b3531a9ecf8ba0e5b5a979df21046c46a63fb0e4ae225095a18b558, 7aa071e2184478eb932bd815a0eb393fb5efd7b322e3d333b908a9d7d33a4186, b55588176b3531a9ecf8ba0e5b5a979df21046c46a63fb0e4ae225095a18b558, 6dfe949ce3664c802ecd34968f18f0e9fc15f6fab58b35272ed7e83ab2442f2b, d64ec3e1fd63333c0d31d524027260e3d61c27921ab3d922a5a47588942ea051, c7550dc220b264239f7250607d6af8a0123107be4c377a3c94e5f8e63984b17d, 6ed6ea86dae39ff40a2b03781c2bbf13f5c7bc022d5419ef82d1d5f61535358c, d40f6568584ba4a9bda4e27dd7ef8f86620b648df32aee2eeb9c900de1b89f7d, 6cf1314c130a41c977aafce4585a144762d3fb65f8fe493e836796b989b002cb, ec8188e4e07aceea9afd588332ffb08549cc610364d8cd4695200f29b70da153, 6ff6f0407f18ac2a5cf56dd333998e5319f769f16d37b8f3cbf56e0f97e7b3d2
GoPIX	MD5	EB0B4E35A2BA442821E28D617DD2DAA2, 6BA5539762A71E542ECAC7CF59BDDF79, 333A34BD2A7C6AAF298888F3EF02C186
StripedFly	MD5	b28c6d00855be3b60e220c32bfad2535, 18f5ccdd9efb9c41aa63efbe0c65d3db, 2cdc600185901cf045af027289c4429c, 54dd5c70f67df5dc8d750f19ececd797, d32fa257cd6fb1b0c6df80f673865581, c04868dabd6b9ce132a790fdc02acc14, c7e3df6455738fb080d741dcbb620b89, d684de2c5cfb38917c5d99c04c21769a, a5d3abe7feb56f49fa33dc49fea11f85, 35fadceca0bae2cdcfdaac0f188ba7e0, 00c9fd9371791e9160a3adaade0b4aa2, 41b326df0d21d0a8fad6ed01fec1389f, 506599fe3aecdfb1acc846ea52adc09f, 6ace7d5115a1c63b674b736ae760423b, 2e2ef6e074bd683b477a2a2e581386f0, 04df1280798594965d6fdfeb4c257f6c, abe845285510079229d83bb117ab8ed6, 090059c1786075591dec7ddc6f9ee3eb

Attack Name	TYPE	VALUE
ThunderCrypt	MD5	120f62e78b97cd748170b2779d8c0c67, d64361802515cf32bd34f98312dfd40d, 3281b2d95e7123a429001400c10ebe28
	SHA256	8258c53a44012f6911281a6331c3ecbd834b6698b7d2dbf4b1828540793340d1
	SHA1	b97308ea9f9c410188d43c34a867fa42c9e9128e
SIGNBT	MD5	9cd90dff2d9d56654dbecdcd409e1ef3, 88a96f8730b35c7406d57f23bbba734d, 54df2984e833ba2854de670cce43b823, Ae00b0f490b122ebab614d98bb2361f7, e6fa116ef2705ecf9677021e5e2f691e, 31af3e7fff79bc48a99b8679ea74b589, 9b62352851c9f82157d1d7fcafeb49d3
LPEClient	MD5	3a77b5054c36e6812f07366fb70b007d, e89fa6345d06da32f9c8786b65111928
BiBi-Linux	SHA256	23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad

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

November 02, 2023 . 3:30 AM

More at www.hivepro.com