Date of Publication
October 2, 2023

Hive Pro®

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

SEPTEMBER 2023

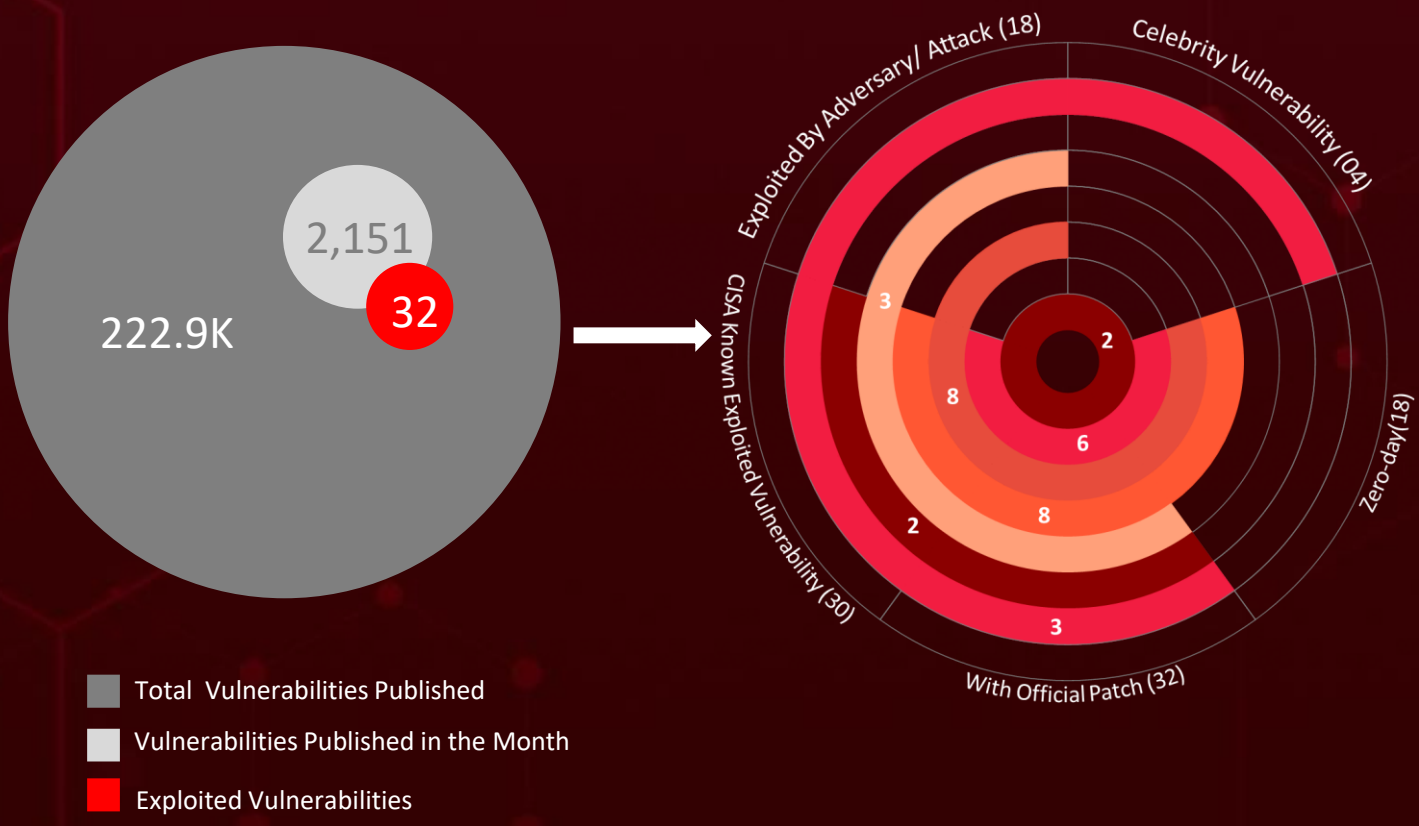
Table Of Contents

Summary

In **September**, the cybersecurity community witnessed significant attention drawn to the discovery of **eighteen zero-day** vulnerabilities. Among them was the **'Five Celebrity Vulnerability**,' which includes the **'ThemeBleed'** flaw in Windows 11, one exploited by **Charming Kitten**, and **three** celebrity vulnerabilities exploited by the **SprySOCKS** Backdoor.

September saw a rise in ransomware attacks, with various strains such as **FreeWorld**, **Akira**, **3AM**, and **Snatch** 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 by training employees to recognize and avoid phishing attacks.

Finally, **twelve adversaries** were active and involved in various campaigns. **Earth Lusca** APT's 'Sneaky Moves' exploited **nine vulnerabilities** to unleash the new Linux **SprySOCKS** Backdoor.



Insights

DreamBus

Botnet exploiting critical vulnerability (CVE-2023-33246) in Apache RocketMQ

ThemeBleed Strikes Windows 11:

Code Execution Threat Unleashed

34 Firms on Alert: Charming Kitten's

'Sponsor' Revelation Shakes Brazil, Israel, and the United Arab Emirates.

APT 33

Using Password Spray Campaigns to Infiltrate Organizations

Agent Tesla New variant

spreads through crafted Excel files, exploiting Office vulnerabilities **CVE-2017-11882 and CVE-2018-0802**

Unveiling the Storm-0324 Collaboration:

The Mastermind Behind Ransomware, Its Connection with FIN7, and Network Breaches

Silent Saboteurs

: United States and East Asia Under Siege - The BlackTech Cyber Saga

CVE-2023-20269:

Akira Ransomware Strikes Gold with Cisco VPN Vulnerability

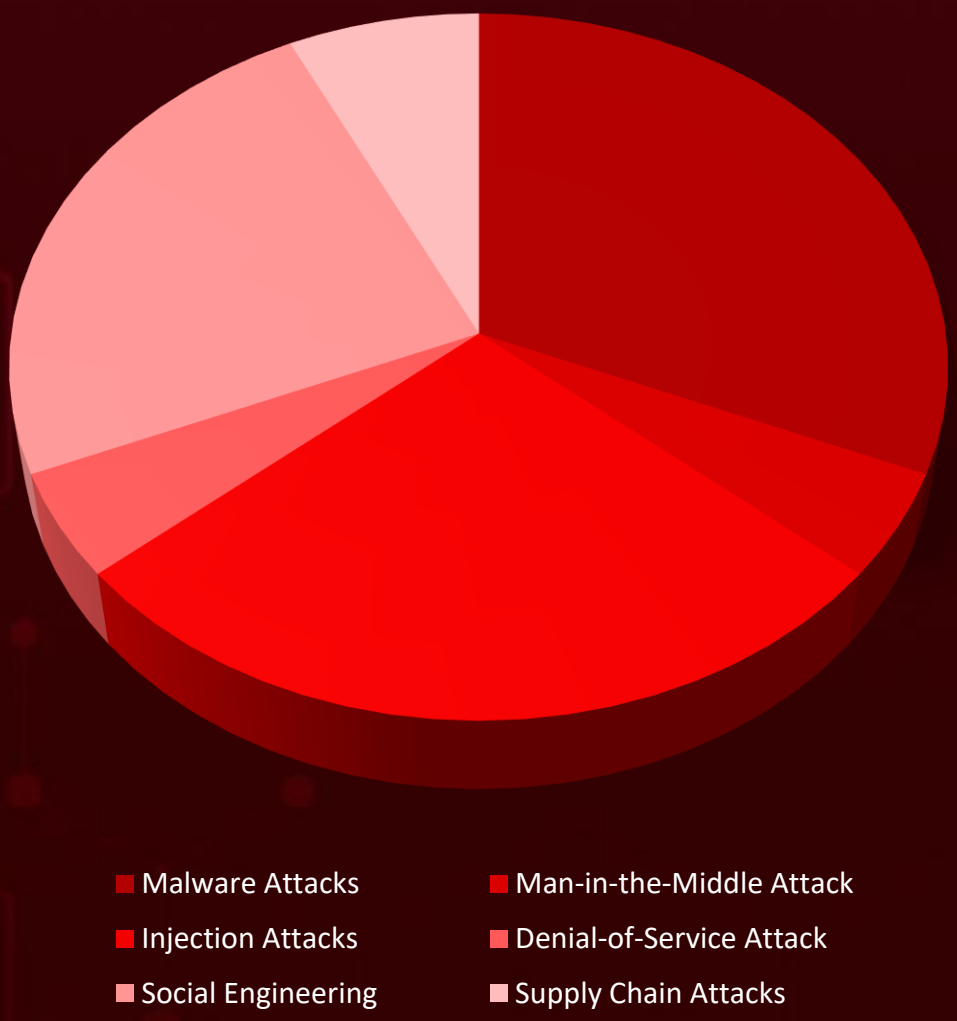
Trend Micro Zero Day Exploited:

CVE-2023-41179 identified in the third-party AV uninstaller module

Sandman APT

An espionage group of unknown origins targeting the Telecommunication sector with the LuaDream backdoor

Threat Landscape



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38146	✗	Windows 11 version 21H2, Windows 11 version 22H2	-
	CISA KEV		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_11_21h2:*:*:*:*:*:*:*:*	-
Microsoft Windows Themes Remote Code Execution Vulnerability (ThemeBleed)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1027: Obfuscated Files or Information	https://msrc.microsoft.com/CVE-2023-38146

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	✓	Microsoft Exchange Server	Charming Kitten
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	Sponsor Backdoor
Microsoft Exchange Server Remote Code Execution Vulnerability (ProxyLogon)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1090: Proxy,T1135: Network Share Discovery,T1005: Data from Local System,T1133: External Remote Service	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	✗	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Remote Code Execution Vulnerability (PROXYSHELL)		CWE ID	ASSOCIATED TTPs	PATCH DETAILS
		CWE-918	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

CVE ID	ZERO-DAY	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	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)		CWE ID	ASSOCIATED TTPs	PATCH DETAILS
		CWE-787	T1556: Modify Authentication Process	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523		Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	SprySOCKS Backdoor
Microsoft Exchange Server Privilege Escalation Vulnerability (PROXYSHELL)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-28432	MinIO Information Disclosure Vulnerability	MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z	✓	✓	✓
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	Apache RocketMQ: 4.2.0 - 5.1.0	✓	✓	✓
CVE-2018-0802	Microsoft Office Memory Corruption Vulnerability	Microsoft Office: 2007 – 2016; Microsoft Word: 2007 - 2016	✓	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office: 2007 - 2016	✗	✓	✓
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Multiple products of Zoho ManageEngine	✗	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	FortiOS: 6.2.0 - 7.2.2	✓	✓	✓
CVE-2023-20269	Cisco Brute Access Vulnerability	Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18	✓	✓	✓
CVE-2023-4863	Google Chrome Heap Buffer Overflow Vulnerability	Google Chrome version 116.0.5845.186 and before	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability (ProxyLogon)	Microsoft Exchange Server	✓	✓	✓
CVE-2023-26369	Adobe Code Execution Vulnerability	Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions,Acrobat Reader 2020, 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions	✓	✓	✓
CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability	Microsoft Office: 365 - 2019, Microsoft Word: before 16.0.5413.1000, Microsoft 365 Apps for Enterprise: before 16.0.5413.1000	✓	✓	✓
CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	Windows: 10 - 11 22H2, Windows Server: 2019 - 2022 20H2	✓	✓	✓
CVE-2023-41064	Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	Apple iOS, iPadOS, and macOS	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-41061	Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	Apple iOS, iPadOS, and watchOS	✓	✓	✓
CVE-2023-3676	Kubernetes Privilege Escalation Vulnerability	kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17	✗	✗	✓
CVE-2023-21715	Microsoft Office Publisher Security Feature Bypass Vulnerability	Microsoft Teams	✓	✓	✓
CVE-2023-38146	Microsoft Windows Themes Remote Code Execution Vulnerability (ThemeBleed)	Windows 11 version 21H2, Windows 11 version 22H2	✗	✗	✓
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Multiple products of Zoho ManageEngine	✗	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Confluence Server and Confluence Data Center	✓	✓	✓
CVE-2023-41179	Trend Micro Arbitrary Code Execution Vulnerability	Trend Micro Apex One OnPremise (2019) Trend Micro Apex One as a Service Worry-Free Business Security 10.0 SP1 Worry-Free Business Security Services (SaaS)	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2022-40684	Fortinet Multiple Products Authentication Bypass Vulnerability	FortiOS, FortiProxy, and FortiSwitch Manager	✗	✓	✓
CVE-2021-22205	GitLab Community and Enterprise Editions Remote Code Execution Vulnerability	GitLab CE/EE	✗	✓	✓
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	TELERIK.WEB.UI.DL	✗	✓	✓
CVE-2019-9670	Synacor Zimbra Collaboration (ZCS) Improper Restriction of XML External Entity Reference	Zimbra Collaboration Suite v8.5 to v8.7.11	✗	✓	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability (PROXYSHELL)	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	✗	✓	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability (PROXYSHELL)	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	✗	✓	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	✗	✓	✓
CVE-2023-3932	GitLab Pipeline Execution Vulnerability	GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-41991	Apple Signature Bypass Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓
CVE-2023-41992	Apple Privilege Escalation Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓
CVE-2023-41993	Apple Arbitrary Code Execution Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓
CVE-2023-5217	libvpx Buffer Overflow Vulnerability	Google Chrome: 100.0.4896.60 - 117.0.5938.92, Firefox 100.0 - 118.0, Firefox ESR 10.0 - 115.3.0, Firefox Focus for Android 108.2.0 - 118.0, Firefox for Android 66.0.4 - 118.0	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
IDAT Loader	Loader	-	Windows	-	Phishing emails
StealC	Information Stealer	-	Windows	-	-
Lumma	Information Stealer	-	Windows	-	Malware-as-a-Service
Amadey	Trojan	-	Windows	-	Phishing emails, exploit kits, and drive-by downloads
SuperBear RAT	RAT	-	Windows	-	Phishing emails
FreeWorld Ransomware	Ransomware	-	MS SQL servers	-	Brute Force
Chae$ 4	Information Stealer	-	-	-	Phishing emails
DreamBus	Botnet	CVE-2023-33246	Apache RocketMQ	✓	Exploiting vulnerabilities
DuckTail	Information Stealer	-	Windows	-	Phishing emails
Agent Tesla	RAT	CVE-2017-11882 CVE-2022-47966	Microsoft Office	✓	Phishing emails
Akira Ransomware	Ransomware	CVE-2023-20269	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)	✓	Cisco VPN products
HijackLoader	Loader	-	-	-	Unknown
PhoenixMiner	Miner	-	-	-	Malicious Installer

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
lolMiner	Miner	-	-	-	Malicious Installer
M3_Mini_Rat	RAT	-	-	-	Malicious Installer
Sponsor Backdoor	Backdoor	CVE-2021-26855	Microsoft Exchange Server	✓	Exploiting well-documented vulnerabilities
3AM Ransomware	Ransomware	-	-	-	Unknown
JSSLoader	RAT	CVE-2023-21715	Microsoft Teams	✓	Spearphishing Link
ShadowPad	Modular RAT	-	-	-	Phishing emails
Packerloader	Loader	-	-	-	Unknown
HTTPSnoop	Backdoor	-	-	-	Phishing emails
PipeSnoop	Backdoor	-	Windows	-	Phishing emails
SprySOCKS backdoor	Backdoor	CVE-2022-40684 CVE-2021-22205 CVE-2019-18935 CVE-2019-9670 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center	✓	Exploiting CVEs

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
VenomRAT	RAT	CVE-2023-25157 CVE-2023-40477	GeoServer & WinRAR: 6.00 - 6.22 beta 1	✓	Phishing emails
Snatch ransomware	Ransomware	-	-	-	Ransomware -as-a-service
LuaDream	Information Stealer	-	-	-	Phishing emails
RedLine Stealer	Information Stealer	-	Windows	-	Phishing emails
Deadglyph Backdoor	Backdoor	-	-	-	Unknown
ZenRAT	RAT	-	Windows	-	SEO poisoning, adware bundles, or email-based attacks.
Bisonal	Backdoor	-	-	-	Visual Basic Script backdoor
ReVBShell	Backdoor	-	-	-	Social engineering
DangerAds	Loader	-	-	-	Phishing
AtlasAgent	Trojan	-	-	-	Phishing

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Smishing Triad	Information theft and Financial fraud	China	-	-	-
Charming Kitten	Information theft and espionage	Iran	CVE-2021-26855	Sponsor Backdoor	Microsoft Exchange Server
Storm-0324	Financial Gain	Unknown	CVE-2023-21715	JSSLoader	Microsoft Teams
APT33	Information theft and espionage, Sabotage and destruction	Iran	CVE-2022-47966 CVE-2022-26134	-	ZohoManageEngine products & Atlassian Confluence Server
Redfly	Information theft and espionage	China	-	ShadowPad and Packerloader	-
ShroudedSnooper	Information theft and espionage	Unknown	-	HTTPSnoop and PipeSnoop	-
Earth Lusca	Information theft and espionage, Financial gain	China	CVE-2022-40684 CVE-2021-22205 CVE-2019-18935 CVE-2019-9670 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207	SprySOCKS Backdoor	FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center

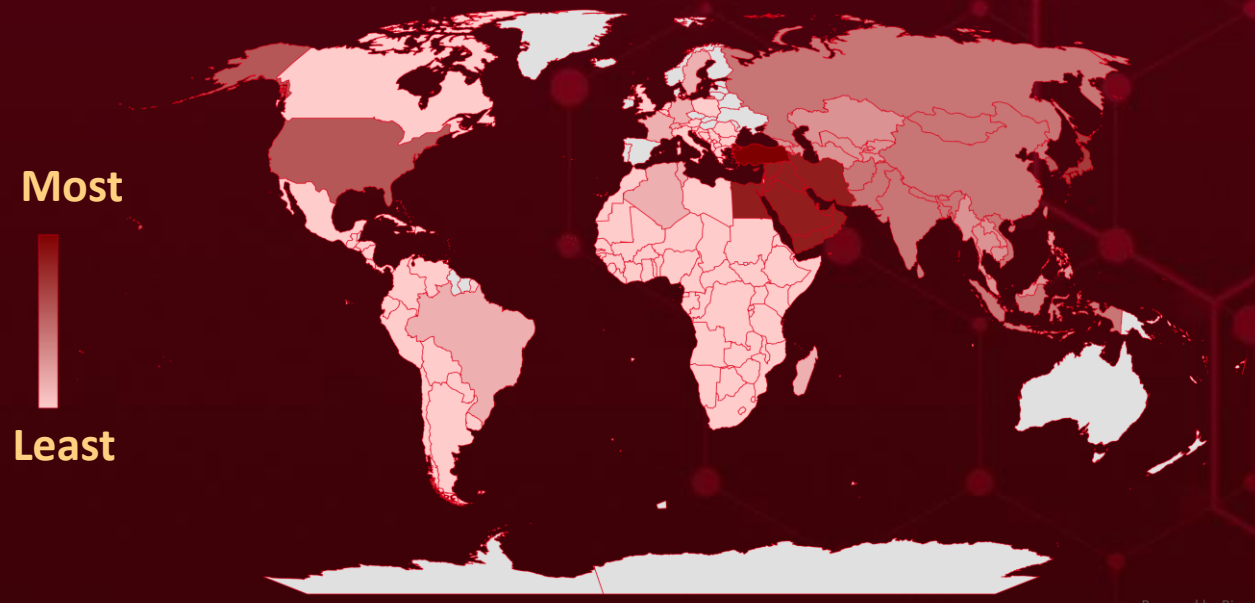
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Sandman APT	Information theft and espionage	China	-	ShadowPad and Packerloader	-
Stealth Falcon	Information theft and espionage	UAE	-	Deadglyph Backdoor	-
TAG-74	Cyber-espionage	China	-	Bisonal and ReVBShell	-
BlackTech	Information theft and espionage	China	-	-	Windows, Linux, and FreeBSD
AtlasCross	Information theft and espionage	Unknown	-	DangerAds and AtlasAgent	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
MINIO	Framework	MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z
APACHE HTTP SERVER PROJECT	Application	Apache RocketMQ: 4.2.0 - 5.1.1
ATLASSIAN	Application	Atlassian Confluence Server, Jira Service Management Server and Data Center (versions 4.20.0-5.8.1), Bitbucket Server and Data Center (versions 8.0-8.13.0)
ASUS	Routers	ASUS RT-AX55: 3.0.0.4.386_50460 ASUS RT-AX56U_V2: 3.0.0.4.386_50460 ASUS RT-AC86U: 3.0.0.4_386_51529
ZOHO	Application	Zoho ManageEngine Multiple on-premise products
FORTINET	Application	Fortinet FortiOS: 7.2.0 - 7.2.2, 7.0.0 - 7.0.8, 6.4.0 - 6.4.10, 6.2.0 - 6.2.11, FortiNAC versions 9.4.0- 8.3.7
CISCO	Security Appliance	Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18
	Application	Google Chrome version 116.0.5845.186 and Before, and Google Chrome: 100.0.4896.60 - 117.0.5938.92
Adobe	Application	Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac),20.005.30514 (Win),and earlier versions, Acrobat Reader 2020,20.005.30516 (Mac),20.005.30514 (Win),and earlier versions
Firefox	Applications	Firefox 100.0 - 118.0, Firefox ESR 10.0 - 115.3.0, Firefox Focus for Android 108.2.0 - 118.0, Firefox for Android 66.0.4 - 118.0

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
Microsoft	Application	Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 – 2019, RTM Mar21SU 15.02.0221.018, Microsoft Office: 365 – 2019, Microsoft Word: before 16.0.5413.1000, Microsoft 365 Apps for Enterprise: before 16.0.5413.1000, Windows: 10 - 11 22H2 Windows Server: 2019 - 2022 20H2, Microsoft Windows Themes and Microsoft Teams
	Operating system	iPhone 8 and later, iPad Pro (all models) iPad Air 3rd generation, and later, iPad 5th generation and later, iPad mini 5th generation and later Macs running macOS Ventura, and Apple Watch Series 4 and later
kubernetes	Applications	kubernetes-csi-proxy earlier to v2.0.0-alpha.0, kubernetes-csi-proxy earlier to v1.1.2, kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17
TREND MICRO	Application	Trend Micro Apex One On Premise (2019) Trend Micro Apex One as a Service Worry-Free Business Security 10.0 SP1 Worry-Free Business Security Services (SaaS)
GitLab	Application	GitLab Community and Enterprise Editions, GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4.
Telerik	Application	Progess Telerik UI for ASP.NET AJAX
zimbra	Application	Synacor Zimbra Collaboration (ZCS), Zimbra Collaboration
GeoServer	Application	GeoServer
WinRAR	Application	WinRAR: 6.00 - 6.22 beta 1
Nagios	Network monitoring software	Nagios XI versions 5.11.1 and lower

Targeted Countries



Color	Countries
	Turkey
	Palestine
	Lebanon
	Bahrain
	Saudi Arabia
	Cyprus
	Kuwait
	Egypt
	Oman
	Iran
	Qatar
	Iraq
	Syria
	Israel
	United Arab Emirates
	Jordan
	Yemen
	Japan
	South Korea
	United States
	Sri Lanka
	Russia
	Bangladesh

Color	Countries
	Indonesia
	Singapore
	China
	North Korea
	Akrotiri and Dhekelia
	Pakistan
	Afghanistan
	Bhutan
	Maldives
	Hong Kong
	Taiwan
	India
	Nepal
	Mongolia
	Vietnam
	Turkmenistan
	Laos
	Azerbaijan
	Uzbekistan
	Tajikistan
	Malaysia
	Philippines

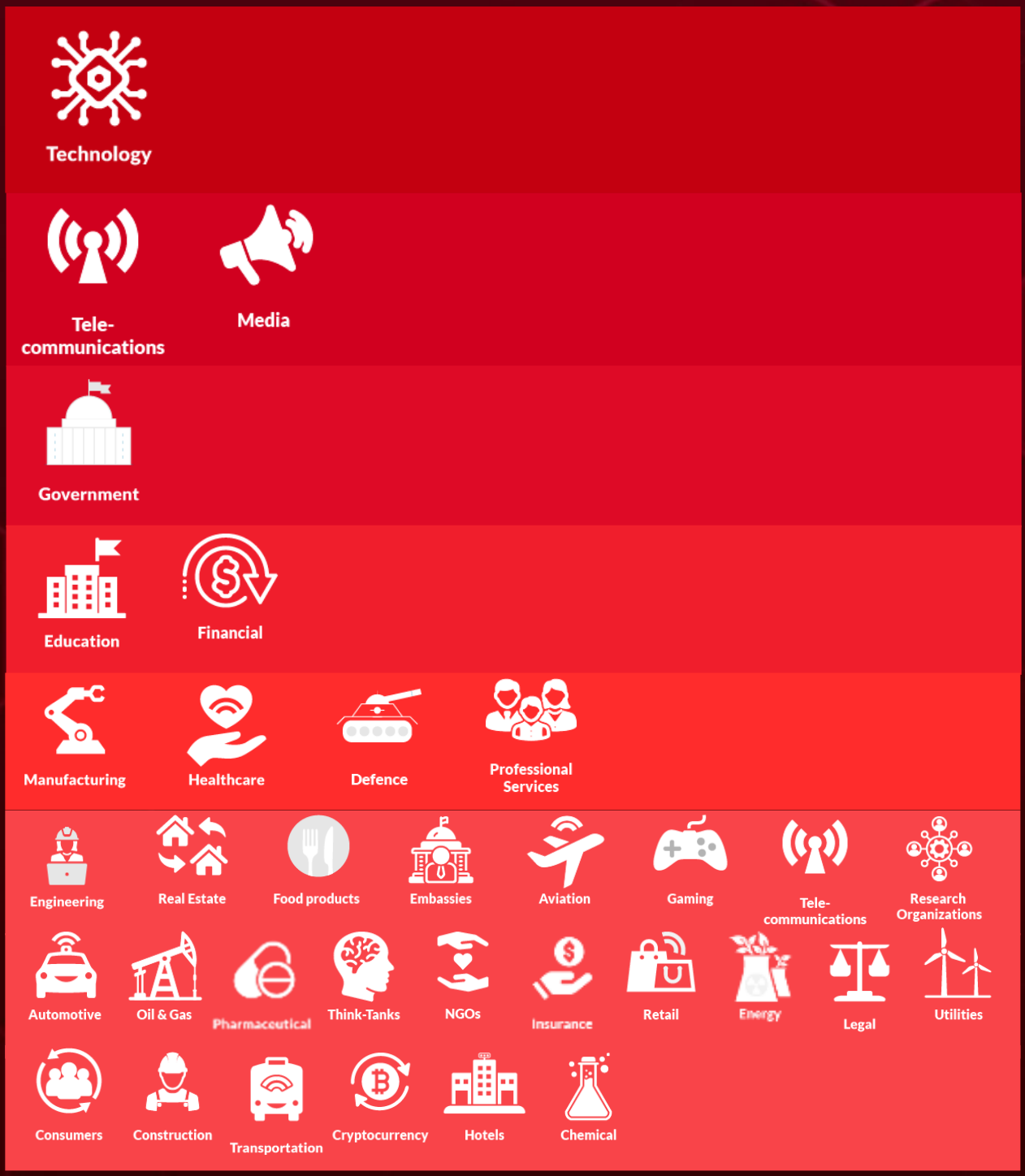
Color	Countries
	Cambodia
	Kyrgyzstan
	Myanmar
	Georgia
	Brunei
	Thailand
	East Timor
	Macao
	Armenia
	Kazakhstan
	Switzerland
	France
	Tunisia
	Algeria
	Sweden
	Germany
	Madagascar
	Brazil
	Senegal
	Belgium
	Guinea
	Angola
	Republic of the Congo

Color	Countries
	Argentina
	Cape Verde
	Burkina Faso
	Botswana
	Italy
	French Guiana
	Ivory Coast
	Saint Barthélemy
	Colombia
	Canada
	Austria
	Greece
	Comoros
	Haiti
	Kenya
	Chad
	Kosovo
	Paraguay
	Costa Rica
	Puerto Rico
	Croatia
	Gabon
	Cuba

Color	Countries
	Albania
	Seychelles
	Western Sahara
	Somalia
	Zambia
	Ghana
	Djibouti
	Bolivia
	Liechtenstein
	Guinea-Bissau
	Luxembourg
	Honduras
	Dominican Republic
	Central African Republic
	Macau
	Chile
	DR Congo
	Panama
	Burundi
	Peru
	Ecuador
	Poland

Targeted Industries

Most



Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1027** Obfuscated Files or Information	**T1566** Phishing	**T1203** Exploitation for Client Execution
T1036 Masqueradin g	**T1190** Exploit Public-Facing Application	**T1204** User Execution	**T1055** Process Injection	**T1588.006** Vulnerabilitie s
T1082 System Information Discovery	**T1204.002** Malicious File	**T1588.005** Exploits	**T1068** Exploitation for Privilege Escalation	**T1059.001** PowerShell
T1140 Deobfuscate/ Decode Files or Information	**T1574** Hijack Execution Flow	**T1105** Ingress Tool Transfer	**T1057** Process Discovery	**T1112** Modify Registry
T1497 Virtualization /Sandbox Evasion	**T1059.003** Windows Command Shell	**T1041** Exfiltration Over C2 Channel	**T1078** Valid Accounts	**T1071** Application Layer Protocol

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LummaC Stealer	MD5	507bddfabd74a3d024b2ad5f67d666ea
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock
Amadey Bot	MD5	952d825a264745bb52b6977ba5983568
	SHA1	627a0a841c2fe194dd54f9ec6b0c1231d7da135f
	SHA256	d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c,
	SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d
	URLS	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe
SuperBear RAT	SHA256	282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb
FreeWorld	SHA256	75975B0C890F804DAB19F68D7072F8C04C5FE5162D2A4199448FC0E1AD03690B

Attack Name	TYPE	VALUE
PhoenixMiner	SHA256	3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3, 201a1979e02bcaa2808e31613a0bef99ad55d514fcaed973840a1bf1efdb4cbe, f4b1dc6456aed765e11878c6a5b9555ee2aec1737219137d187e480599e254c9, D241ef2a157f44dcc323279bd89168c0f6b142de964815ceb0429181eae9a789
lolMiner	SHA256	2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73, aafe94fe2ca6210fde8f5691c066dc128090b097a7d45a69d7ccc977891e08b4, 8ebe85fd149f9b1e93668a733182ad6e0cafd1a0b285800e4e6b226b8673cbaa, ac1af3a386b2dcf0e2a2955101dc91de7f5e62c900ba4476b0b842d1aa951bbe, 2c049deedbc83923abdd41580faa07c98037f09b5fabe98f97a9239a0b6e3542
M3_Mini_Rat	SHA256	7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08
Sponsor Backdoor	SHA1	098b9a6ce722311553e1d8ac5849ba1dc5834c52, 5aee3c957056a8640041abc108d0b8a3d7a02ebd, 764eb6ca3752576c182fc19cff3e86c38dd51475, 2f3eda9d788a35f4c467b63860e73c3b010529cc, e443dc53284537513c00818392e569c79328f56f, c4bc1a5a02f8ac3cf642880dc1fc3b1e46e4da61, 39ae8ba8c5280a09ba638df4c9d64ac0f3f706b6, a200be662cdc0ece2a2c8fc4dbbc8c574d31848a, 5d60c8507ac9b840a13ffdf19e3315a3e14de66a, 50cfb3cf1a0fe5ec2264ace53f96fadfe99cc617, 1aae62acee3c04a6728f9edc3756fabd6e342252, 519ca93366f1b1d71052c6ce140f5c80ce885181, 4709827c7a95012ab970bf651ed5183083366c79, 99c7b5827df89b4fafc2b565abed97c58a3c65b8, e52aa118a59502790a4dd6625854bd93c0deaf27
	File Path	%SYSTEMDRIVE%\inetpub\wwwroot\aspnet_client\, %USERPROFILE%\AppData\Local\Temp\file\, %USERPROFILE%\AppData\Local\Temp\2\low\, %USERPROFILE%\Desktop\, %USERPROFILE%\Downloads\a\, %WINDIR%\, %WINDIR%\INF\MSExchange Delivery DSN\, %WINDIR%\Tasks\, %WINDIR%\Temp\%WINDIR%\Temp\crashpad\1\Files
	IPv4	162.55.137[.]20, 37.120.222[.]168, 198.144.189[.]74, 5.255.97[.]172

Attack Name	TYPE	VALUE
JSSLoader	SHA256	969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, ee8f394d9e192c453d47a0c57261a03921dcbb97248a67427cb6fc6d8833c8a0, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, c328f48c5f4a2c2441bcd0b0c0551547ca254f7ebbb46d30d357e962d8330063, 8279ce0eb52a9f5b5ab02322d1bb7cc9cb5b242b7359c3d4d754687069fcb7b8, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0
ShadowPad	SHA256	656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c, ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646, 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3, d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3
Packerloader	SHA256	32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a
SprySOCKS Backdoor	SHA256	6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc, f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912, eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
	Domains	lt76ux.confenos[.]shop, 2e6veme8xs.bmssystemg188[.]us
VenomRAT	SHA256	61dd71441a2b4955467243e986c38f1ea543bae7b1546f003c4a30074dd6c04e, cabc45f1dab04be3fc63192d98324d2665599a6d6ea2f0277ecd27a62fb694f3, 79b87d7accc9cbd1414b72ca13c48a385be9cb06c1bb53d845e94107b579bf62, 4b84283c40560991da34ef2b465a4724facd0932acebff60466d8d5ff1916bd5, 75c12ccacd764101736b213981355b39056227929214c8963e9bf3ea5a60f6ef, 1648bea3c1c3b00e7f9c9bf7f65be833fa7f291f0e05a342382e9e36f0350c60,

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28432		MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:minio:minio:*:*:*:*:*:*:*:*	-
MinIO Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1082: System Information Discovery	https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33246		Apache RocketMQ: 4.2.0 - 5.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	DreamBus
Apache RocketMQ Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

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:2007:sp3:*:*:*:*:*:*	Agent Tella
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1495: Firmware Corruption	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0802		Microsoft Office: 2007 – 2016; Microsoft Word: 2007 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*	Agent Tella
Microsoft Office Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1495: Firmware Corruption	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966	✗	Multiple products of Zoho ManageEngine	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	-
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42475	✗	FortiOS: 6.2.0 - 7.2.2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	-
Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://fortiguard.com/psirt/FG-IR-22-398

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-20269</td><td>✗</td><td rowspan="2">Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and
Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18</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:h:cisco_systems:asa:6.2.3:*:*:*:*:*:*:*
cpe:2.3:h:cisco_systems:firepower:6.2.3:*:*:*:*:*:*:*</td><td rowspan="2">Akira Ransomware</td></tr>
<tr><td rowspan="3">Cisco Brute Access Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>WORKAROUND</td></tr>
<tr><td>CWE-288</td><td>T1110: Brute Force,T1059: Command and Scripting Interpreter,T1059.008: Network Device CLI</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC#workarounds</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4863		Google Chrome version 116.0.5845.186 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Heap Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-122	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3932		GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	-
GitLab Pipeline Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-862	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/#attacker-can-abuse-scan-execution-policies-to-run-pipelines-as-another-user

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-26369</td><td>  </td><td rowspan="2">Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions,Acrobat Reader 2020, 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions</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:adobe:adobe_reader:23.003.20284:*:*:*:*:*:*:* cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Adobe Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-787</td><td>T1203: Exploitation for Client Execution,T1588: Obtain Capabilities,T1588.005: Exploits,T1204: User Execution, T1204.002: Malicious File</td><td>https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#classic-track</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36761		Microsoft Office: 365 - 2019, Microsoft Word: before 16.0.5413.1000, Microsoft 365 Apps for Enterprise: before 16.0.5413.1000	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_word:-:*:*:*:*:*:*:*	-
Microsoft Word Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1588.006: Vulnerabilities,T1068: Exploitation for Privilege Escalation,T1203: Exploitation for Client Execution, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36761

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36802		Windows: 10 - 11 22H2, Windows Server: 2019 - 2022 20H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_streaming_service:-:*:*:*:*:*:*:*	-
Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1588.006: Vulnerabilities,T1068: Exploitation for Privilege Escalation,T1203: Exploitation for Client Execution, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41064	✗ ZERO-DAY	Apple iOS, iPadOS, and macOS	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-120	T1204: User Execution,T1204.002: Malicious File,T1588: Obtain Capabilities,T1588.005: Exploits,T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1204.003: Malicious Image	https://support.apple.com/en-us/HT213905 https://support.apple.com/en-us/HT213906

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41061	✗ ZERO-DAY	Apple iOS, iPadOS, and watchOS	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1204: User Execution,T1204.002: Malicious File,T1588: Obtain Capabilities,T1588.005: Exploits,T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1204.003: Malicious Image	https://support.apple.com/en-gb/HT213907 https://support.apple.com/en-us/HT213905

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3676	✗	kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:kubernetes:-:*:*:*:*:*:*:*	-
Kubernetes Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1609: Container Administration Command,T1610: Deploy Container,T1059: Command and Scripting Interpreter,T1059.001: PowerShell,T1548: Abuse Elevation Control Mechanism,T1068: Exploitation for Privilege Escalation	https://kubernetes.io/releases/patch-releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21715	✗	Microsoft Teams	Storm-0324
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:*:*	JSSLoader
Microsoft Office Publisher Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-863	T1059: Command and Scripting Interpreter,T1040: Network Sniffing,T1203:Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966	✗	Multiple products of Zoho ManageEngine	APT 33
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	-
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134	✗	Confluence Server and Confluence Data Center	APT 33
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	-
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-2023-41179	✗	Trend Micro Apex One OnPremise (2019) Trend Micro Apex One as a Service Worry-Free Business Security 10.0 SP1 Worry-Free Business Security Services (SaaS)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trend_micro:apex_one:CP_12033:*:*:*:*:*:*:*	-
Trend Micro Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://success.trendmicro.com/dcx/s/solution/000294994/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40684	✗	FortiOS, FortiProxy, and FortiSwitchManager	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Fortinet Multiple Products Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1556: Modify Authentication Process	https://fortiguard.com/psirt/FG-IR-22-377

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22205		GitLab CE/EE	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*	SprySOCKS Backdoor
GitLab Community and Enterprise Editions Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-9670	✗	Zimbra Collaboration Suite v8.5 to v8.7.11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Synacor Zimbra Collaboration (ZCS) Improper Restriction of XML External Entity Reference	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-611	T1068: Exploitation for Privilege Escalation	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41991	✗	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:watchos:10.0:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:17.0:*:*:*:*:*:*:*	Predator
Apple Signature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-347	T1040: Network Sniffing, T1190: Exploit Public-Facing Application	https://support.apple.com/en-us/HT213927

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41992	✗	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:watchos:10.0:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:17.0:*:*:*:*:*:*:*	Predator
Apple Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1068: Exploitation for Privilege Escalation, T1562: Impair Defenses	https://support.apple.com/en-us/HT213927

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41993	✗	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:apple_safari:16.6:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:17.0:*:*:*:*:*:*:*	Predator
Apple Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/HT213927

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-5217</td><td>  </td><td rowspan="2">Google Chrome: 100.0.4896.60 - 117.0.5938.92, Firefox 100.0 - 118.0, Firefox ESR 10.0 - 115.3.0, Firefox Focus for Android 108.2.0 - 118.0, Firefox for Android 66.0.4 - 118.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:google:google_chrome:117.0.5938.92:*:*:*:*:*:*:*
cpe:2.3:a:mozilla:firefox_focus_for_android:118.0:*:*:*:*:*:*:*
cpe:2.3:a:mozilla:firefox_ESR:115.3.0:*:*:*:*:*:*:*
cpe:2.3:a:mozilla:mozilla_firefox:118.0:*:*:*:*:*:*:*
cpe:2.3:a:mozilla:firefox_for_android:118.0:*:*:*:*:*:*:*</td><td rowspan="2">Predator</td></tr>
<tr><td rowspan="2">libvpx Buffer Overflow Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-122</td><td>T1574: Hijack Execution Flow, T1499.004: Application or System Exploitation, T1005: Data from Local System</td><td>https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html
https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
IDAT loader	The IDAT loader is a new, sophisticated malware loader that was first seen in July 2023. It is designed to deliver other malware, such as infostealers and RATs (Remote Access Trojans). The IDAT loader uses a variety of evasion techniques to avoid detection by security software, including process doppelgänging, DLL search order hijacking, and Heaven's Gate.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
StealC	StealC is a new information stealer that is designed to steal sensitive information from compromised systems. It is a Windows-based malware that is uses a variety of evasion techniques to avoid detection by security software, such as code obfuscation, anti-debugging, and anti-virtualization.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	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
Lumma Stealer	Lumma Stealer is a malware that steals sensitive information from infected devices. It is distributed through a Malware-as-a-Service (MaaS) model on Russian-speaking forums. The malware is written in C language and is constantly being updated with new features.	Malware-as-a-Service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Amadey Bot	Amadey Bot is a modular Trojan malware that steals sensitive information and can download other malware. It can be customized to perform a variety of tasks.	Phishing emails, exploit kits, and drive-by downloads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SuperBear	SuperBear is a remote access trojan (RAT) that was first discovered in 2022. It is a sophisticated piece of malware that is designed to steal sensitive information from compromised systems. SuperBear is primarily targeted at journalists and other individuals who cover sensitive topics.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Steal 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
FreeWorld	FreeWorld is a new ransomware that targets Microsoft SQL servers using brute-force attacks. It encrypts files with a .freeworldencryption extension and demands a ransom for decryption. It is a variant of the Mimic ransomware and uses Cobalt Strike to establish persistence on the compromised servers.	Brute Force	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Encrypt	MS SQL servers
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Chae$ 4	A new Chaes malware variant, "Chae$ 4," targeting logistics, finance, and prominent platforms has emerged with enhanced capabilities, including Python-based architecture and an expanded range of targeted services and data theft functions.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DreamBus	DreamBus is a modular Linux-based botnet that has been around since early 201912. The malware can spread internally by scanning private subnet ranges for vulnerable systems, using common and default passwords via brute force or application-specific exploits.	Exploiting vulnerabilities	CVE-2023-33246
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Compromise system	Apache RocketMQ
ASSOCIATED ACTOR			**PATCH LINK**
-			https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

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
DuckTail	DuckTail malware is a .NET Core-based information stealer that targets Facebook users and business accounts. It can extract browser cookies and use social media sessions to obtain sensitive information and place fraudulent advertisements for financial gain. It has been active since 2018 and has evolved with new malicious capabilities to bypass Facebook's security measures.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agent Tesla	New variants of Agent Tesla that have been detected in recent phishing campaigns that target various sectors and regions4512. These variants use crafted Excel documents or malicious links to download the malware onto the victim's device12. They also use AutoIT scripts to obfuscate and execute the malware payload2.	Phishing emails	CVE-2017-11882 CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Compromise data	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira Ransomware	Akira, a relatively new ransomware operation, emerged in March 2023 and is written in C++. It has expanded its tactics by adding a Linux encryptor to target VMware virtual machines. The Akira ransomware group targets Cisco VPN products to breach corporate networks and leverages tools like RustDesk for stealthy access.	Cisco VPN products	CVE-2023-20269
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Extortion of data and Financial Loss	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)
ASSOCIATED ACTOR			**Workaround**
-			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PhoenixMiner	PhoenixMiner Ethereum cryptocurrency mining malware with the filename "svhost.exe". PhoenixMiner is a publicly available miner that relies on the GPU capabilities of computers. The PowerShell launcher executes PhoenixMiner with the Ethereum Classic mining parameters from the victim machine's Windows systems folder.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Data Theft and Espionage	-
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
HijackLoader	A new malware loader, HijackLoader, is swiftly gaining prominence within the cybercriminal sphere, being leveraged to disseminate an array of malicious malware strains, including DanaBot, SystemBC, and RedLine Stealer.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft and compromised systems	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
lolMiner	lolMiner mines cryptocurrency by stealing the computational power of AMD, Nvidia, and Intel graphics cards. lolMiner is compatible with a variety of protocols, including Etchash, Autolykos2, Beam, Grin, Ae, ALPH, Flux, Equihash, Kaspa, Nexa, Ironfish, and others. This campaign's lolMiner version is 1.76, which allows for the simultaneous mining of two different cryptocurrencies.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
M3_Mini_Rat	The M3_Mini_Rat client stub is a PowerShell script that allows the attacker to create a backdoor as well as download and execute other threats. The M3_Mini_Rat payload grants the attackers remote access, allowing them to conduct system reconnaissance.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and Espionage	-
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
Sponsor	The Sponsor backdoor, written in C++, collects host information and executes commands from a remote server. It uses Windows APIs to retrieve current usernames and collect system data such as operating system build and power source status, which is then sent to the command-and-control server through port 80.	Exploiting well-documented vulnerabilities	CVE-2021-26855
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, compromised systems and Espionage	Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINKS**
Charming Kitten			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
3AM Ransomware	'3AM,' a new ransomware outbreak, is a 64-bit executable written in the Rust computer language. It was recently discovered in a cyberattack carried out by a ransomware affiliate. When the encryption process begins, the 3AM ransomware disables numerous services on the infected system. It then appends the '.threeamtime' extension to the encrypted files.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		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
JSSLoader (aka Anunak)	JSSLoader is a remote access Trojan (RAT) with .NET and C++ variations that the threat actors have used since at least 2020. The JSSLoader malware provides access to ransomware-as-a-service (RaaS). When JavaScript is launched, a JSSLoader variation DLL is dropped.	Spearphishing Link	CVE-2023-21715
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	Microsoft Teams
ASSOCIATED ACTOR			**PATCH LINKS**
Storm-0324			https://msrc.microsoft.com/update-guide/en-us/advisory/CVE-2023-21715

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ShadowPad	ShadowPad is a sophisticated modular trojan malware that has been used for cyber espionage campaigns since at least 2015. It is believed to be the successor to the PlugX malware platform and is known to be used by a number of Chinese state-sponsored threat groups, including Redfly.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Redfly			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Packerloader	Packerloader is a sophisticated malware loader that evades detection by decrypting and executing a payload file, often running it directly from memory for added stealth.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		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
HTTPSnoop	HTTPSnoop malware is a backdoor that enables threat actors to listen to incoming requests for specific URLs and execute that content on the infected endpoint. HTTPSnoop uses low-level Windows APIs to monitor HTTP(S) traffic on an infected device for specific URLs	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Disruption of operations	-
ASSOCIATED ACTOR			**PATCH LINK**
ShroudedSnooper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PipeSnoop	PipeSnoop malware is a backdoor that enables threat actors to execute arbitrary shellcode on an infected endpoint through Windows IPC (Inter-Process Communication) pipes. It was first discovered in 2023 and has been used to target telecommunications service providers in the Middle East.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, Disruption of operations	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ShroudedSnooper			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Snatch ransomware	Snatch ransomware is a ransomware-as-a-service (RaaS) variant that was first discovered in 2018. It is known for its ability to reboot devices into Safe Mode, where many security protections are disabled, before encrypting files.	Ransomware-as-a-service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		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.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>SprySOCKS Backdoor</td><td rowspan="6">SprySOCKS is a Linux-targeted backdoor malware that was first observed in September 2023. It is believed to be the work of the China-linked threat actor group Earth Lusca, which has been targeting government agencies and other organizations around the world since at least 2021.</td><td>Exploiting CVEs</td><td>CVE-2022-40684
CVE-2021-22205
CVE-2019-18935
CVE-2019-9670
CVE-2021-34473
CVE-2021-34523
CVE-2021-31207</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Backdoor</td><td rowspan="3">Data Steal and compromised systems</td><td>FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>Earth Lusca</td><td>https://fortiguard.com/psirt/FG-IR-22-377;
https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json;
https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization;
https://wiki.zimbra.com/wiki/Security_Center;
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-2021-31207</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VenomRAT	VenomRAT is a remote access trojan (RAT) malware that is used to steal data and take control of infected devices. It is a highly sophisticated malware that is difficult to detect and remove.	Phishing emails	CVE-2023-25157 CVE-2023-40477
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d; https://www.winrar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LuaDream	LuaDream is a sophisticated malware that is difficult to detect and remove. It is written in Lua, a lightweight programming language that is not commonly used for malware development.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Sandman APT			-

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
RedLine Stealer	A new variant of RedLine Stealer is being distributed as a batch script. This latest variant is more sophisticated and employs a number of techniques to evade detection. Notably, the malware is highly obfuscated, uses multiple encryption layers, and uses different techniques to hide its presence on the victim's system, including creating hidden files and folders.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information stealer		Data Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Deadglyph Backdoor	Deadglyph backdoor's architecture is unusual as it consists of cooperating components one a native x64 binary, the other a .NET assembly. The backdoor has a range of counter-detection mechanisms	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Stealth Falcon			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ZenRAT	ZenRAT is a new malware distributed through fake Bitwarden password manager installers, primarily targeting Windows users. It operates as a modular remote access trojan (RAT) with information-stealing capabilities.	SEO poisoning, adware bundles, or email-based attacks.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Stealth Falcon			-

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
Bisonal	Bisonal is a long-running customized backdoor that, because of its ad ded capability, is likely meant to be used as a fol low-up malware family loaded after i nitial access is established. Bisonal has been spotted assistin g with the TAG-74 infrastructure.	Visual Basic Script backdoor	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
TAG-74			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ReVBShell	TAG-74 utilizes social engineering attacks, employing Microsoft Compiled HTML Help (CHM) files as lures. These CHM files are used to deliver a modified version of an open-source Visual Basic Script backdoor known as "ReVBShell." ReVBShell is configured to enter a sleep mode for a specified duration, a command that can be issued remotely and edited as needed from a server.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
TAG-74			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DangerAds	DangerAds, which functions as a loader. This loader's purpose is to check the host environment and execute the shellcode that loads an x86 or x64 DLL program into memory and initiates the deployment of the final payload AtlasAgent.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
AtlasCross			-

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
AtlasAgent	AtlasAgent used in this attack activity is a Trojan horse program developed by AtlasCross. The AtlasAgent Trojan is a DLL program written in C++. Then, the AtlasAgent will decrypt the CnC domain name and connect to the CnC	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Information Theft and Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
AtlasCross			-

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
Smishing Triad	China	Financial Services, Retail, E-commerce, Postal and Delivery Services, Technology, Telecommunications	United States, United Kingdom, Poland, Sweden, Italy, Indonesia, Japan
	MOTIVE		
	Information theft and Financial fraud		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0005:Defense Evasion, TA0006:Credential Access, TA0042:Resource Development, TA0040:Impact, TA0043:Reconnaissance, TA0001:Initial Access, TA0002:Execution, T1588:Obtain Capabilities, T1589.001:Credentials , T1589:Gather Victim Identity Information , T1598:Phishing for Information , T1036:Masquerading, T1078:Valid Accounts, T1586:Compromise Accounts,			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Storm-0324 (aka DEV-0324)	Unknown	IT, Technology, High-Tech	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-21715	JSSLoader	Microsoft Teams
TTPs			
T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1204: User Execution; T1204.001: Malicious Link; T1203: Exploitation for Client Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Charming Kitten (aka Ballistic Bobcat, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, Charming Kitten, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, MintSandstorm)	Iran	Automotive, Communications, Engineering, Financial Services, Healthcare, Insurance, Law, Manufacturing, Retail, Technology, Telecommunications, Research, Education, Government, Media, and Pharmaceuticals	Brazil, the Middle East, and the United States.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-26855	Sponsor Backdoor	Microsoft Exchange Server
TTPs			
T1595: Active Scanning; T1587.001: Malware; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1059.003: Windows Command Shell; T1569.002: Service Execution; T1543.003: Windows Service; T1078.003: Local Accounts; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1555.003: Credentials from Web Browsers; T1018: Remote System Discovery; T1001: Data Obfuscation			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT 33 (aka Peach Sandstorm, Elfin, Magnallium, Holmium, ATK 35, Refined Kitten, TA451, Cobalt Trinity)	Iran	Aviation, construction, defense, education, energy, financial services, healthcare, government, satellite, pharmaceutical sector, and telecommunications sectors	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022- 47966 CVE-2022- 26134	-	-

TTPs
TA0001 Initial Access; TA0003 Persistence; TA0008 Lateral Movement; TA0011 Command and Control; TA0043 Reconnaissance; TA0002 Execution; TA0006 Credential Access; TA0004 Privilege Escalation; TA0042 Resource Development; T1589 Gather Victim Identity Information; T1589.001 Credentials; T1078 Valid Accounts; T1572 Protocol Tunneling; T1651 Cloud Administration Command; T1098 Account Manipulation; T1203 Exploitation for Client Execution; T1021 Remote Services; T1110 Brute Force; T1110.003 Password Spraying; T1574 Hijack Execution Flow; T1574.002 DLL Side-Loading; T1072 Software Deployment Tools; T1574.001 DLL Search Order Hijacking; T1105 Ingress Tool Transfer; T1588 Obtain Capabilities; T1588.006 Vulnerabilities; T1588.005 Exploits

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Redfly	China	Critical Infrastructure	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ShadowPad, Packerloader	-
TTPs			
TA0001 Initial Access; TA0003 Persistence; TA0008 Lateral Movement; TA0011 Command and Control; TA0043 Reconnaissance; TA0002 Execution; TA0006 Credential Access; TA0004 Privilege Escalation; TA0042 Resource Development; T1584: Compromise Infrastructure; T1036: Masquerading ; T1027: Obfuscated Files or Information; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1486: Data Encrypted for Impact; T1140: Deobfuscate/Decode Files or Information; T1012: Query Registry; T1573.001: Symmetric Cryptography ; T1573: Encrypted Channel ; T1055.001: Dynamic-link Library Injection ; T1055: Process Injection; T1056.001: Keylogging ; T1056: Input Capture ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow; T1059.001: PowerShell			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ShroudedSnooper	Unknown	Telecommunications	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	HTTPSnoop and PipeSnoop	-
TTPs			
TA0001: Initial Access, TA0042: Resource Development, TA0005: Defense Evasion, TA0002: Execution, TA0004: Privilege Escalation, TA0011: Command and Control , T1059: Command and Scripting Interpreter, T1584: Compromise Infrastructure, T1036: Masquerading, T1574.001: DLL Search Order Hijacking, T1190: Exploit Public-Facing Application, T1106: Native API, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information,			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Earth Lusca (aka Bronze University, Charcoal Typhoon, Red Scylla)</td><td>China</td><td rowspan="3">Asia, the Balkans, and a few scattered regions in Latin</td><td rowspan="3">Casinos And Gambling, Technology, Education, Government, Media, Telecommunications, Foreign Affairs, Human Rights, Political Organizations and Cryptocurrency Trading Platforms</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2022-40684
CVE-2021-22205
CVE-2019-18935
CVE-2019-9670
CVE-2021-34473
CVE-2021-34523
CVE-2021-31207</td><td>SprySOCKS Backdoor</td><td>FortiOS, FortiProxy, FortiSwitchManager, GitLab CE/EE, TELERIK.WEB.UI.DLL, Zimbra Collaboration Suite, Microsoft Exchange Server, Confluence Server and Confluence Data Center</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1595.002: Vulnerability Scanning, T1584.004: Server, T1543: Create or Modify: System Process, T1055: Process Injection, T1570: Lateral Tool Transfer, T1112: Modify Registry, T1588.001: Malware, T1007: System Service Discovery, T1560: Archive Collected Data</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Sandman APT	China	Critical Infrastructure	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ShadowPad, Packerloader	-

TTPs
T1584: Compromise Infrastructure; T1036: Masquerading ; T1027: Obfuscated Files or Information; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1486: Data Encrypted for Impact; T1140: Deobfuscate/Decode Files or Information; T1012: Query Registry; T1573.001: Symmetric Cryptography ; T1573: Encrypted Channel ; T1055.001: Dynamic-link Library Injection ; T1055: Process Injection; T1056.001: Keylogging ; T1056: Input Capture ; T1574.002: DLL Side-Loading ; T1574: Hijack Execution Flow; T1059.001: PowerShell

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TAG-74	China	South Korea, Japan, and Russia	Academic, aerospace, defense, government, military, and political organizations
	MOTIVE		
	Cyber-espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Bisonal and ReVBShell	-

TTPs
T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1218: System Binary Proxy Execution; T1218.001: Compiled HTML File; T1480: Execution Guardrails; T1518: Software Discovery; T1518.001: Security Software Discovery; T1132: Data Encoding; T1132.001: Standard Encoding; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1041:Exfiltration Over C2 Channel

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

Stealth Falcon (aka FruityArmor, Project Raven)</td><td>UAE</td><td rowspan="3">Media, Civil Society, Human Rights, Government, Politics, and Nonprofits</td><td rowspan="3">Middle East</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td rowspan="2"></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Deadglyph Backdoor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1583.001: Domains; T1583.003: Virtual Private Server; T1587.001: Malware; T1588.003: Code Signing Certificates; T1047: Windows Management Instrumentation; T1059.003: Windows Command Shell; T1106: Native API; T1204.002: Malicious File; T1546.003: Windows Management Instrumentation Event Subscription; T1027: Obfuscated Files or Information; T1070.004: File Deletion; T1112: Modify Registry; T1134: Access Token Manipulation; T1140: Deobfuscate/Decode Files or Information; T1218.011: Rundll32; T1480.001: Environmental Keying; T1562.001: Disable or Modify Tools; T1620: Reflective Code Loading; T1007: System Service Discovery; T1012: Query Registry; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1518.001: Security Software Discovery; T1005: Data from Local System; T1071.001: Web Protocols; T1090: Proxy; T1573.001: Symmetric Cryptography; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda)	China	Government, industrial, technology, media, electronics, telecommunication, military	U.S. and East Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows, Linux, and FreeBSD
TTPs			
T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1199: Trusted Relationship; T1205: Traffic Signaling; T1542.004: ROMMONkit; T1112: Modify Registry; T1562: Impair Defenses; T1562.003: Impair Command History Logging; T1601.001: Patch System Image; T1021.001: Remote Desktop Protocol; T1021.004: SSH; T1071.002: File Transfer Protocols; T1090: Proxy			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 AtlasCross	Unknown	Healthcare	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	DangerAds and AtlasAgent	-
TTPs			
T1053: Scheduled Task/Job; T1055: Process Injection; T1620: Reflective Code Loading; T1001: Data Obfuscation; T1027: Obfuscated Files or Information; T1027.005: Indicator Removal from Tools; T1134: Access Token Manipulation; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1497: Virtualization/Sandbox Evasion; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1016: System Network Configuration Discovery; T1583: Acquire Infrastructure; T1518: Software Discovery; T1105: Ingress Tool Transfer; T1573: Encrypted Channel; T1082: System Information Discovery			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1591: Gather Victim Org Information	
	T1598: Phishing for Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.005: Exploits
		T1588.006: Vulnerabilities
		T1588.002: Tool
		T1588.003: Code Signing Certificates
		T1588.001: Malware
	T1586: Compromise Accounts	
	T1583: Acquire Infrastructure	
	T1608: Stage Capabilities	T1608.006: SEO Poisoning
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
		T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.005: Botnet
		T1584.004: Server
TA0001: Initial Access	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
	T1133: External Remote Services	
TA0002: Execution	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.006: Python
		T1059.007: JavaScript
		T1059.005: Visual Basic
		T1059.008: Network Device CLI
		T1059.003: Windows Command Shell
		T1059.002: AppleScript
		T1059.001: PowerShell
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1203: Exploitation for Client Execution	
	T1047: Windows Management Instrumentation	
	T1609: Container Administration Command	
	T1129: Shared Modules	
	T1610: Deploy Container	

Tactic	Technique	Sub-technique
TA0002: Execution	T1199: Trusted Relationship	
	T1651: Cloud Administration Command	
	T1072: Software Deployment Tools	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.003: Malicious Image
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1136: Create Account	T1136.001: Local Account
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1505: Server Software Component	T1505.003: Web Shell
		T1505.001: SQL Stored Procedures
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1098: Account Manipulation	
	T1205: Traffic Signaling	
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.004: Network Device Authentication
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.003: Windows Management Instrumentation Event Subscription
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1542: Pre-OS Boot	T1542.004: ROMMONkit
	T1137: Office Application Startup	
TA0004: Privilege Escalation	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
	T1055: Process Injection	T1055.013: Process Doppelgänging
		T1055.001: Dynamic-link Library Injection
		T1055.011: Extra Window Memory Injection
		T1055.012: Process Hollowing
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1068: Exploitation for Privilege Escalation	
	T1548: Abuse Elevation Control Mechanism	
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1134: Access Token Manipulation	
	T1546: Event Triggered Execution	T1546.003: Windows Management Instrumentation Event Subscription
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.001: Binary Padding
		T1027.005: Indicator Removal from Tools
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1140: Deobfuscate/Decode Files or Information	
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.011: Rundll32
	T1055: Process Injection	T1055.013: Process Doppelgänging
		T1055.001: Dynamic-link Library Injection
		T1055.012: Process Hollowing
		T1055.011: Extra Window Memory Injection
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1112: Modify Registry	T1601.001: Patch System Image
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.009: Safe Mode Boot
		T1562.003: Impair Command History Logging
	T1070: Indicator Removal	T1070.006: Timestomp
		T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1556: Modify Authentication Process	T1556.004: Network Device Authentication
	T1542: Pre-OS Boot	T1542.004: ROMMONkit
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
	T1480: Execution Guardrails	T1480.001: Environmental Keying
		T1218.001: Compiled HTML File
	T1134: Access Token Manipulation	
	T1548: Abuse Elevation Control Mechanism	
	T1610: Deploy Container	
	T1205: Traffic Signaling	
	T1620: Reflective Code Loading	
TA0006: Credential Access	T1110: Brute Force	T1110.001: Password Guessing
		T1110.003: Password Spraying
	T1003: OS Credential Dumping	
	T1040: Network Sniffing	
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1056: Input Capture	T1056.001: Keylogging
	T1556: Modify Authentication Process	T1556.004: Network Device Authentication

Tactic	Technique	Sub-technique
TA0007: Discovery	T1083: File and Directory Discovery	
	T1018: Remote System Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1040: Network Sniffing	
	T1012: Query Registry	
	T1518: Software Discovery	
	T1016: System Network Configuration Discovery	
	T1007: System Service Discovery	
	T1087: Account Discovery	
	T1217: Browser Information Discovery	
	T1010: Application Window Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.004: SSH
	T1570: Lateral Tool Transfer	
	T1072: Software Deployment Tools	
TA0009: Collection	T1056: Input Capture	T1056.001: Keylogging
	T1074: Data Staged	
	T1005: Data from Local System	
	T1560: Archive Collected Data	
	T1113: Screen Capture	
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
	T1105: Ingress Tool Transfer	
	T1001: Data Obfuscation	
	T1219: Remote Access Software	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1102: Web Service	
	T1090: Proxy	
	T1205: Traffic Signaling	
	T1571: Non-Standard Port	
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1132: Data Encoding	T1132.001: Standard Encoding
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0040: Impact	T1499: Endpoint Denial of Service	
	T1486: Data Encrypted for Impact	
	T1496: Resource Hijacking	
	T1490: Inhibit System Recovery	

Top 5 Takeaways

#1 In **September**, there were **eighteen** zero-day vulnerabilities, among them the **'Five Celebrity Vulnerabilities**,' which featured the '**ThemeBleed**' flaw in Windows 11.

#2 Throughout the month, ransomware strains including **FreeWorld, Akira, 3AM, and Snatch** actively targeted victims.

#3 Numerous malware families have been observed targeting victims in the wild. These include **IDAT Loader, StealC, Lumma, Amadey, SprySOCKS Backdoor, and SuperBear RAT.**

#4 There were a total of **12** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: **Technology, Telecommunication, Media, Government, and Education.**

#5 Finally, **Earth Lusca** APT's 'Sneaky Moves' exploited **nine** vulnerabilities to unleash the new Linux **SprySOCKS Backdoor** targeting regions across **Asia, a** few scattered regions in **Latin American** and **African** countries.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **32 significant vulnerabilities** and block the indicators related to the **12 active threat actors, 33 active malware,** and **171 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 **32 significant vulnerabilities**

• Testing the efficacy of their security controls by simulating the attacks related to **12 active threat actors, 33 active malware**, and **171 potential MITRE TTPs** in Breach and Attack Simulation(BAS).

Hive Pro Threat Advisories (SEPTEMBER 2023)

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

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

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

Appendix

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

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

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

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

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

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LummaC Stealer	MD5	507bddfabd74a3d024b2ad5f67d666ea
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock
Amadey Bot	MD5	952d825a264745bb52b6977ba5983568
	SHA1	627a0a841c2fe194dd54f9ec6b0c1231d7da135f
	SHA256	d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c,
	SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d
	URLS	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe
SuperBear RAT	SHA256	282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb
FreeWorld	SHA256	75975B0C890F804DAB19F68D7072F8C04C5FE5162D2A4199448FC0E1AD03690B

Attack Name	TYPE	VALUE
Chae$ 4	SHA256	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395dd cf7d134a, 628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac 372a57, 6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e 244898c
	Domains	4.q111[.]sbs, <day_domain>[.]mail89[.]us[.]to, <day_domain>[.]ns99[.]uk[.]ms
	IPv4	18.228.15[.]16, 18.229.122[.]137, 13.248.205[.]89, 13.248.185[.]41
	URLs	hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com, hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com
	WebSocket URLs	ws://54.233.147[.]24, ws://18.231.31[.]151, ws://18.229.170[.]213, ws://54.94.248.[]242, ws://18.231.70[.]213, ws://18.231.91[.]245, ws://18.230.36[.]203, ws://54.232.236[.]117
DreamBus Bot	SHA256	1d0c3e35324273ffeb434f929f834b59dcc6cdd24e9204abd32cc0abefd9f047, 1c49d7da416474135cd35a9166f2de0f8775f21a27cd47d28be48a2ce580d58d, 601a2ff4a7244ed41dda1c1fc71b10d3cfefa34e2ef8ba71598f41f73c031443, 153b0d0916bd3150c5d4ab3e14688140b34fdd34caac725533adef8f4ab621e2, e71caf456b73dade7c65662ab5cf55e02963ee3f2bfb47e5cffc1b36c0844b4d, 9f740c9042a7c3c03181d315d47986674c50c2fca956915318d7ca9d2a086b7f, 371319cd17a1ab2d3fb2c79685c3814dc24d67ced3e2f7663806e8960ff9334c,

Attack Name	TYPE	VALUE
DreamBus Bot	SHA256	21a9f094eb65256e0ea2adb5b43a85f5abfbfdf45f855daab3eb6749c6e69417, 0a8779a427aba59a66338d85e28f007c6109c23d6b0a6bd4b251bf0f543a029f
DuckTail	Domains	marketingagency[.]social, a1outreach[.]software, mangogroup[.]sale, la-roche-posay[.]click, li-ning[.]agency, li-ning[.]news, hrm[.]social, hrms[.]social, mccann[.]fyi, avalonorganics[.]work, li-ningagency[.]news, li-ningjod[.]news, ogilvy[.]social, narscosmetics[.]social, yodo1game[.]software, louisvuitton-social[.]news, luoisviitton[.]news, eucerin[.]work, guessinc[.]work, samsungagency[.]link, brandresource[.]social, recruiterofbrand[.]social, brandrecruitment[.]social, hrmmarketing[.]link, marketingmanager[.]social, recruitmentagency[.]social, marketing-project[.]social, nike-agency[.]link, recuiter[.]company, louisvuitton-agency[.]link, louisvuitton-agencyjod[.]live, mccann[.]expert, ogilvysocial[.]company, louisvuitton-hr[.]news, louisvuitton-jod[.]chat, hyundaimotorjob[.]social, hyundaimotor[.]social, hyundaimotorgroup[.]social, adplexity[.]site, adplexitydesk[.]tech, fbadsguide[.]tech, affiliateguide[.]tech, newguide[.]tech,

Attack Name	TYPE	VALUE
DuckTail	Domains	businessmanagerads[.]tech, businessmanager-update[.]info, marketing-tool[.]info, connectads[.]agency, disruptiveadvertising[.]agency, impressionagency[.]co, themars[.]social, ommmarketing[.]agency, growmemarketing[.]agency, ommmarketing[.]digital, impressiondigitals[.]agency, impressiondigital[.]info, passions[.]agency, brandstyle[.]agency, brandstyle[.]digital
	SHA1	92a7ac122ab87ccfd19224b2be89fd7bbee6d0b1, C8d5b988464e7e49b932a01d3b75e192fc7a0026, 27ac50a5f2751429eed99fd4abff73c2129ba387, 2e1b5903131ad42591021919ac27beecd70c9253, Ce5f839cb8a3473330256ed72c144f689ad3c55d, B14deb48c60771fb05cddf6a16ea9fc4e56ac6be, 1b07ce1f47ba6b19087499fa4ba2e93beac227c4
	SHA256	740fd780b2b45c08d1abb45cddc6d1017c9fcc6bcce54fd8415d87a80d328ff6, d93c40de3e43ec58b115e5590c98ef62de15df9b706ef6d4a06d022fa874bb48, aaf44bce6a5a2ab5b7f3f75f8238d6abe46f9fd2f2e2a2b2672ba6e52f4d5754, 4f43c031ff415fcb2f6865e98e91eaf611eb6a576acfe3250b57dc5e47a7d34f, f433fc47b9ccd66aa80196e04a4e4bf54fe3d1c689e4b5d5bcdf86017c3f8abe, a5026e7a88c3b833ee3678944d003fdfe51f86d44515c470dd2c8aa62e0fd0d2, 4759cb5a37f2c8661c3817206b4d34d65825d80526ce41461f6c11ea56289ff3, 4c546c259cbbf0daf1d0aa00d3385a1ea9e74b6fb2e3692ef44e1da27ba30abc, 71a89855974dcd69f3547632368f2ce8cfa490ee96b514d832f04cc22923f143, a6decb34e5688f543e541dbc79e6884ace29c93d7fc43716eb32204cb3c0003e, 59caef212349c6423e1fc581aaf76ab735269990bb7dc8e193e2877957c71e91, 1000d705806b940af52b54cba98261b64ed658a355e0922d64551c5acb7f1a40,

Attack Name	TYPE	VALUE
DuckTail	SHA256	47f9122f0a25f4909795ede9bb4458495ae70fa2657745ec7c47ee172e040209, 52e295073d2114c0683d95c8d323bddc95baa5c68f8362ebcc81124a06e42672, 6e797da70db98e1f8fb5a7cf794b8a8e90549e8915f4d04f510690ae23aeb505, 25b427a06608ebfc48c778829427a732c17986c64345acf35e92d03ccb126b8f, d3633c2372b67db37b11de741bfa676a425322c5208b8396c62983aed88d2bcc, 600a498e55512723074b6f5a952ffd38b249c30117e9eaafcccda4fd1a0c1e75, e74f131d1e5ed725383ee5b89ec1216c642fbd77928dafd991b406a7f59251b6, 469bcbd18e2b5d4ca15f449d43c13656758503fcc4042a05721ef5f3c35345e2, dec248f011c1f945f590bb5aeefbbcb41bdaa6c665625a594f8b315f014ea4bb, e8d5af5ebff12d0cbb8b1cd70f149a8234b993facc32b3808fc7db94f2bf80a9, 7952eb4832bfe5155e2f37abb68d552ed8f2f426715f2bc65eae5a69f1f28d87, 7c6b1a349ad96d8368e1f9742992f764a7de32e9c078709372210a88a721c532, 7eb994eaa7be9dcfb37bdfd7c8bec1dc8b90e3ec4aa86de6e6125c97eeb64426, af75e8c1f3229868d41b141165714c56baf38f3f49c8c014c4fa18bc934720bf, 6688e027e837f8e86dbbe40e2e663e72a1b7e977ae25d1157ecd8793d947f0c7, 7d15d3cdc41cc0c3452a538ed3bf8e0dbc9a0cbd4bbca453a293287e240dfff8, b83059cc733ad4af37a15a24222b09be3ee02af3964bc62ae5de6354cd85f65b, 61953e2d6e80fca18173bd3ce695274c5a25db449ac32addd8ee5b0ac29efa02, f17d2acb4c1bd0332b3c0cdba83001b82fd96d62d5bf829ae1e409902195b038, 1092ab1743ca59c29bee69d73918ee78e2195fafa232a16ba790429d39dc9083, 1e6ff886f386afbbcf8dc175bd1fbdfd8079448f1cb5a546352d7065c5fa5e7b, a81cbb9871f692350bf21d07b9acc233268df233b79c311a482d9783eb9bd539, d7f4372daf2729c956ce63e0ba2b7149f1bae03da7fbae486bbcfb0bda0f8d70,

Attack Name	TYPE	VALUE
DuckTail	SHA256	3f9300d5d84482010bce08e9cc7b0a5b605086dc4143e8470e9e23ef14f0c27f, e2a343dfa801882625c264f944f89665319ea9b3a2793ec47a02bb4a126f5e15, 8cf5a4d0b6848604c338ad2d8bde8ceab2e86fff0d65e777bc574025f26bad73, 994039645f60d5fc9621cb10826b7583c83667827c195b3fa9d875a8ee50b170, c9c5409e6327f2f443dfa3cb6ffa527b291a34a572c14e93b65205fd305f4ff1, 83126452e240cdebbfaabeda58dcb4ea68f1e9836596e6032119592b4057ca4e, 7395aa619010fee65ef640f46023be5732188df36079e13f023aa2dc69602e21, a09f560a1ddbc7c60695d5651cff0ae0f0911399cb5146bb531caccb4d14089e, 34392151e58955b0bd7eb70a90499127ec5810a8488c2ae5bd4da1f9167a7762, 9d24436f652abe1df6319fbfa0a5468f1061e280d41fb00a60265d6c2aa7871d, 8c87c2d7f3932fa6661daf8fbf058ab4b721d0d6fe0849da30ae695b61d3ddc2, f47a002d93df2190e47e7026663bea34ea0299a4afe2810b8cb45b51bf330a8b, 6578a3dfaa2c59443b02581c0097e8c356babcb388c4ab48ef651c90c262e9e7, 4a56e4a753a5fa615aec4f80eb842ea2f089bd439e93ecf406f8433e97b659e8, a8196b3995bfbc62ec073dd35377a5412db30e9070ab72743694cceaddd2495c, 958ff188086e33caf119347ef7d81a99716e83bc688ed1ada1ad25feab7088b9, 697307235b627a33f4308a14dda9c1f33e38c9efb572026320bca453f6301b0a, b0968ac6489e7f2122ef2deafbc5a5f5968451918a8023c7aa8ded7171264ba4, 625b5b3f5bc9e1fce5486812051b187975210a46bc2d9a712e9ef9ae5c68f09c, d6c18d9efcbb6ce7292c4d6bdba70a64acca10561b66fd88e9e47cb9c7b63392, 4089277eff9f088684f53697c2f5615dcf4c940c1693d9d8c85a7de47dce7161, ce1f6a00bf9f79ffe879c2e7ef40166ecacbe6a17a382544648f0f25c5c4177b, 2c9824d0faff9a0485c36546ac7884697d1773bd221c2586ae9ddb0e54208731,

Attack Name	TYPE	VALUE
DuckTail	SHA256	a99fa349faabd5773816c53a11b67a7be95f277b622ebe93c1ca3625500b8384, 1fcbf708854f7ebf93726d5dd08c08648e84aee0a33a618a29c7e50df09e12d5, cd8b9cc35064b76df01ba5ce7536fd8b60dc773e32889ceca95f586112b6f3c5, 044eba497f9259d18a3ea593de3fc39c6123805ce485cf4a193083f9e0b74bb7, e81db61004834afb0dbf47db128942e3353774764466fb9269e88a553e6dfc33, ee5dcf9b070e19b87842e5c9ce3548bb1507e41d7aad272ae697afcd9f3ab7c2, 7af6cbfd7d1e7fe2f8c8c0382ee43860ec2cbe25ca845588981263ff8144f236, a30548fa4058d1309d4d75dd2dc36a492c503168f4d1c2f6c52cce57069629cc, fc8c250c2346e5440e249942eb8fe7c8b9b7d8d013f275c5fae2ae142ac50171, 8db1a51d514811057d29ddda85858f52303999cebdeae25f88d05a39594afd3a, f7c015d65d4966936927ae5241ead77c9d167d749e97667a571d7439e652ffa3, a3c5cd4f1afbe10de154bf3f669479496ff2e93da660a849ff41c29d5f118a4a, 9ef977e0403f9dff5cebe3935402d7a776ca3c9a79618e4d6992d3754051f603, d6c7c6a9098769b015802a278eb81bc7b72b08c5e18534ac71f01394a95c1f28, 647793166e03397bb1c30f0935330bcabc9f2f0f4ba8d7a821fc145237d96b2f, 300358895c7895c14949c80d7b4ef6fa50ec5027e65e4578d503c39f2bd6618e, e4bf8cfc1035f51020ff033b9366dd1fefef8ae5664e2fde6798831399c51d1d, c1e65ebb05c500b5ade389a2f880e9116b74b24782d9ea13955adab087194b43, 4874878056cebe9627bbf44a3bc977315d6e14492af855319103b99103241c5f, d26b0baa30cc13df88eca57ce22f651a744cf5683b8b62121b4292e1005527f7, d5939fc12c88264cb28ac867767e5492aa145f0499aeaaa83cdaca8b15da07ee, 507376fa684f17508a195426d933e0e2ef92028d5956ed66cba825b6ce61df8e, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df,

Attack Name	TYPE	VALUE
DuckTail	SHA256	a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, 51abe6d7196e93c4264ff508a11611b871bb1c9d96df2086efe84dd48af96cc2, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 07d5d4721c3ed9a860dc10d25f226dd81a83602023c63310f9634b8dd704e7f8, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c, 161d081e9ba94ee1749c3192888702f6a25e8e2fb59b9d1f9d989ffc885566a6, 80160fd48ba4d174ccd1d2d8e72afc3674c1ce7c73ef18d3e372a6d68e6b3227, a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, 8731ec7667084e649622e9f553e291b889eb0709c669545bd19f3ec0c2878687, de0a568803eb5b3d51eac593d2c9174e6fdef9a9ee11f222e5822ae3f182b5b0, a979cf0a2a44f2c23e01eb72cb72cbfadbae40bea38a3d390977d79bad610bc8, 40da0bc61a4ccf170f43981a7d908b0c3b541b1652cbb959b1ea9a87dd5944a7,

Attack Name	TYPE	VALUE
DuckTail	SHA256	d76260578caf24dbb6dd2d10c60b066d7659f5c21da8c998f34ab0f675d626d2, 5d9b287df9b9b3f019e8d5834f117200f0651ecd0988338fb395ef1382fabc26, cd5c66a206e92be1e7eb77d5cb69c63fc2acc9ffbfcf7031713c9fddca11b3e7, f4e9feb547dcd6a233f71c7ad57a0759a584ae94a9e822a64831ed26cb32ecf4, 0241555cc3e21a658c78cbe93ab75eaa4f978a013df22852ada57652a3a57b6a, cc5483d21c84ac73c410194205b529d6190b322b8da49577ee36ae9d8878c0c3
Agent Telsa	MD5	c1ac31ebcbfb8dc95d4eea6d4c95a474
	SHA1	e2437078fe7f3abd635dacae65cf6ae2d10ef98e
	SHA256	fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904 c22638, 36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda770282 0efcfc3a
	URL	hxxp://23[.]95.128.195/3355/chromium[.]exe
	File Name	Order 45232429.xls, dasHost.exe
Akira Ransomware	IPv4	161.35.92[.]242, 173.208.205[.]10, 185.157.162[.]21, 185.193.64[.]226, 149.93.239[.]176, 158.255.215[.]236, 95.181.150[.]173, 94.232.44[.]118, 194.28.112[.]157, 5.61.43[.]231, 5.183.253[.]129 45.80.107[.]220, 193.233.230[.]161, 149.57.12[.]131, 149.57.15[.]181, 193.233.228[.]183, 45.66.209[.]122,

Attack Name	TYPE	VALUE
Akira Ransomware	IPv4	95.181.148[.]101, 193.233.228[.]86, 176.124.201[.]200, 162.35.92[.]242, 144.217.86[.]109, 31.184.236[.]63, 31.184.236[.]71
	SHA256	1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488, 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50, 1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc, 9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163, d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959, 6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
HijackLoader	SHA256	7bd39678ac3452bf55359b44c5192b79412ce61a82cd72eef88f91aba5792ee6, 6b1621bded06b082f83c731319c9deb2fdf751a4cec1d1b2b00ab9e75f4c29ca, e67790b394f5238908fcc326a9db940b200d9b50cbb45f0bfa94038db50beeae, 693cace37b4b6fed2ca67906c7a4b1c11273110561a207a222aa4e62fb4a184a, 04c0a4f3b5f787a0c9fa8f6d8ef19e01097185dd1f2ba40ae4bbbeca9c3a1c72
	URLs	hxxps://www.4sync[.]com/web/directDownload/KFtZysVO/4jBKM7R0.baa89a7b43a7b73227f22ae561718f7f, hxxps://geupdate-service[.]bond/img/3344379399.png
PhoenixMiner	SHA256	3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3, c7e1aa53dc667581f37bcbd0793c2ef909e8a4461c59641cb2c672ebe192609c,

Attack Name	TYPE	VALUE
PhoenixMiner	SHA256	201a1979e02bcaa2808e31613a0bef99ad55d514fcaed973840a1bf1efdb4cbe, f4b1dc6456aed765e11878c6a5b9555ee2aec1737219137d187e480599e254c9, d241ef2a157f44dcc323279bd89168c0f6b142de964815ceb0429181eae9a789
lolMiner	SHA256	2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73, aafe94fe2ca6210fde8f5691c066dc128090b097a7d45a69d7ccc977891e08b4, 8ebe85fd149f9b1e93668a733182ad6e0cafd1a0b285800e4e6b226b8673cbaa, ac1af3a386b2dcf0e2a2955101dc91de7f5e62c900ba4476b0b842d1aa951bbe, 2c049deedbc83923abdd41580faa07c98037f09b5fabe98f97a9239a0b6e3542
M3_Mini_Rat	SHA256	7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08
Sponsor Backdoor	SHA1	098b9a6ce722311553e1d8ac5849ba1dc5834c52, 5aee3c957056a8640041abc108d0b8a3d7a02ebd, 764eb6ca3752576c182fc19cff3e86c38dd51475, 2f3eda9d788a35f4c467b63860e73c3b010529cc, e443dc53284537513c00818392e569c79328f56f, c4bc1a5a02f8ac3cf642880dc1fc3b1e46e4da61, 39ae8ba8c5280a09ba638df4c9d64ac0f3f706b6, a200be662cdc0ece2a2c8fc4dbbc8c574d31848a, 5d60c8507ac9b840a13ffdf19e3315a3e14de66a, 50cfb3cf1a0fe5ec2264ace53f96fadfe99cc617, 1aae62acee3c04a6728f9edc3756fabd6e342252, 519ca93366f1b1d71052c6ce140f5c80ce885181, 4709827c7a95012ab970bf651ed5183083366c79, 99c7b5827df89b4fafc2b565abed97c58a3c65b8, e52aa118a59502790a4dd6625854bd93c0deaf27
	File Path	%SYSTEMDRIVE%\inetpub\wwwroot\aspnet_client\, %USERPROFILE%\AppData\Local\Temp\file\, %USERPROFILE%\AppData\Local\Temp\2\low\, %USERPROFILE%\Desktop\, %USERPROFILE%\Downloads\a\, %WINDIR%\, %WINDIR%\INF\MSExchange Delivery DSN\, %WINDIR%\Tasks\, %WINDIR%\Temp\%WINDIR%\Temp\crashpad\1\Files
	IPv4	162.55.137[.]20, 37.120.222[.]168, 198.144.189[.]74, 5.255.97[.]172

Attack Name	TYPE	VALUE
3AM Ransomware	IPv4	185.202.0[.]111, 212.18.104[.]6, 85.159.229[.]62
	SHA256	079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22, 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e, 680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4, 991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af, Ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc
JSSLoader	SHA256	67a1328242c89b2f54018d31eca071ab7edef6df30fea2633ad1a013aa5feb8a, 2373a6a7223154a2e4e3e84e4bdda0d5a9bc22580caf4f418dae5637efec65e5, 1f2ab2226f13be64feeece1884eaa46e46c097bb79b703f7d622d8ff1a91b938, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, c1e7d6ec47169ffb1118c4be5ecb492cd1ea34f3f3dd124500d337af3e980436, 15f15b643eafcc50777bed33eda25158c7f58f4dbaaaa511072ef913a302a8da, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0, 16f9674ea7c40a0e474966f59c413518509e295608c7ecc37c6096b034b88918, 2e3bc3b059733b4db846d3227abbfa6a7914b551f0175d6f77e22d08b57d49e3, a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 2df508247a4e739b086c9de47d91a26ea7aee4d5cf9bc5cc70b5ad2dc7f102c6, d2b080b9af5d39d72af149afb065e769b1da8005edfe84237942a1b99f4fa36c, 793aa21ed7432ef2b0eda8d80036361878f728dbc4081d72f80fa3694702a4d8, 35f5c781d61d398ce47a8881228346a81afb4915bf083518bf2b4cc8d6a2685b, db1d98e9cca11beea4cfd1bfbe097dffd9fc4cc8b1b02e781863658d8c6f16c7, 410cd107dfd37752936bd20d022ea614cd373aa9d37db255f65dc434e653236a, 3b6d61add64402dc74d237e69d701ad2b0bea9a525798a376cd13f2090bb39ee,

Attack Name	TYPE	VALUE
JSSLoader	SHA256	969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, ee8f394d9e192c453d47a0c57261a03921dcbb97248a67427cb6fc6d8833c8a0, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, c328f48c5f4a2c2441bcd0b0c0551547ca254f7ebbb46d30d357e962d8330063, 8279ce0eb52a9f5b5ab02322d1bb7cc9cb5b242b7359c3d4d754687069fcb7b8, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0
ShadowPad	SHA256	656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c, ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646, 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3, d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3
Packerloader	SHA256	32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a
SprySOCKS Backdoor	SHA256	6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc, f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912, eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
	Domains	lt76ux.confenos[.]shop, 2e6veme8xs.bmssystemg188[.]us
VenomRAT	SHA256	61dd71441a2b4955467243e986c38f1ea543bae7b1546f003c4a30074dd6c04e, cabc45f1dab04be3fc63192d98324d2665599a6d6ea2f0277ecd27a62fb694f3, 79b87d7accc9cbd1414b72ca13c48a385be9cb06c1bb53d845e94107b579bf62, 4b84283c40560991da34ef2b465a4724facd0932acebff60466d8d5ff1916bd5, 75c12ccacd764101736b213981355b39056227929214c8963e9bf3ea5a60f6ef, 1648bea3c1c3b00e7f9c9bf7f65be833fa7f291f0e05a342382e9e36f0350c60,

Attack Name	TYPE	VALUE
VenomRAT	SHA256	b23e4ea87917a517565de8471a101ab55c2a31186c8a23e9e8af71b359d35aa9, 65235e5bd2f9b30e2b272602a83a8f3805cfca50252da8a79e279f232a6d3990, ecc3971af558300b451a87b51d0324737174ea1993d8aa7424078fb1bd97ffb3, f9497f07d69b043501cc52bf2db7828abad35a14bd95bb05e6b5ab9e4408de4e, 48f61821feeaa45c53daaeb567e142ce9614d131dcf886506a31bf0ba2d75c45, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, f6ad1568aa318f7d27c41ce47b5b3a1a2aceb0fb470d7528117364b67463501e, d0e7f2c67877f06c0e8854b1a37f6f04d181537d77e242f46401415da17f9b03, 8ef5c7eaa352e547c2e0de266844122ab471cd2ac73a9388b4f1416b2ac8c840, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, d845bc06b40c5810390a226e0608090aa7ea67f603af8bbd4f00318102bb8b7d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, b9b75fe8ce464a4ae9c0578741718777da09646ea89f42ac3663cbf365681b3d, a9e8b6b187c3bbfccfec6266b95c079bf27752d22bcd04c97df8a62f4a6dcd59, 4c69911de167a507a1c6effb9724ab72ca0026d1fdfa9c747f70800abdbcbbe5, 9e8f792af1587b867f477863e2c19d7443f2926ba1e933cf073dcdc68a748dad, 78a11a10e8d26f98221c9981f1d35b91ce67714a044400fe9933756435b4b690, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1, 997a1ea14695bc0275446cd35e362ae48a4f3a6f108d91fea49ba1c83803edd1, 4694bd08ad1446ae0deb2ea6db86658930422cbef632e88ef7ab2218ff75e509, 35afd46abb89d050971ffc41a372e2f64046404783e33d896cb77a3b3855d2e0, 45c95edaadc2c82c1ce03f7e9d9a60be0361f6f964e845ac74fecf0403c1bfa3, 45c95edaadc2c82c1ce03f7e9d9a60be0361f6f964e845ac74fecf0403c1bfa3, e8c6798610293bad3d42472fcc5df23ce3498d91eb2f05cec76a9cd7c5248d29,

Attack Name	TYPE	VALUE
VenomRAT	SHA256	d0bd2f3e2c91bd604ed1d4604d65deff63d443c8abac736873edc085cfca002e, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 0a141bbe00db6f1f5626a3991bc5b3699c49a275f17a7c8a3825c06a5877fa19, 9f917ff3160a74ffe217d5941530753fbd1292a31141a0bc6d4e889bb58cb883, 9f917ff3160a74ffe217d5941530753fbd1292a31141a0bc6d4e889bb58cb883, e2ba06f64e174ff0daa92c39e13ca9a4b735c005d01b65a43a20b6af81f0068b, 0ea528ae0f3931379941f569ae55f0ec2c0714ccd1c2c36cc39e20ba58e11113, 96e560ca4abd5f6309f52eabdaffb87399aa91e70cc9f548c35753f8526206f3, a99b925b26f753b0da74d16c53161ada4f2048ceb28b81e2b532c8c840efd31b, bd5244f5beeb1ca343da306f4f2cf40a4d7aee3e60d75eda37823d61124b24d0, ac12768102db5b1943913955258737223 2c85e2237afe093f2cd7f75f876f155, ac12768102db5b1943913955258737223 2c85e2237afe093f2cd7f75f876f155, 8283f5942a09cefc09ede83ec97cea26ae094c41b4df2036844a7a5e51bdc4ae, e0b3ea9079e7606ef7575bedd5fc648c63b6d0e12b27d6c9dcbdc17d8a758e33, e0b3ea9079e7606ef7575bedd5fc648c63b6d0e12b27d6c9dcbdc17d8a758e33, Bb593c07ee6598e8ba0f941809a93be8c42051b03aecd2356ded08f35630871a
Snatch ransomware	SHA256	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd, 7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3, 28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c,

Attack Name	TYPE	VALUE
Snatch ransomware	SHA256	fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066, a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae, 6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0, 510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1, ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d, 2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57, 251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d, 3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924, 6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7, 84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5, a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84, b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40, 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d, 0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
	Emails	sn.tchnews.top@protonmail[.]me, funny385@swisscows[.]email, funny385@proton[.]me, russellrspeck@seznam[.]cz, russellrspeck@protonmail[.]com, Mailz13MoraleS@proton[.]me, datasto100@tutanota[.]com, snatch.vip@protonmail[.]com
	Domains	tutanota[.]com / tutamail[.]com / tuta[.]io, mail[.]fr, keemail[.]me, protonmail[.]com / proton[.]me, swisscows[.]email, sn.tchnews.top@protonmail[.]me
LuaDream	SHA1	1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4, 27894955aaf082a606337ebe29d263263be52154, 5302c39764922f17e4bc14f589fa45408f8a5089, 77e00e3067f23df10196412f231e80cec41c5253, b9ea189e2420a29978e4dc73d8d2fd801f6a0db2, fb1c6a23e8e0693194a365619b388b09155c2183, ff2802cdbc40d2ef3585357b7e6947d42b875884

Attack Name	TYPE	VALUE
LuaDream	File Paths	%ProgramData%\FaxConfig, %ProgramData%\FaxLib
	Domains	mode.encagil[.]com, ssl.explorecell[.]com
HTTPSnoop	SHA256	1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb, 7495c1ea421063845eb8f4599a1c17c105f700ca0671ca874c5aa5aef3764c1c, 3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7, 04cf425e57e7d511f03189749c8c0a95483eeeb4c423e9ee1a6a766d2fe0094c, c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0
PipeSnoop	SHA256	e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d, 9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb
RedLine Stealer	SHA256	ddb7185f7da4beef972a1188d55c722a924862eb97c2fd42e5bbbd8d9074055b, d8c681f4bde8e5a20849ec21389d6592229e995fbb0155952b93d7e792df7cca, de2949c25878b7849a5fe7e6f7820005ab07c370c4754a6284d11162573145bf, 8fb369b47a2e6046a68026aea6c6f1198dcc6bfe9418d0f75118d24d37a68abb, bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466, 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4, 6c5a4a8b7554000d5ab5221c43f25f093ba6a37c6b2511335e002f333c5af6c4, bf803adb5695fce143062e6f51980d46537167b7a9e0e85ad13a999e35bd0466, 9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0, 6cbe9be190f521408438262d0c7f2ccbfab32a6df558cec2a264285fdfffe5c2, 53af2c266c7f18e7c1ab16460d3c09d773fe93ac0a840fa83a30cc1020d1019a, 4f1c1565afc782e688945c07a486205c59d43a98ae577c5d065bfed9a47a983d, b5d8caa15cbf53d002edc6194abd0de43e4a139cc04f9703ae7bfc397bca66c8,

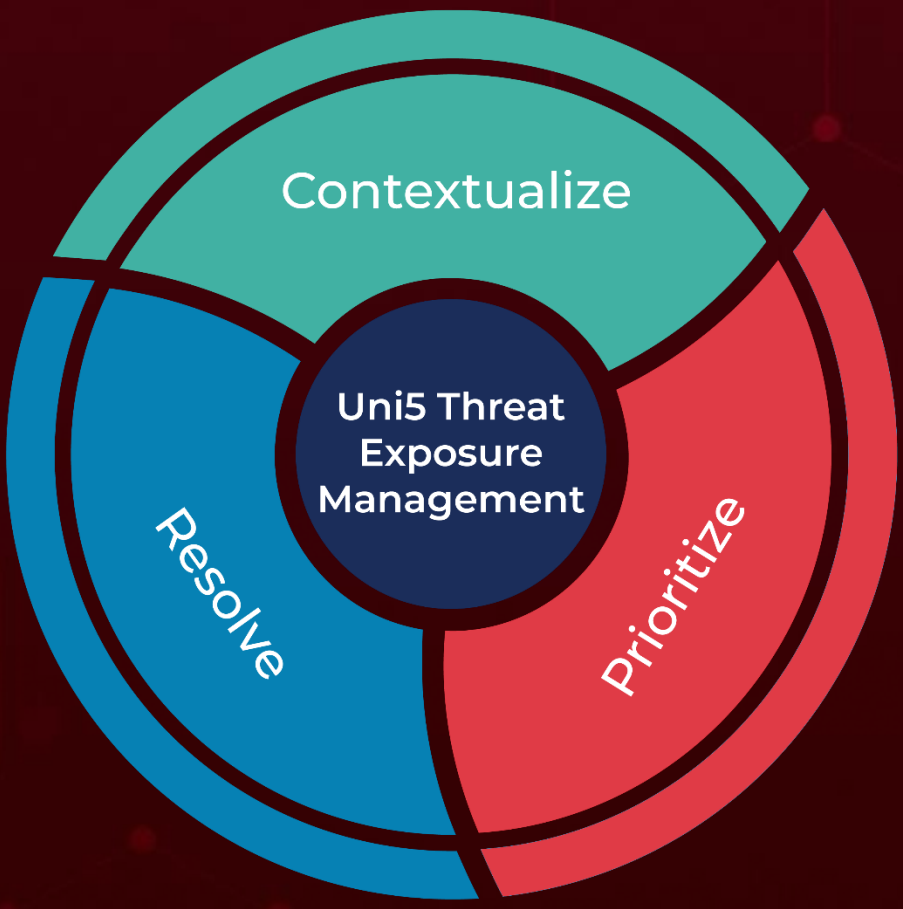
Attack Name	TYPE	VALUE
RedLine Stealer	SHA256	9bacf20a00f73124039c4476d600e70293ae60d1d1d28290a63000b510f313f0, 43328f774db70b98c4cbe83cc3be18de20a29b073b483eec49c64c6c301e4079, 1b5f1e505e57b9915418f251f9c2343302f0737bdd85126666db56a27f0142f2, b83e50fa2c5c54e027f3bfe859e2a69e883bbb0080fed20aca176f77ad120fa1
Deadglyph Backdoor	SHA1	c40f1f46d230a85f702daa38cfa18d60481ea6c2, 740d308565e215eb9b235cc5b720142428f540db, 1805568d8362a379af09fd70d3406c6b654f189f, 9cb373b2643c2b7f93862d2682a0d2150c7aec7e, f47cb40f6c2b303308d9d705f8cad707b9c39fa5, 3d4d9c9f2a5aceff9e45538f5ebe723acaf83e32, 3d2accea98dbdf95f0543b7c1e8a055020e74960, 4e3018e4fd27587bd1c566930ae24442769d16f0
	IPv4	135.125.78[.]187, 185.25.50[.]60
ZenRAT	SHA256	60098db9f251bca8d40bf6b19e3defa1b81ff3bdc13876766988429a2e922a06, 8378c6faf198f4182c55f85c494052a5288a6d7823de89914986b2352076bb12, 986aa8e20962b28971b3a5335ef46cf96c102fa828ae7486c2ac2137a0690b76, ba36d9d6e537a1c1ecdf1ace9f170a3a13c19e77f582a5cae5c928a341c1be8d, d7d59f7db946c7e77fed4b927b48ab015e5f3ea8e858d330930e9f7ac1276536, e0c067fc8e10a662c42926f6cdadfa5c6b8c90d5dff3f0e9f381210180d47d37, e318b2c1693bc771dfe9a66ee2cebcc2b426b01547bb0164d09d025467cb9ee3, f7573ad27ff407e84d3ebf173cbeaaa6aba62eb74b4b2b934bc0433df3d9e066
	Domains	bitwariden[.]com, crazygameis[.]com, geogebraa[.]com, obsploject[.]com
	IPv4:Port	185.156.72[.]8:9890, 185.186.72[.]14:9890
Bisonal	SHA256	11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd, 01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd, a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5,

Attack Name	TYPE	VALUE
Bisonal	SHA256	89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893becec1a9bc, 0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514
	File Name	SearchFilterHost.ex, msfltr32.exe, MySnake.EXE
	Domains	formsgle.freedynamicdns[.]net, satreci.bounceme[.]net, hanseo1.hopto[.]org, sarang.serveminecraft[.]net
ReVBShell	SHA256	aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71, 8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34, ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c, 465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c, 6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a, df7d584d56af6fcf3cca31ed0d3a4d34abd2c1019b8d223a230f8a78075a7d9a, 078a8026f32b8d05258285dc527408388c651f6c3eaebc45f8bb3f4b42248631
DangerAds	MD5	f8bafe2ce6f11a32109abbab1c42e2cf
	SHA256	9c2f990f2d23f380f1cf8f83e9e23749f7ef097bda5b530c7d43fbf5feb3ba99
AtlasAgent	MD5	ca48431273dfcd2bd025e55f2de30635, ba85467ceff628be8b4f0e2da2a5990c
	Domains	activequest[.]goautodial[.]com, ops-ca[.]mioying[.]com, app[.]basekwt[.]com, secure[.]poliigon[.]com, engage[.]adaptqe[.]com, chat[.]thedresscodeapp[.]com, superapi-staging[.]mlmprotec[.]com, search[.]allaccountingcareers[.]com, order[.]staging[.]photobookworldwide[.]com, crm[.]cardabel[.]com, public[.]pusulait[.]com

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

October 02, 2023 . 8:00 AM

More at www.hivepro.com