Date of Publication
January 11, 2024

Hive Pro®

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

DECEMBER 2023

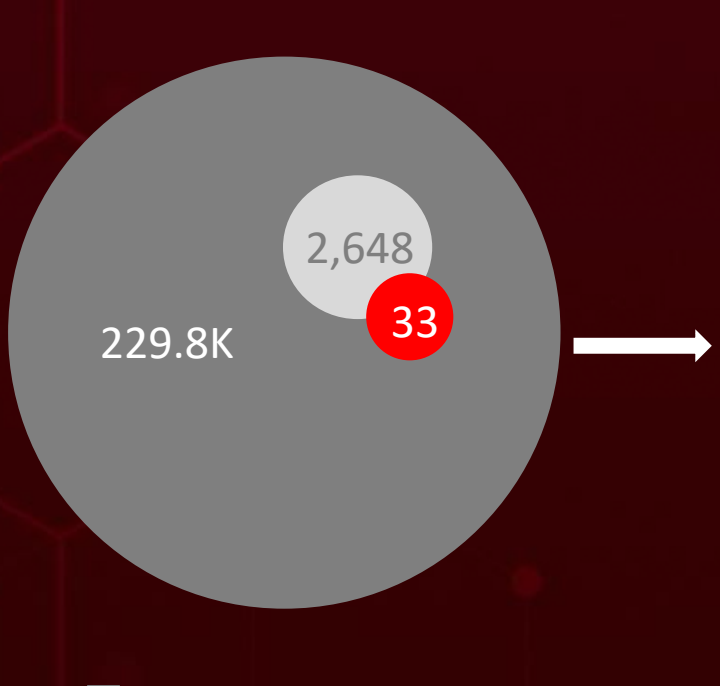
Table Of Contents

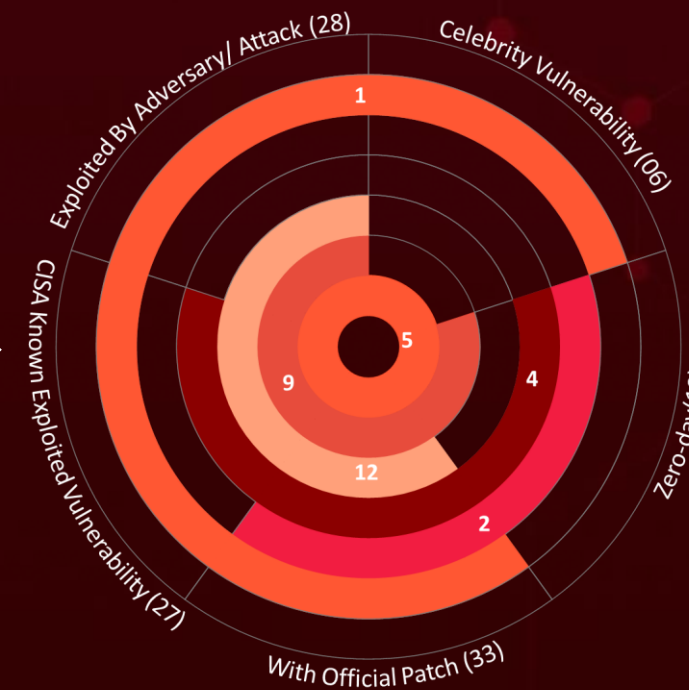
Summary

In **December**, the cybersecurity landscape witnessed a surge in attention due to the discovery of **nineteen zero-day** vulnerabilities. Notably, the **'Five Celebrity Vulnerabilities'** took center stage, featuring flaws like **FOLLINA** and **PROXYSHELL** exploited by **APT28**, **LOG4J** exploited by **Lazarus**, **ProxyNotShell** exploited by **Play Ransomware**, and **ProxyLogon** exploited by **Kuiper ransomware**.

During the same period, ransomware attacks experienced a noticeable uptick, with strains such as **Cactus**, **Crucio**, **BlueSky**, and **Mallox** actively targeting victims. As ransomware continues to advance in sophistication, organizations are urged to fortify their defenses by implementing robust backup and disaster recovery strategies. Additionally, employee training to recognize and thwart phishing attacks is crucial.

In parallel, **eighteen adversaries** were active across diverse campaigns. **APT28**, renowned for sophisticated phishing activities, exploited **nine vulnerabilities** for initial access. Their primary objectives included extracting user credentials and initiating subsequent malicious activities. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.





Total Vulnerabilities Published

Vulnerabilities Published in the Month

Exploited Vulnerabilities

Insights

Cactus Ransomware

strategically aims at establishing persistence within corporate networks through the **exploitation of Qlik Sense vulnerabilities**

CVE-2023-26360: Adobe ColdFusion Zero-Day

Targets government servers, leading to potential unauthorized code execution

Sandman APT

linked to China's Storm-0866 (Red Dev 40), deploys LuaDream and KEYPLUG concurrently within victim environments

BlueSky Ransomware

Deployed worldwide by exploiting CVE-2023-27350

Zero Click Two vulnerabilities

in Microsoft Windows can be chained to achieve RCE on vulnerable Outlook clients.

APT 29

Exploits Critical Vulnerability in JetBrains TeamCity, Posing Substantial Risk to Developer Environments

Cloud Atlas APT

exploiting **CVE-2017-11882**, a **six-year-old** memory corruption vulnerability in Microsoft Office to initiate the execution of malicious payloads

Operation RusticWeb

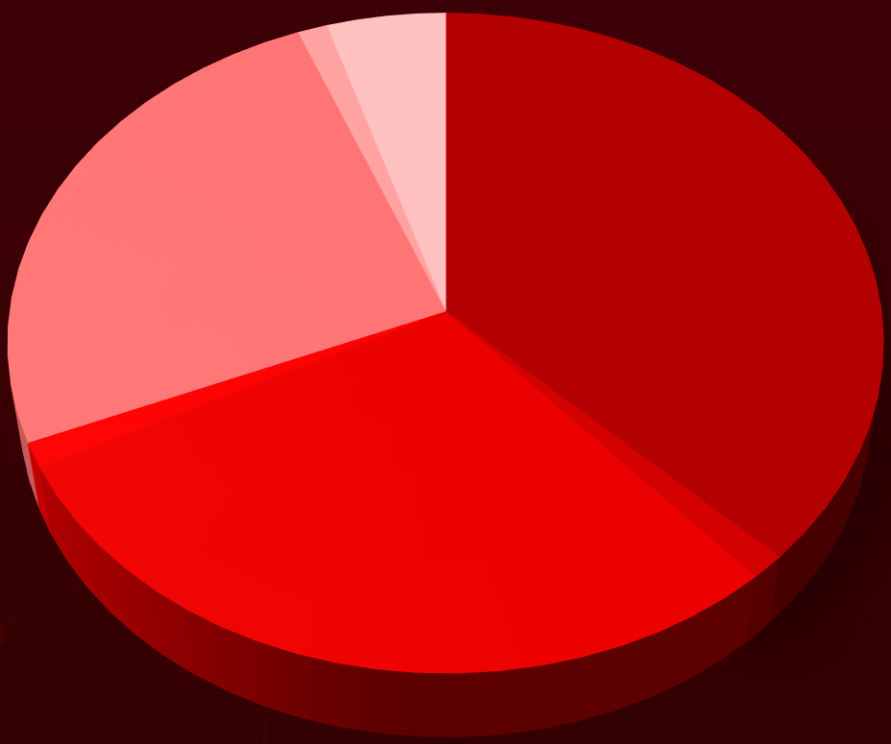
A phishing campaign targeting the Indian government and defense sector, deploying Rust-based malware

In December 2023

, a geopolitical cybersecurity landscape unfolds, revealing **Turkey**, **Egypt**, the **United States**, **Cyprus**, and **Israel** as the top-targeted countries

Highlighted in December 2023 is a cyber battleground encompassing the **government**, **telecommunications**, **healthcare**, and **manufacturing** sectors, designating them as the top industries

Threat Landscape



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Windows Server: 2008 – 2022, Windows: 7 – 11 21H2	APT28
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
FOLLINA (Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	✗	Microsoft Exchange Server	APT28
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	-
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	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-2021-44228		Apache Log4j2	Lazarus Group
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	NineRAT, DLRAT, BottomLoader, HazyLoad, LockBit Ransomware
LOG4J (Apache Log4j2 Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917 CWE-20 CWE-400 CWE-502	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41040		Microsoft Exchange Server	-
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*	Play Ransomware
ProxyNotShell (Microsoft Exchange Server Server-Side Request Forgery Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1552.005: Cloud Instance Metadata API	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-41082	✓	Microsoft Exchange Server	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*	Play Ransomware
ProxyNotShell (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-502	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	✓	Microsoft Exchange Server	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*	Kuiper ransomware
ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2023-41266	Qlik Sense Enterprise path traversal vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-41265	Qlik Sense Enterprise Privilege escalation vulnerability	Qlik Sense Enterprise for Windows	✗	✓	✓
CVE-2023-48365	Qlik Sense Enterprise remote code execution vulnerability	Qlik Sense Enterprise for Windows	✗	✗	✓
CVE-2023-26360	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	✓	✓	✓
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF and NG	✗	✓	✓
CVE-2022-30190	FOLLINA (Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability)	Microsoft Windows	✓	✓	✓
CVE-2023-23397	Microsoft Office Outlook Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR	✓	✓	✓
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Windows Server & Microsoft Internet Explorer	✓	✓	✓
CVE-2021-42292	Microsoft Excel Security Feature Bypass	Microsoft Office & Excel	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2021-42321	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✓	✓	✓
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2020-17144	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2020-0688	Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2023-42916	Apple WebKit Out-of-Bounds Read Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2023-42917	Apple WebKit Memory Corruption Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2023-20588	AMD Speculative Execution Information disclosure Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-23752	Joomla Improper Access Control Vulnerability	Joomla!	✗	✓	✓
CVE-2017-5638	Apache Struts Remote Code Execution Vulnerability	Apache Struts	✓	✓	✓
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS	✗	✓	✓
CVE-2020-12812	Fortinet FortiOS SSL VPN Improper Authentication Vulnerability	Fortinet FortiOS	✗	✓	✓
CVE-2022-41040	ProxyNotShell (Microsoft Exchange Server Server-Side Request Forgery Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2022-41082	ProxyNotShell (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2019-1068	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2020-0618	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2023-7024	Google Chrome Heap buffer overflow in WebRTC Vulnerability	Google Chrome	✓	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2023-7102	Barracuda ESG Arbitrary Code Execution Vulnerability	Barracuda Email Security Gateway (ESG) Appliance	✓	✗	✓
CVE-2023-7101	Spreadsheet::ParseExcel Arbitrary Code Execution Vulnerability	Spreadsheet::Parse Excel	✓	✓	✓
CVE-2023-51467	Apache OFBiz Pre-authentication Remote Code Execution Vulnerability	Apache OFBiz	✓	✗	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Cactus ransomware	Ransomware	CVE-2023-41266 CVE-2023-41265 CVE-2023-48365	Qlik Sense Enterprise for Windows	✓	Exploiting critical Qlik Sense vulnerabilities
SugarGh0st RAT	RAT	-	-	-	-
Gh0st RAT	RAT	-	-	-	-
Crucio Ransomware	Ransomware	-	-	-	-
Agent Racoon	Backdoor	-	-	-	-
Ntospy	Tool	-	-	-	-
BlueSky Ransomware	Ransomware	CVE-2023-27350	PaperCut MF and NG	✓	Phishing emails, phishing websites, and trojanized downloads
Tor2Mine	Crypto Miner	CVE-2023-27350	PaperCut MF and NG	✓	Exploiting Vulnerability
DanaBot	MaaS	-	-	-	Phishing
AsyncRAT	RAT	-	-	-	distributed through WSF script files
KrasueRAT	RAT	-	Linux	-	-
XorDdos Trojan	Trojan	-	-	-	Launch brute force attack
MrAnon Stealer	Infostealer	-	-	-	Phishing
NineRAT	RAT	CVE-2021-44228	Apache Log4j2	✓	Exploiting vulnerability
DLRAT					
BottomLoader	Downloader				

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
HazyLoad	Downloader	CVE-2021-44228	Apache Log4j2	✓	Exploiting vulnerability
LuaDream	Modular backdoor	-	-	-	DLL hijacking
KEYPLUG					-
Editbot Stealer	Infostealer	-	-	-	Unknown
More_Eggs	Backdoor	-	-	-	Phishing
GraphicalProton	Backdoor	CVE-2023-42793	TeamCity	✓	Phishing
Rhadamanthys stealer	Infostealer	-	-	-	Phishing
NKAbuse	Backdoor	CVE-2017-5638	Apache Struts Remote Code Execution Vulnerability	✓	Exploiting vulnerability
Pierogi++	Backdoor	-	-	-	-
Micropsia	Infostealer	-	-	-	Phishing
BarbWire	Backdoor	-	-	-	-
Play Ransomware	Ransomware	CVE-2018-13379 CVE-2020-12812 CVE-2022-41040 CVE-2022-41082	Fortinet FortiOS, Microsoft Exchange Server	✓	Exploiting vulnerabilities
ODAgent	Downloader	-	-	-	Unknown
OilCheck					
OilBooster					Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SC5k	Downloader	-	-	-	Phishing
Kuiper ransomware	Ransomware	CVE-2021-26855	Microsoft Exchange Server	✓	Exploiting vulnerability
PikaBot	Loader and backdoor	-	-	-	Malvertising
JaskaGO	Infostealer	-	-	-	Phishing
Mallox Ransomware	Ransomware	CVE-2019-1068 CVE-2020-0618	Microsoft SQL Server	✓	Exploiting vulnerabilities
MuddyC2Go	Backdoor	-	-	-	Phishing
Bandook RAT	RAT	-	-	-	Phishing
MetaStealer	Stealer	-	-	-	Emails
LONEPAGE	Backdoor	CVE-2023-38831	WinRAR	✓	-
SEASPY	Backdoor	CVE-2023-7102 CVE-2023-7101	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::ParseExcel	✓	Exploiting vulnerabilities
SALTWATER	Backdoor	CVE-2023-7102 CVE-2023-7101	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::ParseExcel	✓	Exploiting Vulnerabilities
AppleSeed	Backdoor	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
AlphaSeed	Backdoor	-	-	-	Phishing
Meterpreter	Backdoor	-	-	-	Phishing
TinyNuke	Trojan	-	-	-	Phishing

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
CyberAv3ngers	Information theft and espionage	Iran	-	Crucio Ransom ware	-
AeroBlade	Information theft and espionage	Unkno wn	-	-	-
Star Blizzard	Information theft and espionage	Russia	-	-	-
APT28	Information theft and espionage	Russia	CVE-2022-30190 CVE-2023-23397 CVE-2023-38831 CVE-2021-40444 CVE-2021-42292 CVE-2021-42321 CVE-2021-34473 CVE-2020-17144 CVE-2020-0688	-	Microsoft Windows, RARLAB WinRAR, Windows Server & Microsoft Internet Explorer, Microsoft Office & Excel, Microsoft Exchange Server
Lazarus Group	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	CVE-2021-44228	NineRAT, DLRAT, BottomL oader, HazyLoa d	Apache Log4j2
Sandman	Information theft and espionage	Unkno wn	-	LuaDrea m, KEYPLUG	-
Storm-0866	Information theft and espionage	China	-	LuaDrea m, KEYPLUG	-

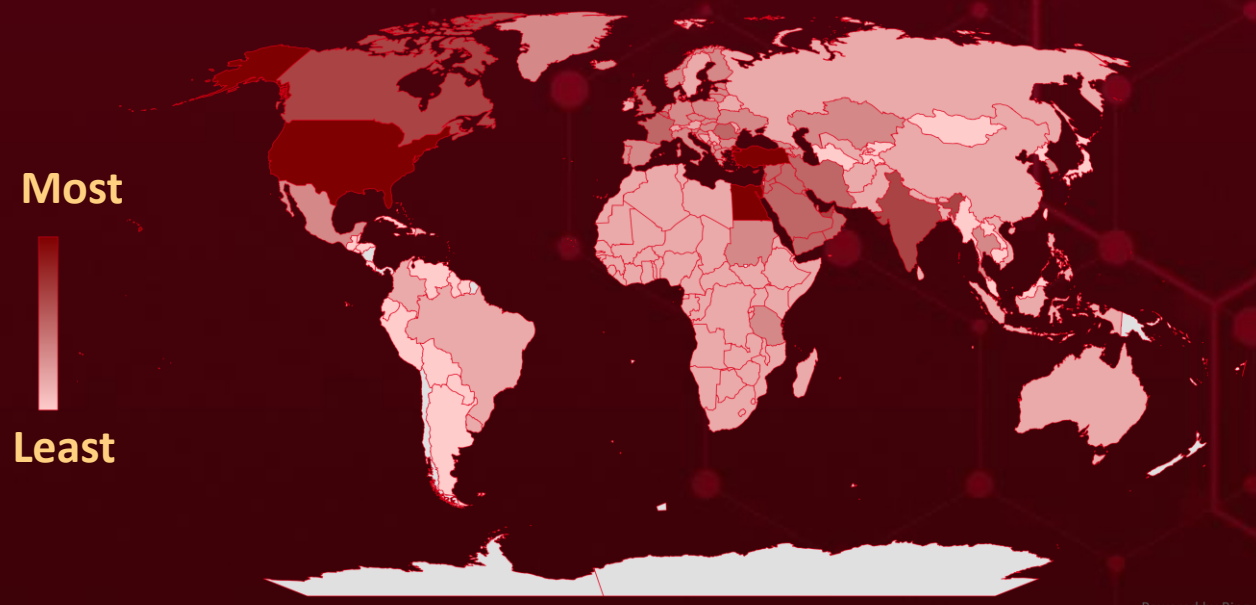
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
TA4557	Information theft and espionage	Unknown	-	More_Eggs	-
GambleForce	Information theft and espionage	Unknown	CVE-2023-23752	-	Joomla!
APT 29	Information theft and espionage	Russia	CVE-2023-42793	GraphicalProton	JetBrains TeamCity versions prior to 2023.05.4
Gaza Cybergang	Information theft and espionage	Gaza	-	Pierogi++, Micropsia, and BarbWire	-
OilRig	Information theft and espionage	Iran	-	ODAgent, OilCheck, OilBooster, SC5k downloader	-
TA577	Information theft and espionage	Unknown	-	PikaBot	-
MuddyWater	Information theft and espionage	Iran	-	MuddyC2Go, Venom Proxy, SimpleHelp	-
Cloud Atlas	Information theft and espionage	Russia	CVE-2017-11882	-	Microsoft Office
UAC-0099	Information theft and espionage	Unknown	CVE-2023-38831	LONEPAGE	WinRAR
UNC4841	Information theft and espionage	China	CVE-2023-7102 CVE-2023-7101	SEASPY and SALTWATER	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
Kimsuky	Information theft and espionage	North Korea	-	AppleSeed, AlphaSeed, Meterpreter, TinyNuke	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Qlik	Application	Qlik Sense Enterprise for Windows
Adobe	Application	Adobe ColdFusion
PaperCut	Application	PaperCut MF and NG
ATLASSIAN	Application	Atlassian Confluence Server: 4.0 - 8.5.3 Confluence Data Center: 4.0-8.7.0 Assets Discovery: before 6.2.0 Atlassian Companion App for MacOS: before 2.0.0 Jira Service Management Server: 5.4.0 - 5.11.1 Jira Service Management Data Center: 5.4.0 - 5.11.1 Bitbucket Data Center: 7.17.0 - 8.12.0 Bitbucket Server: 7.17.0 - 8.12.0 Confluence Data Center and Server 6.13.x - 8.3.0
Microsoft	Application	Microsoft Exchange Server, Microsoft Office & Excel, Microsoft Internet Explorer, Microsoft Azure, Microsoft Office Outlook, Microsoft SQL Server
RARLAB WinRAR	Application	RARLAB WinRAR
APACHE HTTP SERVER PROJECT	Framework	Apache Log4j2, Apache Struts, Apache OFBiz before 18.12.11
	Application	Apple Multiple Products
TC	Application	JetBrains TeamCity before 2023.05.4

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	webservice	Joomla! 4.0.0 through 4.2.7
FORTINET	Application	Fortinet FortiOS
	Browser	Google Chrome: 100.0.4896.60 - 120.0.6099.110
Barracuda	Security Appliance	Barracuda's Email Security Gateway (ESG): 5.1.3 - 9.2.1.001
 OpenBSD	Secure networking utilities	OpenSSH 9.0 to 9.5

Targeted Countries



Color	Countries
	Turkey
	Egypt
	United States
	Cyprus
	Israel
	Akrotiri and Dhekelia
	Canada
	United Arab Emirates
	India
	Lebanon
	Romania
	Iran
	Syria
	Yemen
	Iraq
	Jordan
	Saudi Arabia
	France
	Belgium
	Bahrain
	United Kingdom
	Palestine

Color	Countries
	Qatar
	Oman
	Kuwait
	Sudan
	Norway
	Mexico
	Albania
	Slovakia
	Croatia
	Lithuania
	Czech Republic
	Netherlands
	Denmark
	Poland
	Estonia
	South Korea
	Finland
	Thailand
	Georgia
	Luxembourg
	Germany
	Montenegro

Color	Countries
	Greece
	North Macedonia
	Greenland
	Azerbaijan
	Hungary
	Portugal
	Iceland
	Slovenia
	Armenia
	Spain
	Italy
	Tanzania
	Kazakhstan
	Ukraine
	Latvia
	Bulgaria
	Senegal
	Vietnam
	Switzerland
	Guinea
	Bangladesh
	Guinea-Bissau
	Chad

Color	Countries
	Burundi
	Uganda
	Algeria
	Afghanistan
	Anguilla
	Rwanda
	Indonesia
	Gabon
	Antigua and Barbuda
	Sri Lanka
	Cameroon
	Togo
	Ireland
	Botswana
	Isle of Man
	Faroe Islands
	Aruba
	Central African Republic
	Burkina Faso
	Barbados
	Ivory Coast
	São Tomé and Príncipe

Color	Countries
	Jersey
	Seychelles
	Australia
	Somalia
	Djibouti
	South Sudan
	Kenya
	Svalbard
	Abkhazia
	Gibraltar
	Zimbabwe
	Tunisia
	Dominican Republic
	Bhutan
	Austria
	Uzbekistan
	Lesotho
	Brazil
	Liberia
	Pakistan
	Libya
	Philippines
	Liechtenstein

Targeted Industries

Most

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery	**T1059.001** PowerShell
T1588 Obtain Capabilities	**T1036** Masquerading	**T1071** Application Layer Protocol	**T1588.006** Vulnerabilities	**T1055** Process Injection
T1053.005 Scheduled Task	**T1140** Deobfuscate/ Decode Files or Information	**T1204** User Execution	**T1041** Exfiltration Over C2 Channel	**T1566.001** Spearphishing Attachment
T1053 Scheduled Task/Job	**T1203** Exploitation for Client Execution	**T1071.001** Web Protocols	**T1083** File and Directory Discovery	**T1105** Ingress Tool Transfer
T1560 Archive Collected Data	**T1547** Boot or Logon Autostart Execution	**T1070** Indicator Removal	**T1204.002** Malicious File	**T1588.005** Exploits

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Cactus	SHA256	0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8, 09e7e3f23bac60ce7a4024ed7972981865f030c3edba9cda760d055f0a46e448, 0a8088e2ba539541f476836c6f4e5812c4ae5c52133801faa1bc3806a4ade683, 1ea49714b2ff515922e3b606da7a9f01732b207a877bcdd1908f733eb3c98af3, 21d7ad955dbc5732be90f3d6dbb4e161ef9cf511a7989e72c4ea1c5e44744167, 4b0a5d6a176317437978211a423a7c1cdf832baa7984bba09aeeb5a1e4d07aa3, 509a533ade43406eb50fa9cb8984b2e10d008ad0ea8c22d0652f3ee101125bb7, 6642d79f4d1044b756e2c3221ace37a71b4a671e18847f2940e2ea349dc6cb67, 69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc, 70a580e734c2331098fa3ecf3f1c928e17ddb92f99f75956c3f805b065222685, 729f0ff446c0aa04fdae3529ef02cf552e63782e841c24f3c4cb481b4b947859, 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17, 7a8c7166ebdae96e7adceaf50c064bf1cf85d3c360a6ff513414dc3078a6aa54, 9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a, a5296d07dabb3d7b53fce4cf803190bfa57e062abeb11a6d801250acb7005c5f, c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd, d1db583aad156dc4edd093a64aade4180a77477cb247347e3fc97cae401d061f, d455264bbb253a659149ba186f872920d83e3c6a0cab13965aa52a6b49406019, d7429c7ecea552403d8e9b420578f954f5bf5407996afaa36db723a0c070c4de, e9ac9436b5d61dd85e87e0fcd11b729a91466fe2f55f1f32501202d9ed98d562
NineRAT	SHA256	534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433, ba8cd92cc059232203bcadee260ddbae273fc4c89b184249749556607476982c4,

Attack Name	TYPE	VALUE
NineRAT	SHA256	47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30, f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59, 5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541, 82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def
DLRAT	SHA256	e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f, 9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a
Bottom Loader	SHA256	0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f
HazyLoad	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
LuaDream	Domains	mode.encagil[.]com, ssl.explorecell[.]com
	SHA1	fc8fdf58cd945619cbfede40ba06aada10de9459
	IPv4	185.82.218[.]230
KEYPLUG	Domains	dan.det-ploshadka[.]com, ssl.e-novauto[.]com, yum.luxyries[.]com
	SHA1	a7932112b7880c95d77bc36c6fcced977f4a5889, b6d759c9ea5d2136bacb1b2289a31c33500c8de8
	IPv4	172.67.216[.]63, 185.38.142[.]129, 37.120.140[.]205, 45.129.199[.]122, 45.90.59[.]17, 5.2.67[.]176, 5.2.72[.]130, 5.255.88[.]188, 79.110.52[.]160
GraphicalProton	SHA256	01b5f7094de0b2c6f8e28aa9a2ded678c166d615530e595621e692a9c0240732, 34c8f155601a3948ddb0d60b582cfe87de970d443cc0e05df48b1a1ad2e42b5e, 620d2bf14fe345eef618fdd1dac242b3a0bb65ccb75699fe00f7c671f2c1d869, 773f0102720af2957859d6930cd09693824d87db705b3303cef9ee794375ce13,

Attack Name	TYPE	VALUE
GraphicalProto n	SHA256	7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53, 8afb71b7ce511b0bce642f46d6fc5dd79fad86a58223061b684313966efef9c7, 971f0ced6c42dd2b6e3ea3e6c54d0081cf9b06e79a38c2ede3a2c5228c27a6dc, cb83e5cb264161c28de76a44d0edb450745e773d24bec5869d85f69633e44dcf, cd3584d61c2724f927553770924149bb51811742a461146b15b34a26c92cad43, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e, f1b40e6e5a7cbc22f7a0bd34607b13e7e3493b8aad7431c47f1366f0256e23eb, c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4, 4bf1915785d7c6e0987eb9c15857f7ac67dc365177a1707b14822131d43a6166, 18101518eae3eec6ebe453de4c4c380160774d7c3ed5c79e1813013ac1bb0b93, 19f1ef66e449cf2a2b0283dbb756850cca396114286e1485e35e6c672c9c3641, 1e74cf0223d57fd846e171f4a58790280d4593df1f2313204407656 0a5455ff8, 219fb90d2e88a2197a9e08b0e7811e2e0bd23d59233287587ccc4642c2cf3d67, 92c7693e82a90d08249edeafbca6533fed81b62e9e056dec34c24756e0a130a6, b53e27c79eed8531b1e05827ace2362603fb9f77f53cee2e34940d570217cbf7, c37c109171f32456bbe57b8676cc533091e387e6ba733fbaa01175c43cfb6ebd, c40a8006a7b1f10b1b42fdd8d6d0f434be503fb3400fb948ac9ab8ddfa5b78a0, c832462c15c8041191f190f7a88d25089d57f78e97161c3003d68d0cc2c4baa3, f6194121e1540c3553273709127dfa1daab96b0acfab6e92548bfb4059913c69
Play Ransomware	MD5	09f341874f72a5cfcedbca707bfd1b3b, 57bcb8cfad510109f7ddedf045e86a70
	SHA256	453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb, 47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57, 75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212, 7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41266	✗	Qlik Sense Enterprise for Windows	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022 :-:*:*:enterprise:windows:*:*	Cactus ransomware
Qlik Sense Enterprise path traversal vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1202: Indirect Command Execution, T1059: Command and Scripting Interpreter,	https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41265	✗	Qlik Sense Enterprise for Windows	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022 :-:*:*:enterprise:windows:*:*	Cactus ransomware
Qlik Sense Enterprise Privilege escalation vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1068: Exploitation for Privilege Escalation	https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48365	✗	Qlik Sense Enterprise for Windows	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*	Cactus ransomware
Qlik Sense Enterprise remote code execution vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1059: Command and Scripting Interpreter	https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26360	✗	ColdFusion: 2016 update 15 and earlier versions ColdFusion: 2021 Update 5 and earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:2021:Update 5:*:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities	https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350		PaperCut MF: before22.0.9 PaperCut NG: before22.0.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*	BlueSky Ransomware, Tor2Mine
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1190: Exploit Public-Facing Application; T1588.006: Vulnerabilities	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23397		Microsoft Windows	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps::*:*:*:enterprise:*:*:*	-
Microsoft Office Outlook Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-294	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831		WinRAR version 6.22 and older versions	APT28, UAC-0099
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	LONEPAGE
RARLAB WinRAR Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40444		Windows Server & Microsoft Internet Explorer	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
Microsoft MSHTML Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42292	✗	Microsoft Office & Excel	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:excel:2013:sp1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:*	-
Microsoft Excel Security Feature Bypass	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42292

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42321	✗	Microsoft Exchange Server	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_21:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_22:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_10:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_11:*:*:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42321

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-17144		Microsoft Exchange Server	APT28
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_31:*:*:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-17144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23752		Joomla! 4.0.0 through 4.2.7	GambleForce (aka EagleStrike)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:joomla:joomla\!:*:*:*:*:*:*:*:*	-
Joomla Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059:Command and Scripting Interpreter, T1005: Data from Local System	https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-0688	✗	Microsoft Exchange Server	APT28
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_30:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_14:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_15:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_3:*:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_4:*:*:*:*:*:*:*	-
Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-1068	✗	Microsoft SQL Server	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sql_server:-:*:*:*:*:*:*:*	Mallox Ransomware
Microsoft SQL Server Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059:Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42916		iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple WebKit Out-of-Bounds Read Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-125	T1059: Command and Scripting Interpreter	https://support.apple.com/enus/HT214031; https://support.apple.com/enus/HT214032; https://support.apple.com/en-us/HT214033

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2023-42917</td><td>  </td><td rowspan="3">iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td>-</td></tr>
<tr><td rowspan="3">Apple WebKit Memory Corruption Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-787</td><td>T1059: Command and Scripting Interpreter</td><td>https://support.apple.com/enus/HT214031; https://support.apple.com/enus/HT214032; https://support.apple.com/en-us/HT214033</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20588	✗	Windows Server: 2008 - 2022 23H2 Windows: 10 - 11 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
AMD Speculative Execution information disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-369	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-20588

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42793	✗	JetBrains TeamCity versions prior to 2023.05.4	APT 29
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	GraphicalProton
JetBrains TeamCity Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1082: System Information Discovery	https://www.jetbrains.com/teamcity/download/other.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-5638	✗	Apache Struts: 2.3.5 - 2.5.10	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:struts:*:*:*:*:*:*:*:*	NKAbuse
Apache Struts Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://struts.apache.org/download.cgi#struts-ga

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379	✗	FortiOS: 5.6.3 - 6.0.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Play Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter	https://fortiguard.com/advisory/FG-IR-18-384 http://www.fortiguard.com/psirt/FG-IR-20-233

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-12812	✗	FortiOS: 6.0.0 - 6.4.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Play Ransomware
Fortinet FortiOS SSL VPN Improper Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-178	T1082: System Information Discovery	https://fortiguard.com/psirt/FG-IR-19-283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7024	✗	Google Chrome: 100.0.4896.60 - 120.0.6099.110	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Heap buffer overflow in WebRTC Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗	Microsoft Office 2007 - 2016	Cloud Atlas
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*:*	-
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7101	✗	Spreadsheet::ParseExcel version 0.65	UNC4841
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:douglas_wilson:spreadsheet_parseexcel:0.65:*:*:*:*:*:*:*	SEASPY and SALTWATER
Spreadsheet::ParseExcel Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-95	T1059: Command and Scripting Interpreter	https://github.com/jmcnamara/spreadsheet-parseexcel/commit/bd3159277e745468e2c553417b35d5d7dc7405bc

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7102	 ZERO-DAY	Barracuda's Email Security Gateway (ESG): 5.1.3 - 9.2.1.001	UNC4841
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:barracuda:esg_appliance:9.2.1.001:*:*:*:*:*:*:*	SEASPY and SALTWATER
Barracuda ESG Arbitrary Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1104	T1059: Command and Scripting Interpreter	https://www.barracuda.com/company/legal/esg-vulnerability

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-51467	 ZERO-DAY	Apache OFBiz before 18.12.11	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*	-
Apache OFBiz Pre-authentication Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918 CWE-287	T1059: Command and Scripting Interpreter	https://ofbiz.apache.org/download.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2020-0618</td><td>  </td><td rowspan="2">Microsoft SQL Server</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:microsoft:sql_server:-:*:*:*:*:*:*:*</td><td rowspan="2">Mallox Ransomware</td></tr>
<tr><td rowspan="3">Microsoft SQL Server Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1059: Command and Scripting Interpreter</td><td>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cactus	CACTUS ransomware targets large commercial entities, gains initial access to networks through Qlik Sense vulnerabilities, exfiltrates sensitive data, and communicates with victims through Tox. It employs a variety of tools and tactics to distribute the ransomware binary and maintain persistence within the environment, while also attempting to obtain credentials and escalate privileges through lateral movement.	Exploiting critical Qlik Sense vulnerabilities	CVE-2023-41266 CVE-2023-41265 CVE-2023-48365
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, Compromised Systems	Qlik Sense Enterprise for Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SugarGh0st RAT	SugarGh0st is a customized variant of the Gh0st RAT. SugarGh0st is equipped with some customized features in its reconnaissance capability in looking for specific ODBC registry keys, loading library files with specific file extensions and function name, customized commands to facilitate the remote administration tasks directed by the C2, and to evade earlier detections.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise	-
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
Gh0st RAT	Gh0st Rat is a Windows malware that can remotely control a computer to log keystrokes, take screenshots, execute arbitrary commands, download and install additional malware.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crucio Ransomware	It is a customized Ransomware designed to infiltrate and exfiltrate data from key Israeli targets.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data loss, Compromised Systems	-
ASSOCIATED ACTOR			PATCH LINK
CyberAv3ngers			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agent Racoon	Agent Racoon is a malicious program written using the .NET framework. This malware creates a communication channel with its C&C server by leveraging the DNS protocol.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Execute commands and exfiltrate data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Ntospy	This malware is a Network Provider DLL module designed to steal user credentials.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Tool		Steal Credentials	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlueSky Ransomware	BlueSky Ransomware is a modern malware using advanced techniques to evade security defenses. It predominantly targets Windows hosts and utilizes the Windows multi-threading model for fast encryption.	Phishing emails, phishing websites, and trojanized downloads	CVE-2023-27350
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data	PaperCut MF and NG
ASSOCIATED ACTOR			PATCH LINK
-			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Tor2Mine	Tor2Mine is based on XMRigCC and uses a script that attempts to disable malware protection, execute a miner payload, and harvest Windows credentials.	Exploiting Vulnerability	CVE-2023-27350
TYPE		IMPACT	AFFECTED PRODUCTS
Crypto Miner		Harvest Credentials	PaperCut MF and NG
ASSOCIATED ACTOR			PATCH LINK
-			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

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
DanaBot	DanaBot is written in Delphi programming language, capable of stealing credentials and hijacking infected systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
MaaS		Data theft for financial gain	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a malware known for stealing credentials and executing various malicious activities since 2019. Its recent variant, distributed through WSF script files, employs sophisticated fileless techniques. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system.	distributed through WSF script files	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Steal Credentials	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KrasueRAT	The Krasue rootkit is a Linux Kernel Module (LKM) and targets Linux Kernel versions 2.6x/3.10.x. The rootkit masquerades as a VMware driver and does not contain a valid digital signature.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data theft for financial gain	Linux
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
XorDdos Trojan	XOR DDoS is a Linux Trojan malware with rootkit capabilities that was used to launch large-scale DDoS attacks. Its name stems from the heavy usage of XOR encryption in both malware and network communication to the C&Cs. It is built for multiple Linux architectures like ARM, x86 and x64.	Launch brute force attack	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Collect data, execute commands, launch DDoS	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MrAnon Stealer	MrAnon Stealer is a infostealer malware currently being used in phishing malicious campaigns. This malicious software is designed to pilfer victims' credentials, system details, browser sessions, and cryptocurrency extensions.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NineRAT	NineRAT, part of Lazarus Group's Operation Blacksmith, is a D programming language-based remote access trojan. It steals sensitive information, including credentials, system data, and browser sessions.	Exploiting vulnerability	CVE-2021-44228
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	Apache Log4j2
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			https://logging.apache.org/log4j/2.x/security.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DLRAT	DLRAT is a Remote Access Trojan (RAT), written in the D programming language. Linked to the Lazarus Group, it executes commands for extensive system reconnaissance upon activation.	Exploiting vulnerability	CVE-2021-44228
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	Apache Log4j2
RAT			
ASSOCIATED ACTOR			PATCH LINK
Lazarus Group			https://logging.apache.org/log4j/2.x/security.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BottomLoader	BottomLoader is a DLang-based malware downloader that acts as the initial stage of a cyber attack. Its primary function is to fetch and execute additional malicious payloads.	Exploiting vulnerability	CVE-2021-44228
		IMPACT	AFFECTED PRODUCTS
TYPE		Malware deployment	Apache Log4j2
Downloader			
ASSOCIATED ACTOR			PATCH LINK
Lazarus Group			https://logging.apache.org/log4j/2.x/security.html

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HazyLoad	HazyLoad is a specialized proxy tool identified in the Lazarus Group's Operation Blacksmith campaign. Its primary function is to create a lasting connection between the compromised host and infrastructure controlled by the attackers.	Exploiting vulnerability	CVE-2021-44228
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	Apache Log4j2
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			https://logging.apache.org/log4j/2.x/security.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LuaDream	LuaDream is a newly emerged backdoor malware with global reach. Functioning as an info-stealing malware, it has the capability to extract sensitive data, including credentials, system information, and user data, using various protocols.	DLL hijacking	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft	-
Modular backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Sandman and Storm-0866			-

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
KEYPLUG	KEYPLUG is a modular backdoor malware written in C++. It has the capability to steal sensitive data, assume control of a computer, and execute various other attacks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Modular backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Sandman and Storm-0866			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Editbot Stealer	Editbot Stealer is a malware that targets compromised networks, operated through a central command and control server. It specializes in stealing sensitive information such as browsing history, internet cookies, and login credentials.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	-
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
More_Eggs	More_Eggs is a JScript backdoor employed by the TA4557. It possesses the capability to collect data on installed anti-malware programs, assess the existence of various antivirus tools, and download as well as execute additional payloads.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
TA4557			-

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
GraphicalProton	GraphicalProton, linked to APT29, is a backdoor (also known as BlueBravo) utilized in campaigns involving TeamCity exploitation. The malware acts as a loader, communicating through OneDrive or Dropbox.	Phishing	CVE-2023-42793
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, Lateral movement	TeamCity
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
APT29			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys stealer	Rhadamanthys, the information-stealing malware, has taken a significant leap with its v0.5.0 upgrade, introducing expanded stealing features, raw syscalls, and an enhanced loader design, showcasing advanced evasion techniques. Its modular architecture allows for continuous updates, showcasing improved loader design and enhanced spying functionalities.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		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
NKAbuse	NKAbuse is a multiplatform malware that hides in blockchain networks, acts as a backdoor and flooder, and targets Linux systems and IoT devices. It infects through vulnerabilities and uses NKN to communicate with its command-and-control server.	Exploiting vulnerability	CVE-2017-5638
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, Launching DDoS attacks	Apache Struts Remote Code Execution Vulnerability
ASSOCIATED ACTOR			**PATCH LINK**
-			https://struts.apache.org/download.cgi#struts-ga

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Pierogi++	Pierogi++ is a backdoor malware targeting Palestinians, developed by Gaza Cyber Gang. It spies, executes commands, and uploads files. It's written in C++ for stealth and lacks Ukrainian clues.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Disruption, Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
Gaza Cyber Gang			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Micropsia	Micropsia is stealthy Windows malware that steals passwords, credit card info, documents, records keystrokes, takes screenshots, spies on browsing, and sends data to attackers.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft	-
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
Gaza Cybergang			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BarbWire	BarbWire, a potent malware developed by the APT-C-23 hacking group, has emerged as a significant threat to Israeli national security and private citizens alike.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, Launching DDoS attacks	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Gaza Cybergang			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SC5k	SC5k, an Iran-linked OilRig downloader, grabs and runs hidden malware on your system. It hides in cloud APIs, targets Israel.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Data Theft, Disruption	-
ASSOCIATED ACTOR			PATCH LINK
OilRig			-

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
Play Ransomware	The Play ransomware group, active since June 2022, employs a double-extortion model, impacting businesses globally. Utilizing legitimate tools for malicious activities, the group has affected approximately 300 entities.	Exploiting vulnerabilities	CVE-2018-13379 CVE-2020-12812 CVE-2022-41040 CVE-2022-41082
		IMPACT	**AFFECTED PRODUCTS**
TYPE		data loss, Compromised Systems	Fortinet FortiOS, Microsoft Exchange Server
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://fortiguard.com/advisory/FG-IR-18-384; http://www.fortiguard.com/psirt/FG-IR-20-233; https://fortiguard.com/psirt/FG-IR-19-283; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ODAgent	ODAgent, an Iran-linked OilRig downloader, hides in cloud APIs to infect systems and fetch more malware. It targets Israel, especially healthcare, manufacturing, and government.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Data Theft, Disruption	-
ASSOCIATED ACTOR			**PATCH LINK**
OilRig			-

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
OilCheck	OilCheck, an OilRig reconnaissance malware, gathers system info and helps launch future attacks. It hides as Windows processes and targets Israel's government, military, and critical infrastructure.	Unknown	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, Disruption	-
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
OilRig			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
OilBooster	OilBooster, linked to OilRig group, is a downloader that silently grabs more malware onto your system. It hides in cloud APIs, targets Israel.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, Disruption	-
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
OilRig			-

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
Kuiper ransomware	The Kuiper ransomware, developed in Golang, is compatible with Windows, Linux, and OSX systems, and is associated with a suspected intrusion at a government financial department in Africa.	Exploiting vulnerability	CVE-2021-26855
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PikaBot	PikaBot, a versatile malware, downloads other threats like ransomware, gives attackers remote control, and hides on Windows systems.	Malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader and backdoor		Data Theft, Downloading other malware	-
ASSOCIATED ACTOR			**PATCH LINK**
TA577			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JaskaGO	JaskaGO is a new cross-platform information stealer malware. This malware is designed to target and compromise systems running both Windows and macOS operating systems.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft, Data exfiltration	-
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
Mallox Ransomware	Mallox is a resilient Ransomware-as-a-Service (RaaS) threat, utilizing tactics like exploiting MS-SQL vulnerabilities and employing brute force attacks. Operating with a prolonged presence, Mallox's recent variant, "Mallox.Resurrection," exhibits consistent Functionalities.	Exploiting vulnerabilities	CVE-2019-1068 CVE-2020-0618
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	Microsoft SQL Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Bandook RAT	The Bandook malware is a persistent remote access trojan (RAT) that surfaced in 2007. Programmed in Delphi and C++, it has evolved through various iterations over the years and has historical associations with Dark Caracal. It featured prominently in a campaign dubbed 'Operation Manul'.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Remote access trojan		Data exfiltration	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
MuddyC2Go	MuddyC2Go, employed by the Iranian nation-state actor identified as MuddyWater, functions as a backdoor for carrying out cyber espionage attacks on the telecommunications sectors of Egypt, Sudan, and Tanzania.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, data breaches, and financial losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MetaStealer	A new information-stealing malware, available for sale for USD125 per month or USD1000 for unlimited use. Crafted to stealthily infiltrate target systems, facilitating the potential theft of passwords, cryptocurrency wallets, banking information, identity compromise, and financial losses.	Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Theft of passwords, cryptocurrency wallets, banking information, identity compromise, and financial losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LONEPAGE	The VBS malware LONEPAGE, when executed, it creates a hidden PowerShell process that communicates with a hardcoded C2 URL to fetch a text file	-	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Deploying additional payloads like keyloggers, data stealers, and screenshot tools	WinRAR
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0099			Update WinRAR version to 6.23 or later versions

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SEASPY	This malware is a persistent backdoor that masquerades as a legitimate network service. The malware is designed to listen to commands received from the Threat Actor's Command-and-Control through TCP packets.	Exploiting Vulnerabilities	CVE-2023-7102 CVE-2023-7101
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Monitor Traffic, Execute commands	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://www.barracuda.com/company/legal/esg-vulnerability

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SALTWATER	SALTWATER is a module for the Barracuda SMTP daemon (bsmtpd) that has backdoor functionality. SALTWATER can upload or download arbitrary files, execute commands, and has proxy and tunneling capabilities	Exploiting Vulnerabilities	CVE-2023-7102 CVE-2023-7101
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Upload and download files, execute commands	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UNC4841			https://www.barracuda.com/company/legal/esg-vulnerability

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
AppleSeed	AppleSeed is a backdoor that can receive the threat actor's commands from the C&C server and execute the received commands. The threat actor can use AppleSeed to control the infected system.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data theft, install additional malwares, take screenshots	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AlphaSeed	AlphaSeed is a malware developed in Golang and supports similar features to AppleSeed such as command execution and infostealing.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

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

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
CyberAv3ngers (also known as CyberAveng3rs, Cyber Avengers)</td><td>Iran</td><td rowspan="3">Critical Infrastructure (specifically, Water and Wastewater Systems), Energy, Food, Beverage, Manufacturing, Healthcare, and Shipping</td><td rowspan="3">United States of America and Israel</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Crucio Ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0006: Credential Access; TA0007: Discovery; TA0001: Initial Access; TA0040: Impact; T1110: Brute Force; T1584: Compromise Infrastructure; T1552: Unsecured Credentials; T1190:Exploit Public-Facing Application; T1057: Process Discovery; T1486: Data Encrypted for Impact</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 AeroBlade	Unknown	Aerospace	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1001: Data Obfuscation; T1016: System Network Configuration Discovery; T1027: Obfuscated Files or Information; T1598.002: Spearphishing Attachment; T1029: Scheduled Transfer; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1071.001: Web Protocols; T1082: System Information Discovery; T1083: File and Directory Discovery; T1105: Ingress Tool Transfer; T1106: Native API; T1137.001: Office Template Macros; T1140: Deobfuscate/Decode Files or Information; T1203: Exploitation for Client Execution; T1204.002: Malicious File; T1221: Template Injection; T1559.002: Dynamic Data Exchange			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto)	Russia	Academia, Defense, Governmental Organizations, NGOs, Think Tanks and Politicians	Canada, India, Lebanon, UAE, Ukraine, USA, NATO, UK
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; T1593: Search Open Websites/Domains; T1078: Valid Accounts; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.002: Email Accounts; T1583: Acquire Infrastructure; T1583.001: Domains; T1586: Compromise Accounts; T1586.002: Email Accounts; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1550: Use Alternate Authentication Material; T1550.004: Web Session Cookie; T1539: Steal Web Session Cookie; T1114: Email Collection; T1114.002: Remote Email Collection; T1114.003: Email Forwarding Rule

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Diplomatic, Education, Electrical, Embassies, Energy, Engineering, Financial, Foreign Affairs, Government, Healthcare, Industrial, Information Technology, Intelligence organization, IT, Logistics, Media, NGOs, Oil and gas, Telecommunications, Think Tanks, Transit Pipeline, Transportation, Utilities	Afghanistan, Albania, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, North Macedonia, Norway, Pakistan, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, SouthAfrica, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, United Arab Emirates, Uganda, United Kingdom, Ukraine, United States, Uzbekistan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-30190 CVE-2023-23397 CVE-2023-38831 CVE-2021-40444 CVE-2021-42292 CVE-2021-42321 CVE-2021-34473 CVE-2020-17144 CVE-2020-0688	-	Microsoft Windows, RARLAB WinRAR, Windows Server & Microsoft Internet Explorer, Microsoft Office & Excel, Microsoft Exchange Server

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation;TA0005: Defense Evasion; TA0006: Credential Access;TA0007: Discovery; TA0009: Collection;T1583: Acquire Infrastructure; T1588.006: Vulnerabilities; T1588.005: Exploits;T1560: Archive Collected Data; T1110: Brute Force;T1140: Deobfuscate/Decode Files or Information: T1114: Email Collection;T1203: Exploitation for Client Execution;T1068: Exploitation for Privilege Escalation;T1498: Network Denial of Service;T1566.001: Spearphishing Attachment;T1566.002: Spearphishing Link;T1057: Process Discovery; T1221: Template Injection;T1204.001:Malicious Link; T1078:Valid Accounts

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

Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</td><td>North Korea</td><td rowspan="3">Manufacturing, Agricultural and Physical security companies</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2021-44228</td><td>NineRAT, DLRAT, BottomLoader, HazyLoad</td><td>Apache Log4j2</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1574: Hijack Execution Flow; T1134: Access Token Manipulation; T1547: Boot or Logon Autostart: Execution; T1102: Web Service; T1082: System Information Discovery; T1003: OS Credential Dumping; T1003.005: Cached Domain Credentials; T1112: Modify Registry; T1518: Software Discovery; T1136: Create Account; T1098: Account Manipulation; T1033: System Owner/User: Discovery; T1105: Ingress Tool Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Sandman	Unknown	Telecommunication providers, and Government entities	The Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	LuaDream, KEYPLUG (aka ELFSHELF)	-
TTPs			
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; T1497: Virtualization/Sandbox Evasion; T1129: Shared Modules			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0866 (aka Red Dev 40)	China	Telecommunication providers, and Government entities	The Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	LuaDream, KEYPLUG (aka ELFSHELF)	-
TTPs			
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; T1497: Virtualization/Sandbox Evasion; T1129: Shared Modules			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA4557	Unknown	Recruiters	Philippines
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	More_Eggs	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; T1566: Phishing; T1566.001: Spearphishing: Attachment; T1566.002: Spearphishing Link; T1218: System Binary Proxy Execution; T1047: Windows Management Instrumentation; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1497: Virtualization/Sandbox Evasion; T1070: Indicator Removal; T1070.004: File Deletion; T1622: Debugger Evasion; T1220: XSL Script Processing; T1082: System Information Discovery; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 GambleForce (aka EagleStrike)	Unknown	Government, Gambling, Retail, and Travel	Australia, Brazil, China, India, Indonesia, the Philippines, South Korea, Thailand and APAC region
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-23752	-	Joomla!
TTPs			
TA0043: Reconnaissance; TA0042: Resource: Development; TA0001: Initial Access; TA0011: Command and Control; TA0010: Exfiltration; T1595: Active Scanning; T1595.002: Vulnerability: Scanning; T1595.003: Wordlist Scanning; T1592: Gather Victim Host Information; T1592.002: Software; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1190: Exploit Public-Facing Application; T1071: Application Layer Protocol; 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"> 
APT 29 (aka Midnight Blizzard, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)</td><td>Russia</td><td rowspan="3">Government, Political, Diplomatic agencies, and Technology</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2023-42793</td><td>GraphicalProton</td><td>JetBrains TeamCity versions prior to 2023.05.4</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1003 - OS Credential Dumping; T1020 - Automated Exfiltration; T1027 - Obfuscated Files or Information; T1033 - System Owner/User Discovery; T1036 - Masquerading; T1041 - Exfiltration Over C2 Channel; T1046 - Network Service Scanning; T1047 - Windows Management Instrumentation; T1049 - System Network Connections Discovery; T1053 - Scheduled Task/Job; T1055 - Process Injection; T1057 - Process Discovery; T1059 - Command and Scripting Interpreter; T1068 - Exploitation for Privilege Escalation; T1098 - Account Manipulation; T1190 - Exploit Public-Facing Application; T1203 - Exploitation for Client Execution; T1210 - Exploitation of Remote Services; T1505 - Server Software Component; T1547 - Boot or Logon Autostart Execution; T1555 - Credentials from Password Stores; T1558 - Steal or Forge Kerberos Tickets; T1562 - Impair Defenses; T1564 - Hide Artifacts; T1567 - Exfiltration Over Web Service; T1568 - Dynamic Resolution; T1572 - Protocol Tunneling; T1574 - Hijack Execution Flow; T1590 - Gather Victim Network Information; T1592 - Gather Victim Host Information; T1531 - Account Access Removal; T1140 - Deobfuscate/Decode Files or Information; T1550 - Use Alternate Authentication Material; T1195 - Supply Chain Compromise; T1102 - Web Service</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Gaza Cybergang (aka TA402, Extreme Jackal, Molerats, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)</td><td>Gaza</td><td rowspan="3">Manufacturing, Agricultural and Physical security companies</td><td rowspan="3">Middle East</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Pierogi++, Micropsia, and BarbWire</td><td>-</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; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1083: File and Directory Discovery; T1082: System Information Discovery; T1204: User Execution; T1598: Phishing for Information; T1566.001: Spearphishing Attachment; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1543: Create or Modify System Process; T1587: Develop Capabilities; T1587.001: Malware</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
OilRig (aka APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, DEV-0861, EUROPIUM, Hazel Sandstorm, Scarred Manticore)</td><td>Iran</td><td rowspan="3">Healthcare sector, Manufacturing company, Local government</td><td rowspan="3">Israel</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>ODAgent, OilCheck, OilBooster, SC5k downloader</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.006: Web Services; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1585.002: Email Accounts; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell: T1106: Native API; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1564: Hide Artifacts; T1564.003: Hidden Window; T1070: Indicator Removal; T1070.004: File Deletion; T1202: Indirect Command: Execution; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1027: Obfuscated Files or: Information; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1560: Archive Collected Data; T1560.003 : Archive via Custom Method; T1074: Data Staged; T1074.001: Local Data Staging; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1008: Fallback Channels; T1105: Ingress Tool Transfer; T1102: Web Service; T1102.002: Bidirectional Communication; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA577	Unknown	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PikaBot	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0042: Resource Development; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1566: Phishing; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1036: Masquerading; T1059.007: JavaScript; T1059: Command and Scripting Interpreter ; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1218.007: Msiexec			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)	Iran	Telecommunications	Egypt, Sudan, and Tanzania
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	MuddyC2Go, Venom Proxy, SimpleHelp	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1047: Windows Management Instrumentation; T1189: Drive-by Compromise; T1105: Ingress Tool Transfer; T1056: Input Capture; T1566: Phishing; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1027: Obfuscated Files or Information; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Cloud Atlas (aka Inception Framework, Oxygen, ATK 116, Blue Odin, The Rocra)	Russia	Russian agro-industrial enterprise and a state-owned research company	Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Africa, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-11882	-	Microsoft Office

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1589: Gather Victim Identity Information; T1589.002: Email Addresses; T1583: Acquire Infrastructure; T1583.001: Domains; T1585: Establish Accounts; T1585.002: Email Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1608: Stage Capabilities; T1608.001: Upload Malware; T1566: Phishing; T1566.001: Spearphishing Attachment; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1203: Exploitation for Client Execution; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1564: Hide Artifacts; T1564.004: NTFS File Attributes; T1221: Template Injection; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UAC-0099	-	-	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-38831	LONEPAGE	WinRAR
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1547: Boot or Logon Autostart Execution; T1053: Scheduled Task/Job; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1560: Archive Collected Data; T1106: Native API; T1176: Browser Extensions; T1566: Phishing; T1566.001: Spearphishing Attachment; T1036: Masquerading; T1041: Exfiltration Over C2 Channel; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1071: Application Layer Protocol; T1071.001: Web Protocols;			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC4841	China	-	-
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2023-7102 CVE-2023-7101	SEASPY and SALTWATER	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
TTPs			
TA0002: Execution; TA0042: Resource Development; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1204.002: Malicious File; T1203: Exploitation for Client Execution; T1588.005: Exploits; T1659: Content Injection			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)</td><td>North Korea</td><td rowspan="2">Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>AppleSeed, AlphaSeed, Meterpreter, TinyNuke</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; T1547: Boot or Logon Autostart Execution; T1056: Input Capture; T1036: Masquerading; T1543: Create or Modify System Process; T1071: Application Layer Protocol; T1102: Web Service; T1113: Screen Capture; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1021: Remote Services; T1566: Phishing; T1566.002: Spearphishing Link</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
	T1592: Gather Victim Host Information	
	T1593: Search Open Websites/Domains	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	T1590.004: Network Topology
	T1592: Gather Victim Host Information	T1592.002: Software
	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.003: Wordlist Scanning
	T1589: Gather Victim Identity Information	T1589.002: Email Addresses
TA0042: Resource Development	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
	T1584: Compromise Infrastructure	T1584.004: Server
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.003: Cloud Accounts
		T1585.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.002: DNS Server
		T1583.005: Botnet
		T1583.008: Malvertising
		T1583.004: Server
		T1583.006: Web Services
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.002: Tool
		T1588.001: Malware
	T1586: Compromise Accounts	T1586.002: Email Accounts
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1659: Content Injection	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
TA0002: Execution	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.007: JavaScript
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1203: Exploitation for Client Execution	
	T1129: Shared Modules	
	T1569: System Services	T1569.002: Service Execution
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1559: Inter-Process Communication	T1559.001: Component Object Model
		T1559.002: Dynamic Data Exchange
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1098: Account Manipulation	
	T1176: Browser Extensions	
	T1133: External Remote Services	
	T1136.002: Create Account	T1136.002: Domain Account
	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1137: Office Application Startup	T1137.001: Office Template Macros
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
TA0004: Privilege Escalation	T1098: Account Manipulation	
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1543.001: Launch Agent
		T1543.004: Launch Daemon
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
TA0005: Defense Evasion	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1036: Masquerading	T1036.007: Double File Extension
		T1036.008: Masquerade File Type
		T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	T1027.009: Embedded Payloads

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1484: Domain Policy Modification	T1484.001: Group Policy Modification
	T1562: Impair Defenses	
	T1221: Template Injection	
	T1202: Indirect Command Execution	
	T1480: Execution Guardrails	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
	T1070: Indicator Removal	T1070.006: Timestomp
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1564: Hide Artifacts	T1564.002: Hidden Users
	T1622: Debugger Evasion	
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1134: Access Token Manipulation	
	T1220: XSL Script Processing	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1110: Brute Force	
	T1552: Unsecured Credentials	
	T1539: Steal Web Session Cookie	
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
		T1555.004: Windows Credential Manager
	T1558: Steal or Forge Kerberos Tickets	T1558.001: Golden Ticket
	T1606: Forge Web Credentials	
	T1557: Adversary-in-the-Middle	
TA0007: Discovery	T1018: Remote System Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
	T1046: Network Service Discovery	
	T1087: Account Discovery	
	T1016: System Network Configuration Discovery	
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1622: Debugger Evasion	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1007: System Service Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1040: Network Sniffing	
	T1518: Software Discovery	T1518.001: Security Software Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.006: Windows Remote Management
		T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
TA0009: Collection	T1056: Input Capture	T1056.001: Keylogging
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1074: Data Staged	T1074.001: Local Data Staging
	T1114: Email Collection	T1114.002: Remote Email Collection
		T1114.003: Email Forwarding Rule
	T1005: Data from Local System	
	T1119: Automated Collection	
	T1557: Adversary-in-the-Middle	
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.004: DNS
	T1659: Content Injection	
	T1105: Ingress Tool Transfer	
	T1104: Multi-Stage Channels	
	T1572: Protocol Tunneling	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1568: Dynamic Resolution	
	T1008: Fallback Channels	
	T1571: Non-Standard Port	
TA0010: Exfiltration	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
	T1029: Scheduled Transfer	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1048: Exfiltration Over Alternative Protocol	
TA0040: Impact	T1657: Financial Theft	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1498: Network Denial of Service	
	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
	T1489: Service Stop	

Top 5 Takeaways

#1 In **December**, there were **nineteen zero-day** vulnerabilities, with the '**Five** Celebrity Vulnerabilities' taking center stage. These featured flaws such as **FOLLINA**, **PROXYSHELL**, **LOG4J**, **ProxyNotShell**, and **ProxyLogon**.

#2 Throughout the month, ransomware strains including **Cactus, Crucio, BlueSky, Play,** and **Mallox** actively targeted victims.

#3 Numerous malware families have been observed targeting victims in the wild. These include **NineRAT**, **DLRAT**, **BottomLoader**, **HazyLoad**, and **LockBit** Ransomware

#4 There were a total of **18** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: Government, Telecommunications, Healthcare, and Manufacturing

#5 Finally, APT28, renowned for sophisticated phishing activities, exploited **nine** vulnerabilities for initial access. Their primary objectives included extracting user credentials and initiating subsequent malicious activities.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **33 significant vulnerabilities** and block the indicators related to the **18 active threat actors, 46 active malware,** and **251 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 **33 significant vulnerabilities**

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

Hive Pro Threat Advisories (DECEMBER 2023)

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

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

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

Appendix

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

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

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
Cactus	SHA256	0933f23c466188e0a7c6fab661bdb8487cf7028c5cec557efb75fde9879a6af8, 09e7e3f23bac60ce7a4024ed7972981865f030c3edba9cda760d055f0a46e448, 0a8088e2ba539541f476836c6f4e5812c4ae5c52133801faa1bc3806a4ade683, 1ea49714b2ff515922e3b606da7a9f01732b207a877bcdd1908f733eb3c98af3, 21d7ad955dbc5732be90f3d6dbb4e161ef9cf511a7989e72c4ea1c5e44744167, 4b0a5d6a176317437978211a423a7c1cdf832baa7984bba09aeeb5a1e4d07aa3, 509a533ade43406eb50fa9cb8984b2e10d008ad0ea8c22d0652f3ee101125bb7, 6642d79f4d1044b756e2c3221ace37a71b4a671e18847f2940e2ea349dc6cb67, 69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc, 70a580e734c2331098fa3ecf3f1c928e17ddb92f99f75956c3f805b065222685, 729f0ff446c0aa04fdae3529ef02cf552e63782e841c24f3c4cb481b4b947859, 78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17, 7a8c7166ebdae96e7adceaf50c064bf1cf85d3c360a6ff513414dc3078a6aa54, 9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a, a5296d07dabb3d7b53fce4cf803190bfa57e062abeb11a6d801250acb7005c5f, c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd, d1db583aad156dc4edd093a64aade4180a77477cb247347e3fc97cae401d061f, d455264bbb253a659149ba186f872920d83e3c6a0cab13965aa52a6b49406019, d7429c7ecea552403d8e9b420578f954f5bf5407996afaa36db723a0c070c4de, e9ac9436b5d61dd85e87e0fcd11b729a91466fe2f55f1f32501202d9ed98d562

Attack Name	TYPE	VALUE
SugarGh0st RAT	IPv4	103[.]148[.]245[.]235, 103[.]108[.]67[.]191
	Hostname	account[.]drive-google-com[.]tk, login[.]drive-google-com[.]tk
	SHA256	8584094f79fce97321ee82ca5da41b6830ecc6a0921bcaddb8dd337827cd7d1a, 3436135bb3839521e7712882f0f6548aff78db66a1064408c49f820a0b85d980, c758eed6660786097b63ac6748236b5b6084783703ea7ee2111e8f0bcaa3652e, 6dff111b6adc9e33bed20eae99bec779f1c29dd55895a71125cfbe3c90950eb2, 7c87451261dfce64fda987eb395694b5330fd958466c46c931440cd9dc227505, ddac61f918ed87b49ef15d05873e7f52b919758aef713145f6a7d538c714fa2e, f3ea4611c72d57eabf381d5639c3c8d1840cb005ed811f3038410fb2e04978c1, 9d9a0af09fc9065bacabf1a193cad4386b5e8e5101639e07efa82992b723f3b0, 5ad182c913f0b5cb6a34126137c335110d4c9472f5c745cb7a438d108b03b27c, 38c815729f34aef6af531edf3f0c3f09635686dbe7e5db5cb97eca5b2b5b7712, adb4eb33213fa81c8b6cc013a6f4a43fa8b70eb8027433cf4339b532cb6e84cf, 2e543adb701afd40affcb4c51bd8246398b0210bee641ca9aeffcca893c9e4a5, 7cacdc84a0d690564c8471a4f58ab192ef7d9091ab0809933f616010bbf6846a, 66982ebd5ebb75633723c7057a1e948ac3aafe3ff808397eb0c55c853c82f9e6, 21f19d87d2169c82efd76ddb1baa024a1e59b93f82d28f276de853fc3ef8b20e, 362fde3362e307af3787b9bf0b5c71f87b659a3217e054c4d0acea8b9e6d74b0, ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e, 9783c0eee31ce6c5f795ecf387025af5d55208ff2713c470af2042721ab38606, 410d7dc973d188cd0d962a59f48deb1cfc73adf37857765e90194f6e878d4488, bd0a1efe07fcb4af4bec1b2881a0711f0be34044680ad8cff958a68a70d4a914, ff0f28f96bbb6c80fc3823fe71d5e07e1a05b06986e82a2fbe324d68ba5ab2ea

Attack Name	TYPE	VALUE
Gh0st RAT	SHA256	83fbbd31e43ad25a8921c98d97b287ebc8902451f7647c2266e5f0688471e8b6
Crucio Ransomware	MD5	BA284A4B508A7ABD8070A427386E93E0
	SHA1	66AE21571FAEE1E258549078144325DC9DD60303
	SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
Agent Racoon	SHA256	4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, e0748ce315037253f278f7f8f2820c7dd8827a93b6d22d37dafc287c934083c4, baed169ce874f6fe721e0d32128484b3048e9bf58b2c75db88d1a8b7d6bb938d, 3a2d0e5e4bfd6db9c45f094a638d1f1b9d07110b9f6eb8874b75d968401ad69c, 4351911f266eea8e62da380151a54d5c3fbbc7b08502f28d3224f689f55bffba, 354048e6006ec9625e3e5e3056790afe018e70da916c2c1a9cb4499f83888a47, dee7321085737da53646b1f2d58838ece97c81e3f2319a29f7629d62395dbfd1
	File Path	c:/windows/temp/onedriveupdater.exe, c:/windows/system32/msmdlb.exe, c:/windows/temp/onedriveupdater.exe, c:/program files (x86)/google/update/googleupdate.exe, c:\windows\temp\mslb.ps1
Ntospy	SHA256	e30f8596f1beda8254cbe1ac7a75839f5fe6c332f45ebabff88aadbce3938a19, 1a4301019bdf42e7b2df801e04066a738d184deb22afcad9542127b0a31d5cfa, e7682a61b6c5b0487593f880a09d6123f18f8c6da9c13ed43b43866960b7aa8e, 58e87c0d9c9b190d1e6e44eae64e9a66de93d8de6cbd005e2562798462d05b45, 7eb901a6dbf41bcb2e0cdcbb67c53ab722604d6c985317cb2b479f4c4de7cf90, f45ea12579f636026d29009190221864f432dbc3e26e73d8f3ab7835fa595b86, bcd2bdea2bfecd09e258b8777e3825c4a1d98af220e7b045ee7b6c30bf19d6df
BlueSky Ransomware	MD5	7b68bc3dd393c2e5273f180e361f178a
	SHA1	07610f11d3b8ccb7b60cc8ad033dda6c7d3940c4
	SHA256	e6b413c8b8b2dfc4d8879acf85981a64020f094dcff27aa95f500f4be600bc67, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24,

Attack Name	TYPE	VALUE
BlueSky Ransomware	SHA256	5cda02a670505a523a18df8cbb216b77dc3f69f3ec22d7ee90f1d1dae1eddf10, 40bf3b2f344995352d9a9703c4e0fb12a752c105b9fb133d6cce7e9e5e99df4a, 2ee6dfbfb2afd7442c9f2212eb142876698851c3ffb552ee420c0281e35a836e, e32fc8ad818d2ef217aaa4f467c7a8af1dad88fdd5166186f732b2e233c90148, 11e409f8b0799cd64c53d40ff10cbc639a1f85cd5ba6544fe42689a96302cc2e, c72e5ff7858844e335fafdd54395be85d708cfb9a91ade6f398fc0f1c9b50919, 38478119e3344e735cf60442e7528db63046a543a5f422db8f946b2c2693d19a, 4fd0c22d92f8bf7a062497867a802bdbab4c802ac10c8b529fe7f896e7517492, 1b44b3e401f26547ee820bc0fe90904c55ec59d74e4385fe5bdd1826738fa9e6, 22a020af0e4be83dea45c0700d065d9ae64630748c02b58397f6c6d91c3efb0d, 4c752131e47710d47dd0084a22ac03cd5924eb617e97cf895159ae03d86f561e, 6e1057e52d296655f932b8a9da7302b31379ce5b9ba4cc32ed3af4c15c7adcf0, 905de085d2a9ebf553e3325eb9c878b9855f85c10f77e80c46519056658d6bab, d401be3ec0699cfdc1a16a9243ebc25181385e428122b0b1a283b7a8d47dd0bc, 99828018b3af892707985f6a3f8c3d34ae1d1575fdefd7a05f1e6861181ec1b2, afccc93c4122d7e63543fc342a4ba9319c4969797c0c3ed32b944b07c83aea16, 2176a3cdf5db56f5dcab475f362d459d4b2b3dafc3c146caaf3100009d0c8a5f, 11ae63b3a7caac549374aaa3c7fea9cba7f23ae83118745fee0a4157f61156f2, 18329783ad51783d679aec6111ca171eb1176f8fa866949a5267009c14605aa6, 9e302bb7d1031c0b2a4ad6ec955e7d2c0ab9c0d18d56132029c4c6198b91384f, 8dfd7ee796dd98daefbc1458a34f0460ebd8508df319d44ab48f4cbc579a7f09, baaa0e49398ef681ef71e84a7a86dd2b78f36ac83785e0d9a061067ebaf8b006, c0514cd580275b54f5b1d69086c9f415e7afb805479bfea50251e82dc2e60e12, 376fdb43699c90fd6cca2706c14827791137b3a753c7368a202de63f588fdb2f, 94733075d7ccdc9d770f71200e11f84c00b8a529182b504fb997e9b331470f9a,

Attack Name	TYPE	VALUE
BlueSky Ransomware	SHA256	c3d5248230230e33565c04019801892174a6e5d8f688d61002e369b0b9e441ff, 311dc38f619f40f06bee5157119ab4b93684924f53e4ff2da34412f9dac111a4, 3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb, 840af927adbfdeb7070e1cf73ed195cf48c8d5f35b6de12f58b73898d7056d3d, 47971a5a44f487f341d482fdcb91271a2aea4d3eee7191c69568690d2fe9f251, 91795d3e8925e647444eb383e52cdc5046db10fa320afc817fab29b085e7d76f, 06ad123df8f3fcc6ca4785c0b52fc57e6e54f44e403fca2fdbd339580d3c53b0, d6386b2747335f7b0d13b1f69d995944ad8e9b71e09b036dbc0b907e583d857a, c75748dc544629a8a5d08c0d8ba7fda3508a3efdaed905ad800ffddbc8d3b8df, b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec, 2280898cb29faf1785e782596d8029cb471537ec38352e5c17cc263f1f52b8ef, e75717be1633b5e3602827dc3b5788ff691dd325b0eddd2d0d9ddcee29de364f, 1c99798c7aaabba3c0af8e75b7af7bfde290448b7570c7fac43e02f2690e1248, b39fcf37d9019cc92127ee82c03df5e37aa8238cd76cc6eca2e3d1e7e977fc26, D4f4069b1c40a5b27ba0bc15c09dceb7035d054a022bb5d558850edfba0b9534
Tor2Mine	MD5	9e88c287eb376f3c319a5cb13f980d36, 08bdf000031bbad1a836381f73adace5
	SHA1	3dff4ae3c421c9143978f8fc9499dca4aed0eac5, 501af977080d56a55ff0aeba66b58e7f3d1404ea
	SHA256	f955eeb3a464685eaac96744964134e49e849a03fc910454faaff2109c378b0b, 74b6d14e35ff51fe47e169e76b4732b9f157cd7e537a2ca587c58dbdb15c624f
DanaBot	SHA256	8ffd4fd0e29d6888e9eaf78a6f698436f8a4477cdba8b6271015f7b012d1f8e0, 67540a00b6fa011944ba222eb8b83f877aa75328204dbd02b242ad9a678d1a83, e7351978a0011be925a7831e37a82750c51b2ef5e913b42d69b3d509fe8e6b8a, 2cf2d35802c12f09cc2700baf30816c6155a6095651dad6bfff440d1c772e0d9, 7a3996fdfa138ac0d4692820c82e1ae23fd5874c8c7bd89c11b56d5cd31480dd, a41d5274599dfe60823b477ea0dc20b9c8e9b398d8b287701f8cb02ea605ad84,

Attack Name	TYPE	VALUE
DanaBot	SHA256	6eba004a9ea73c873bd66739431db34ebc3eb3928b9ecf0b89132ad473ef20b3
AsyncRAT	IPv4	185[.]81[.]157[.]242
	MD5	0a80a592d407a2a8b8b318286dc30769, 61b7507a6814e81cda6b57850f9f31da, 750dc2354b0454eafd66900687a0f7d6, 790562cefbb2c6b9d890b6d2b4adc548, a31191ca8fe50b0a70eb48b82c4d6f39, ac12d457d3ee177af8824cdc1de47f2a, b98e76816350a6a527fc311dae62b85e, c09266666ee71ade24e0e5f889cc8199
	SHA1	316b99a2bf664ccd94eb050005975c52806d2163, 3b10e9a10fc90e2a0a28f13a84c9b58eeb382dfc, 921bd5cb08b5c6a77a28e2864417bb8cdefafbf0
	SHA256	621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c, 70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75, a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387
	Hostname	drippmedsot[.]mywire[.]org
	URL	hxxp://drippmedsot[.]mywire[.]org:6606, hxxp://drippmedsot[.]mywire[.]org:7707, hxxp://drippmedsot[.]mywire[.]org:8808, hxxp://za[.]com/Order_ed333c91f0fd[.]zip
	Hostname	drippmedsot[.]mywire[.]org
KrasueRAT	IPv4	128.199.226[.]11
	MD5	100a5f3875e430f6de03d99752fbb6a7, 5055925b5bcd715d5b70b57fdbeda66b
	SHA1	051bc3273a20a53d730a3beaff2fadcd38d6bb85, eddb4476ca610f3c5e895f4811c9744704552d2f
	SHA256	38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353, 3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59, 4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1, 8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831, 902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc, 97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772,

Attack Name	TYPE	VALUE
KrasueRAT	SHA256	afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4, b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d, c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5, e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632, Ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f
XorDdos Trojan	SHA256	ce0f1914e0f0748f85ecc18d8470de2a0b2b60be7eaab7a459899f77993e82e6, 664fd170b1d07e372b3daa91aab78a8151d3f0b0361a2b3157b405314dd219a2, c0b0225201fd3a4c08245e58bbb4b844e0d3426e89b9ac3fc34db37d994fb182, 44046ce4a3a47b4d22ac7697817bfc16e18d835a33f0898c3e4df359c33d158c, 2154547c69bf8bee7f296bd8ce56ffa4115da65c2308e9fc6d5079b2eb9dec93, c9bd6d01eb7258fef88ec5c9276431c1db45f063b316f83943e45b6a40a76783, 4616bc3ba5c245946819c55db573b552ba1c0cc5e0c54c433ffb1824452fc609, a40d947d6a1d92c2789968ce0d2e6eb1734e248e2d30828c61a41f4ac840e8a0, 311c93575efd4eeeb9c6674d0ab8de263b72a8fb060d04450daccc78ec095151
MrAnon Stealer	SHA256	29ca95ce3eca818872a7ad47e4fafa3f9582836e0b24c5a6486df76397344521, 075e40be20b4bc5826aa0b031c0ba8355711c66c947bbbaf926b92edb2844cb0, 48e09b8043c0d5dfc2047b573112ead889b112108507d400d2ce3db18987f6c9, 0efba3964f4b760965e94b4d1a597e6cd16241b8c8bf77a664d6216d1420b312, 8a8c9acf09c84ab5ea4c098eace93888a88b82a1485255073c93ce6080d05ec7, 96ec8ef2338d36b7122a76b0398d97e8d0ed55c85e31649ea00e57d6b1f53628, 8b71525ca378463784ce2d81a8371714580c58f0d305a2aa4630dc964c8c0ee0, 45ee224e571d0fd3a72af1d7a7718e61a1aad03b449cf85377411d51c135bb22

Attack Name	TYPE	VALUE
NineRAT	SHA256	534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433, ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4, 47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30, f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59, 5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541, 82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def
DLRAT	SHA256	e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f, 9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a
Bottom Loader	SHA256	0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f
HazyLoad	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
LuaDream	Domains	mode.encagil[.]com, ssl.explorecell[.]com
	SHA1	fc8fdf58cd945619cbfede40ba06aada10de9459
	IPv4	185.82.218[.]230
KEYPLUG	Domains	dan.det-ploshadka[.]com, ssl.e-novauto[.]com, yum.luxyries[.]com
	SHA1	a7932112b7880c95d77bc36c6fcced977f4a5889, b6d759c9ea5d2136bacb1b2289a31c33500c8de8
	IPv4	172.67.216[.]63, 185.38.142[.]129, 37.120.140[.]205, 45.129.199[.]122, 45.90.59[.]17, 5.2.67[.]176, 5.2.72[.]130, 5.255.88[.]188, 79.110.52[.]160

Attack Name	TYPE	VALUE
Editbot Stealer	SHA256	3f7bd47fbbf1fb0a63ba955c8f9139d6500b6737e5baf5fdb783f0cedae94d6d
	SHA1	eed59a282588778ffbc772085b03d229a5d99e35
	MD5	669e7ac187fb57c4d90b07d9a6bb1d42
GraphicalProton	SHA256	01B5F7094DE0B2C6F8E28AA9A2DED678C166D615530E595621E692A9C0240732, 34C8F155601A3948DDB0D60B582CFE87DE970D443CC0E05DF48B1A1AD2E42B5E, 620D2BF14FE345EEF618FDD1DAC242B3A0BB65CCB75699FE00F7C671F2C1D869, 773F0102720AF2957859D6930CD09693824D87DB705B3303CEF9EE794375CE13, 7B666B978DBBE7C032CEF19A90993E8E4922B743EE839632BFA6D99314EA6C53, 8AFB71B7CE511B0BCE642F46D6FC5DD79FAD86A58223061B684313966EFEF9C7, 971F0CED6C42DD2B6E3EA3E6C54D0081CF9B06E79A38C2EDE3A2C5228C27A6DC, CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF, CD3584D61C2724F927553770924149BB51811742A461146B15B34A26C92CAD43, EBE231C90FAD02590FC56D5840ACC63B90312B0E2FEE7DA3C7606027ED92600E, F1B40E6E5A7CBC22F7A0BD34607B13E7E3493B8AAD7431C47F1366F0256E23EB, C7B01242D2E15C3DA0F45B8ADEC4E6913E534849CDE16A2A6C480045E03FBEE4, 4BF1915785D7C6E0987EB9C15857F7AC67DC365177A1707B14822131D43A6166, 18101518EAE3EEC6EBE453DE4C4C380160774D7C3ED5C79E1813013AC1BB0B93, 19F1EF66E449CF2A2B0283DBB756850CCA396114286E1485E35E6C672C9C3641, 1E74CF0223D57FD846E171F4A58790280D4593DF1F23132044076560A5455FF8, 219FB90D2E88A2197A9E08B0E7811E2E0BD23D59233287587CCC4642C2CF3D67, 92C7693E82A90D08249EDEAFBCA6533FED81B62E9E056DEC34C24756E0A130A6, B53E27C79EED8531B1E05827ACE2362603FB9F77F53CEE2E34940D570217CBF7,

Attack Name	TYPE	VALUE
GraphicalProton	SHA256	C37C109171F32456BBE57B8676CC533091E387E6BA733FBAA01175C43CFB6EBD, C40A8006A7B1F10B1B42FDD8D6D0F434BE503FB3400FB948AC9AB8DDFA5B78A0, C832462C15C8041191F190F7A88D25089D57F78E97161C3003D68D0CC2C4BAA3, F6194121E1540C3553273709127DFA1DAAB96B0ACFAB6E92548BFB4059913C69
Rhadamanthys stealer	SHA256	bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4

Attack Name	TYPE	VALUE
Pierogi++	SHA1	32d0073b8297cc8350969fd4b844d80620e2273a, 3ae41f7a84ca750a774f777766ccf4fd38f7725a, 42cb16fc35cfc30995e5c6a63e32e2f9522c2a77, 5128d0af7d700241f227dd3f546b4af0ee420bbc, 5e46151df994b7b71f58556c84eeb90de0776609, 60480323f0e6efa3ec08282650106820b1f35d2f, 75a63321938463b8416d500b34a73ce543a9d54d, aeeeee47becaa646789c5ee6df2a6e18f1d25228, da96a8c04edf8c39d9f9a98381d0d549d1a887e8, f3e99ec389e6108e8fda6896fa28a4d7237995be
	Domians	aracaravan[.]com, beatricewarner[.]com, swsan-lina-soso[.]info, zakaria-chotzen[.]info
Micropsia	SHA1	003bb055758a7d687f12b65fc802bac07368335e, 19026b6eb5c1c272d33bda3eab8197bec692abab, 2a45843cab0241cce3541781e4e19428dcf9d949, 5619e476392c195ba318a5ff20e40212528729ba, 745657b4902a451c72b4aab6cf00d05895bbc02f, 95fc3fb692874f7415203a819543b1e0dd495a57, c3038d7b01813b365fd9c5fd98cd67053ed22371
	Domains	bruce-ess[.]com, claire-conway[.]com, delooyp[.]com, izocraft[.]com, jane-chapman[.]com, porthopeminorhockey[.]net, wayne-lashley[.]com
BarbWire	SHA1	4dcdb7095da34b3cef73ad721d27002c5f65f47b, 694fa6436302d55c544cfb4bc9f853d3b29888ef
	Domain	wanda-bell[.]website
Kuiper Ransomware	SHA1	90dd8718560a23faddf99e64b52175d1d765397c
	MD5	84820f3eb491a2fde1f52435cd29646c
	IPv4	91.92.251[.]25
Play Ransomware	MD5	09f341874f72a5cfcedbca707bfd1b3b, 57bcb8cfad510109f7ddedf045e86a70
	SHA256	453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb, 47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57, 75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212,

Attack Name	TYPE	VALUE
Play Ransomware	SHA256	7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986, 7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234af8, 7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40354f8aca, c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c, e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8bf3d5c74, e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da742972999b95da
	SHA1	6e8582faeaf34f63fbe0083a811bcce1aa6c31de, e6c381859f53d0c0db9fcd30fa601ecb935b93e0
	IPv4	85.203.44[.]5, 85.203.44[.]8
MuddyC2Go	SHA256	1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca, 25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a
	IPv4	94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 45.150.64(.)39 , 95.164.46[.]199, 94.131.98[.]14
ODAgent	SHA1	7E498B3366F54E936CB0AF767BFC3D1F92D80687
OilCheck	SHA1	8D84D32DF5768B0D4D2AB8B1327C43F17F182001, DDF0B7B509B240AAB6D4AB096284A21D9A3CB910
OilBooster	SHA1	1B2FEDD5F2A37A0152231AE4099A13C8D4B73C9E
PikaBot	SHA256	0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5, da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff, 69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320
	Domains	anadesky[.]ovmv[.]net, cxtensones[.]top

Attack Name	TYPE	VALUE
PikaBot	IPv4	172[.]232[.]186[.]251, 57[.]128[.]83[.]129, 57[.]128[.]164[.]11, 57[.]128[.]108[.]132, 139[.]99[.]222[.]29, 172[.]232[.]164[.]77, 54[.]37[.]79[.]82, 172[.]232[.]162[.]198, 57[.]128[.]109[.]221
JaskaGO	SHA256	7bc872896748f346fdb2426c774477c4f6dcedc9789a44bd9d3c889f778d5c4b, f38a29d96eee9655b537fee8663d78b0c410521e1b88885650a695aad89dbe3f, 6efa29a0f9d112cfbb982f7d9c0ddfe395b0b0edb885c2d5409b33ad60ce1435, f2809656e675e9025f4845016f539b88c6887fa247113ff60642bd802e8a15d2, 85bffa4587801b863de62b8ab4b048714c5303a1129d621ce97750d2a9a989f9, 37f07cc207160109b94693f6e095780bea23e163f788882cc0263cbddac37320, e347d1833f82dc88e28b1baaa2657fe7ecbfe41b265c769cce25f1c0e181d7e0, c714f3985668865594784dba3aeda1d961acc4ea7f59a178851e609966ca5fa6, 9b23091e5e0bd973822da1ce9bf1f081987daa3ad8d2924ddc87eee6d1b4570d, 1c0e66e2ea354c745aebda07c116f869c6f17d205940bf4f19e0fdf78d5dec26, e69017e410aa185b34e713b658a5aa64bff9992ec1dbd274327a5d4173f6e559, 6cdda60ffbc0e767596eb27dc4597ad31b5f5b4ade066f727012de9e510fc186, 44d2d0e47071b96a2bd160aeed12239d4114b7ec6c15fd451501c008d53783cf, 8ad4f7e14b36ffa6eb7ab4834268a7c4651b1b44c2fc5b940246a7382897c98e, 888623644d722f35e4dcc6df83693eab38c1af88ae03e68fd30a96d4f8cbcc01, 3f139c3fcad8bd15a714a17d22895389b92852118687f62d7b4c9e57763a8867, 207b5ee9d8cbff6db8282bc89c63f85e0ccc164a6229c882ccdf6143ccefdcbc

Attack Name	TYPE	VALUE
Mallox Ransomware	SHA1	3d434b7cc9589c43d986bf0e1cadb956391b5f9a, 9295a02c49aa50475aa7876ca80b3081a361ff7d, 3fa79012dfdac626a19017ed6974316df13bc6ff, 7e7957d7e7fd7c27b9fb903a0828b09cbb44c196, 08a236455490d5246a880821ba33108c4ef00047, 0d2711c5f8eb84bd9915a4191999afd46abca67a, 0e45e8a5b25c756f743445f0317c6352d3c8040a, 11d7779e77531eb27831e65c32798405746ccea1, 246e7f798c3bfba81639384a58fa94174a08be80, 273e40d0925af9ad6ca6d1c6a9d8e669a3bdc376, 2a6f632ab771e7da8c551111e2df786979fd895d, 2c49fa21b0a8415994412fe30e023907f8a7b46e, 33c24486f41c3948fbd761e6f55210807af59a1f, 4c863df8ea7446cb7fba6e582959bc3097f92b5c, 4fcfb65cb757c83ed91bc01b3f663072a52da54b, 5229a5d56836c3d3fc7fb12a43a431b5c90f771d, 552862af77b204ac1f69b9e25937cc60e30e6c0f, 5d0b9521cca0c911d49162e7f416a1463fbaefae, 5d9cc0bc652b1d21858d2e4ddd35303cd9aeb2a3, 63408c84c5d642cf1c5b643a97b84e22e18323c0, 643918830b87691422d6d7bd669c408679411303, 65d7cb5f1770b77b047baf376bd6b4cf86c5d42c, 88eef50d85157f2e0552aab07cac7e7ec21680f5, 88f8629423efe84e2935eb71d292e194be951a16, 9d182e17f88e26cb0928e8d07d6544c2d17e99f5, a8886c9417b648944d2afd6b6c4941588d670e3c, db3fd39fc826e87fa70840e86d5c12eef0fe0566, ee15c76e07051c10059a14e03d18a6358966e290, fb05a6fafc28194d011a909d946b3efa64cdb4cf
	IPv4	104[.]21.76.77, 104[.]237.62.211, 172[.]67.191.103, 64[.]185.227.155, 80[.]66.75.37
MuddyC2Go	SHA256	1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca, 25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a
	IPv4	94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 45.150.64(.)39 , 95.164.46[.]199, 94.131.98[.]14

Attack Name	TYPE	VALUE
Bandook RAT	SHA256	8904ce99827280e447cb19cf226f814b24b0b4eec18dd758e7fb93476b7bf8b8, d3e7b5be903eb9a596b9b2b78e5dd28390c6aadb8bdd4ea1ba3d896d99fa0057, 3169171e671315e18949b2ff334db83f81a3962b8389253561c813f01974670b, e87c338d926cc32c966fce2e968cf6a20c088dc6aedf0467224725ce36c9a525, 2e7998a8df9491dad978dee76c63cb1493945b9cf198d856a395ba0fae5c265a, 430b9e91a0936978757eb8c493d06cbd2869f4e332ae00be0b759f2f229ca8ce, cd78f0f4869d986cf129a6c108264a3517dbcf16ecfc7c88ff3654a6c9be2bca
	IPv4	77.91.100[.]237, 45.67.34[.]219
MetaStealer	Domains	wgcuwcgociewewoo[.]xyz, ockimqekmwecocug[.]xyz, kiqewcsyeyaeusag[.]xyz, cewgwsyookogmmki[.]xyz, startworkremotely[.]com, csyeywqwyikqaiim[.]xyz, iqaeaoeueeqouweo[.]xyz, mmswgeewswyyywqk[.]xyz, accounts[.]google[.]com, iqwgwsigmigiqgoa[.]xyz
	SHA256	949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca, 99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb, c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f
LONEPAGE	SHA256	8aca535047a3a38a57f80a64d9282ace7a33c54336cd08662409352c23507602, 4e8de351db362c519504509df309c7b58b891baf9cb99a3500b92fe0ef772924, a10209c10bf373ed682a13dad4ff3aea95f0fdcd48b62168c6441a1c9f06be37, 39d56eab8adfe9eb244914dde42ec7f12f48836d3ba56c479ab21bdbc41025fe, 96ab977f8763762af26bad2b6c501185b25916775b4ed2d18ad66b4c38bd5f0d,

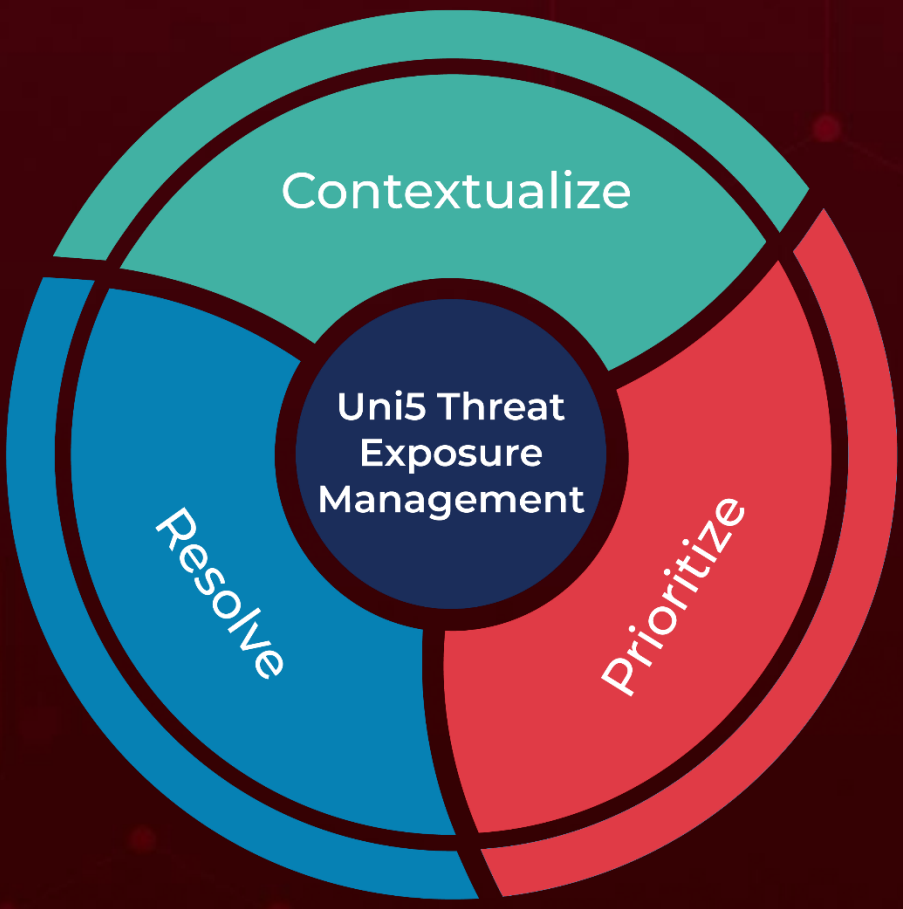
Attack Name	TYPE	VALUE
LONEPAGE	SHA256	e34fc4910458e9378ea357baf045e9c0c21515a0b8818a5b36daceb2af464ea0, 6f5f265110490158df91ca8ad429a96f8af69ca30b9e3b0d9c11d4fef74091e8
SEASPY	MD5	7b83e4bd880bb9d7904e8f553c2736e3
SALTWATER	MD5	d493aab1319f10c633f6d223da232a27
AppleSeed	MD5	db5fc5cf50f8c1e19141eb238e57658c, 6a968fd1608bca7255c329a0701dbf58, cafc26b215550521a12b38de38fa802b, 76831271eb117b77a57869c80bfd6ba6, b5d3e0c3c470d2d41967229e17259c87, 4511e57ae1eacdf1c2922bf1a94bfb8d, 02843206001cd952472abf5ae2b981b2, 8aeacd58d371f57774e63d217b6b6f98, cacf04cd560b70eaaf0e75f3da9a5e8f, 7a7937f8d4dcb335e96db05b2fb64a1b, f3a55d49562e41c7d339fb52457513ba, 5d3ab2baacf2ad986ed7542eeabf3dab, d4ad31f316dc4ca0e7170109174827cf, 1f7d2cbfc75d6eb2c4f2b8b7a3eec1bf, ae9593c0c80e55ff49c28e28bf8bc887, b6f17d59f38aba69d6da55ce36406729, 153383634ee35b7db6ab59cde68bf526, c560d3371a16ef17dd79412f6ea99d3a, 0cce02d2d835a996ad5dfc0406b44b01
	URL	hxxp://bitburny.kro[.]kr/aha/, hxxp://bitthum.kro[.]kr/hu/, hxxp://doma2.o-r[.]kr//, hxxp://my.topton.r-e[.]kr/address/, hxxp://nobtwoseb1.n-e[.]kr//, hxxp://octseven1.p-e[.]kr//, hxxp://tehyeran1.r-e[.]kr//, hxxp://update.ahnlaib.kro[.]kr/aha/, hxxp://update.doumi.kro[.]kr/aha/, hxxp://update.onedrive.p-e[.]kr/aha/, hxxp://yes24.r-e[.]kr/aha/
AlphaSeed	MD5	d94c6323c3f77965451c0b7ebeb32e13, 52ff761212eeaadcd3a95a1f8cce4030, 4cb843f2a5b6ed7e806c69e6c25a1025, b6ab96dc4778c6704b6def5db448a020
Meterpreter	MD5	232046aff635f1a5d81e415ef64649b7, 58fafabd6ae8360c9d604cd314a27159, e582bd909800e87952eb1f206a279e47, ac99b5c1d66b5f0ddb4423c627ca8333

Attack Name	TYPE	VALUE
Meterpreter	IPv4	104.168.145[.]83:993, 159.100.6[.]137:993, 38.110.1[.]69:993, 107.148.71[.]88:993
TinyNuke	MD5	e34669d56a13d607da1f76618eb4b27e
	IPv4	45.114.129[.]138:33890

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

January 11, 2024 . 10:00 PM

More at www.hivepro.com