Date of Publication
January 3, 2025

Hive Pro

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

DECEMBER 2024

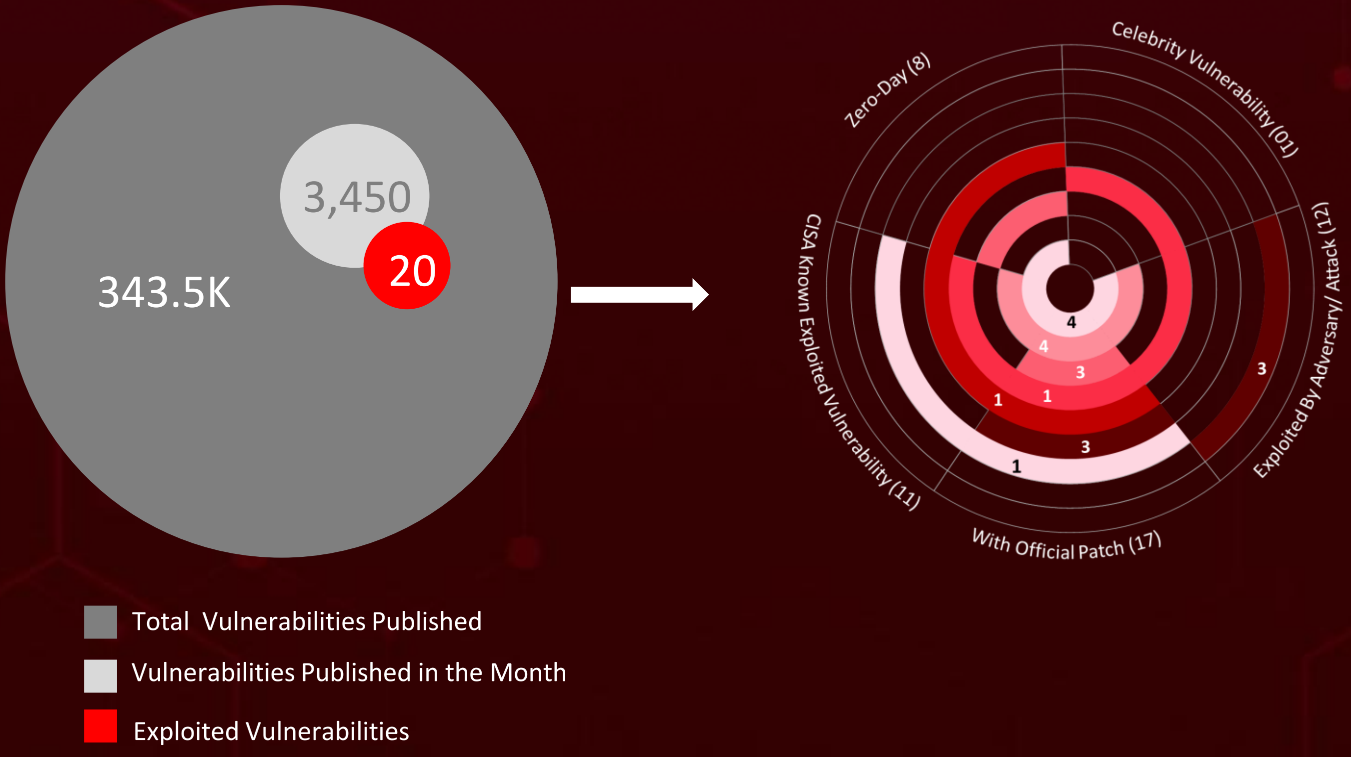
Table Of Contents

Summary

December saw a surge in cybersecurity threats, with the discovery of **eight** zero-day vulnerabilities and critical flaws in widely used platforms. Notably, two critical zero-day vulnerabilities **CVE-2024-50623** and **CVE-2024-55956** were identified in Cleo's file transfer products Harmony, VLTrader, and LexiCom. These vulnerabilities, currently being exploited by threat actors, allow unrestricted file uploads and downloads, potentially enabling remote code execution (RCE). Organizations using these tools for secure file transfers are at significant risk, with the **Cl0p ransomware** gang actively targeting these flaws.

Ransomware attacks also spiked in December, with groups like **Helldown** and **Black Basta** leading aggressive campaigns. These incidents underscore the growing complexity of ransomware tactics, highlighting the critical need for strong backup systems, disaster recovery plans, and continuous employee training to identify and avoid phishing attempts.

In addition, at least **eight** distinct threat actors carried out targeted operations throughout the month. Among them was **Secret Blizzard**, also known as Turla, a Russian cyber-espionage group that has leveraged tools and infrastructure from at least six other threat actors over the past seven years. Known for maintaining long-term access to systems, Turla deploys advanced backdoors like **TwoDash** and **TinyTurla**, often focusing on politically sensitive intelligence and cutting-edge research. Meanwhile, **Cloud Atlas** introduced a sophisticated, previously unknown toolset, using phishing emails to exploit a known vulnerability. This attack chain drops malicious files, such as the **VBShower** and **PowerShower** backdoors, allowing attackers to infiltrate systems with stealth.



Insights

In December 2024, a geopolitical cybersecurity landscape unfolds, revealing **Russia, United States, France,** and **Germany** as the top-targeted countries

Highlighted in **December 2024** is a cyber battleground encompassing the **Government, Healthcare,** and **Defense** sectors, designating them as the top industries

SmokeLoader evolves into a dual threat, serving as an initial access vector and operational menace

Horns&Hooves campaign, deceives Russian users with malware-laden business documents, leveraging malicious JScript files to deploy NetSupport RAT

Botnets Exploit

Unpatched D-Link routers remain under siege as botnets like FICORA and CAPSAICIN exploit vulnerabilities in the Home Network Administration Protocol (HNAP)

Earth Koshchei

orchestrates a sophisticated RDP attack campaign, blending spear-phishing tactics with malicious RDP configuration files

Elpaco ransomware

offshoot of Mimic Leveraging brute-force RDP attacks and exploiting the critical Zerologon vulnerability (CVE-2020-1472) for privilege escalation

Secret Blizzard

has harnessed tools and infrastructure from at least six other threat actors, employing advanced backdoors like TwoDash and TinyTurla

Zero-day Flaws CVE-2024-50623 and CVE-2024-55956 in Cleo's file transfer products actively exploited by the Cl0p ransomware gang

CVE-2023-34990 a critical path traversal flaw. Exploited via crafted web requests, this flaw allows remote attackers to execute unauthorized code or commands, potentially leading to full device compromise

Threat Landscape

20 Vulnerabilities

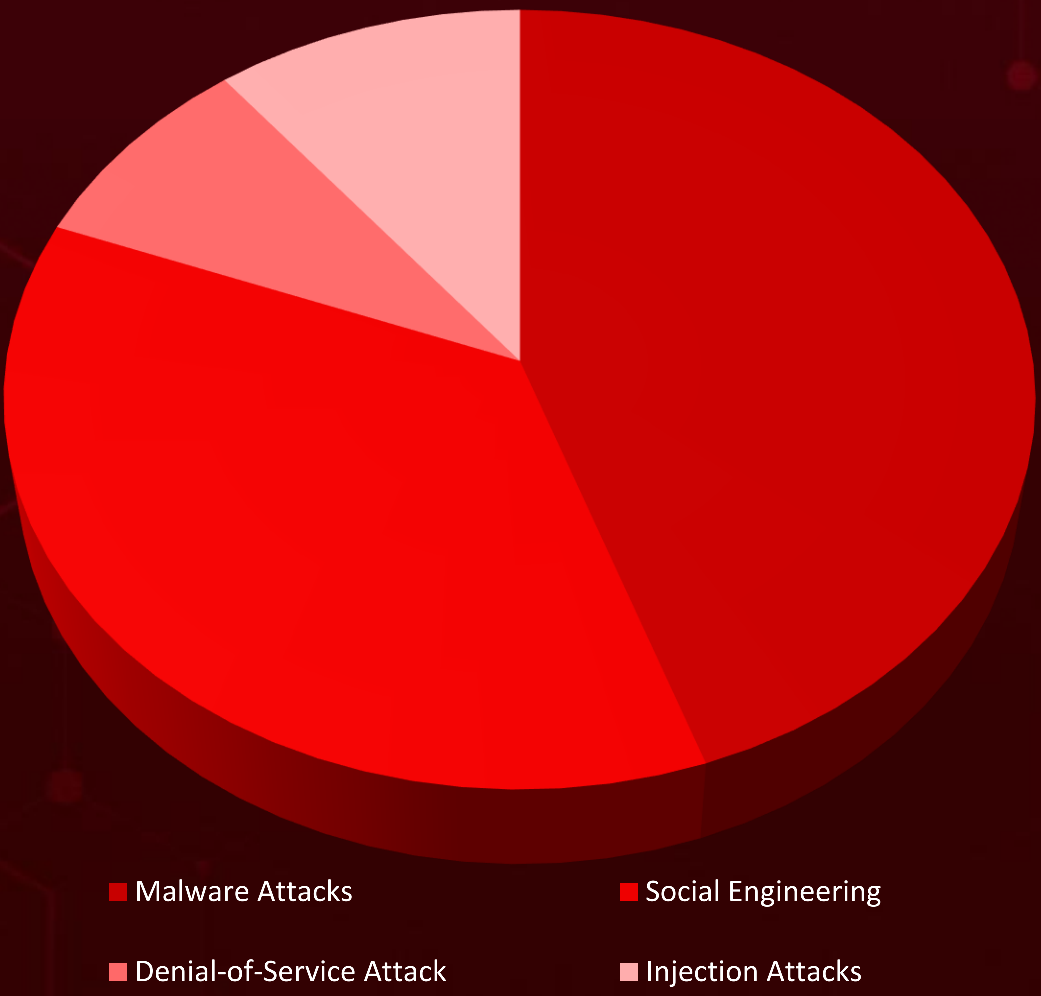
162 MITRE ATT&CK TTPs

24 Industries

8 Adversaries

219 Countries

34 Attacks



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	✗	Microsoft Netlogon	-
	CISA KEV		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	Elpaco ransomware
Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-330	T1068: Exploitation for Privilege Escalation, T1210: Exploitation of Remote Services	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2017-0199	Microsoft Office And WordPad Remote Code Execution Vulnerability	Microsoft Office and WordPad	✓	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓
CVE-2024-11667	Zyxel Multiple Firewalls Path Traversal Vulnerability	Zyxel Firewalls	✗	✓	✓
CVE-2024-45841	I-O DATA DEVICE UD-LT1/EX Incorrect Permission Assignment for Critical Resource Vulnerability	UD-LT1, UD-LT1/EX	✓	✗	✓
CVE-2024-47133	I-O DATA DEVICE UD-LT1/EX OS Command Injection Vulnerability	UD-LT1, UD-LT1/EX	✓	✗	✓
CVE-2024-52564	I-O DATA DEVICE UD-LT1/EX Inclusion of Undocumented Features Vulnerability	UD-LT1, UD-LT1/EX	✓	✗	✓
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	✗	✓	✓
CVE-2024-50623	Cleo Multiple Products Unrestricted File Upload Vulnerability	Cleo Harmony, Cleo VLTrader, Cleo LexiCom	✓	✓	✓
CVE-2024-49138	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows	✓	✓	✓
CVE-2024-55956	Cleo Multiple Products Remote Code Execution Vulnerability	Cleo Harmony, Cleo VLTrader, Cleo LexiCom	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-53677	Apache Struts Remote Code Execution Vulnerability	Apache Struts	✗	✗	✓
CVE-2023-34990	Fortinet FortiWLM Relative Path Traversal Vulnerability	Fortinet FortiWLM	✗	✗	✓
CVE-2018-0802	Microsoft Office Memory Corruption Vulnerability	Microsoft Office and Word	✓	✓	✓
CVE-2024-3393	Palo Alto Networks Denial of Service (DoS) Vulnerability	PAN-OS	✗	✓	✓
CVE-2024-52046	Apache MINA Remote Code Execution Vulnerability	Apache MINA	✗	✗	✓
CVE-2015-2051	D-Link DIR-645 Router Remote Code Execution Vulnerability	D-Link DIR-645 Router	✗	✓	✓
CVE-2019-10891	D-Link DIR-806 Router Command Injection Vulnerability	D-Link DIR-806 Router	✗	✗	✗
CVE-2022-37056	D-Link Go-RT-AC750 Command Injection Vulnerability	D-Link Go-RT-AC750 Router	✗	✗	✗
CVE-2024-33112	D-Link DIR-845L router Command Injection Vulnerability	D-Link DIR-845L router	✗	✗	✗

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SmokeLoader	Loader	CVE-2017-0199 CVE-2017-11882	Microsoft Office	✓	Phishing
Helldown	Ransomware	CVE-2024-11667	Zyxel Multiple Firewalls	✓	Exploitation of vulnerabilities in Zyxel
NetSupport RAT	RAT	-	Windows	-	Phishing
BurnsRAT	RAT	-	Windows	-	Phishing
RevC2	Backdoor	-	-	-	Phishing
Venom	Loader	-	-	-	Phishing
Elpaco	Ransomware	-	-	-	Phishing
Termite	Ransomware	-	-	-	Phishing
Realst Stealer	Stealer	-	-	-	Social Engineering
Black Basta	Ransomware	-	-	-	-
Zbot	Loader	-	-	-	Social Engineering
DarkGate	Loader	-	-	-	Social Engineering
Mauri	Ransomware	CVE-2023-46604	Apache ActiveMQ	✓	Exploiting Vulnerability
Quasar RAT	RAT	CVE-2023-46604	Apache ActiveMQ	✓	Exploiting Vulnerability
TinyTurla	Backdoor	-	-	-	Social Engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
TwoDash	Downloader	-	-	-	-
Wainscot	Backdoor	-	-	-	-
CrimsonRAT	Backdoor	-	-	-	Phishing
PUMAKIT	Rootkit, loader	-	-	-	-
Cl0p	Ransomware	CVE-2024-50623 CVE-2024-55956	Cleo Harmony, Cleo VLTrader, Cleo LexiCom	✓	Exploiting Vulnerabilities
VIPKeyLogger	Infostealer	CVE-2017-11882	Windows	✓	Phishing emails
Yokai	Backdoor	-	-	-	-
WmRAT	RAT	-	Windows	-	Spear-phishing emails
MiyaRAT	RAT	-	Windows	-	Spear-phishing emails
VBShower	Backdoor	CVE-2018-0802	Microsoft Office and Word	✓	Phishing and Exploit vulnerabilities
VBCloud	Backdoor	CVE-2018-0802	Microsoft Office and Word	✓	Phishing and Exploit vulnerabilities
PowerShower	Backdoor	CVE-2018-0802	Microsoft Office and Word	✓	Phishing and Exploit vulnerabilities
BellaCPP	Trojan	-	Windows	-	Phishing
BellaCiao	Dropper Trojan	-	Windows	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
OtterCookie	Backdoor	-	-	-	Phishing
PlugX	Loader	-	-	-	Phishing
Rakshasa	Hack tool	-	-	-	Phishing
FICORA	Botnet	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112	D-Link DIR-645 Router, D-Link DIR-806 Router, D-Link Go-RT- AC750 Router, D-Link DIR-845L router	✓	Exploiting Vulnerabilities
CAPSAICIN	Botnet	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112	D-Link DIR-645 Router, D-Link DIR-806 Router, D-Link Go-RT- AC750 Router, D-Link DIR-845L router	✓	Exploiting Vulnerabilities

Adversaries Summary

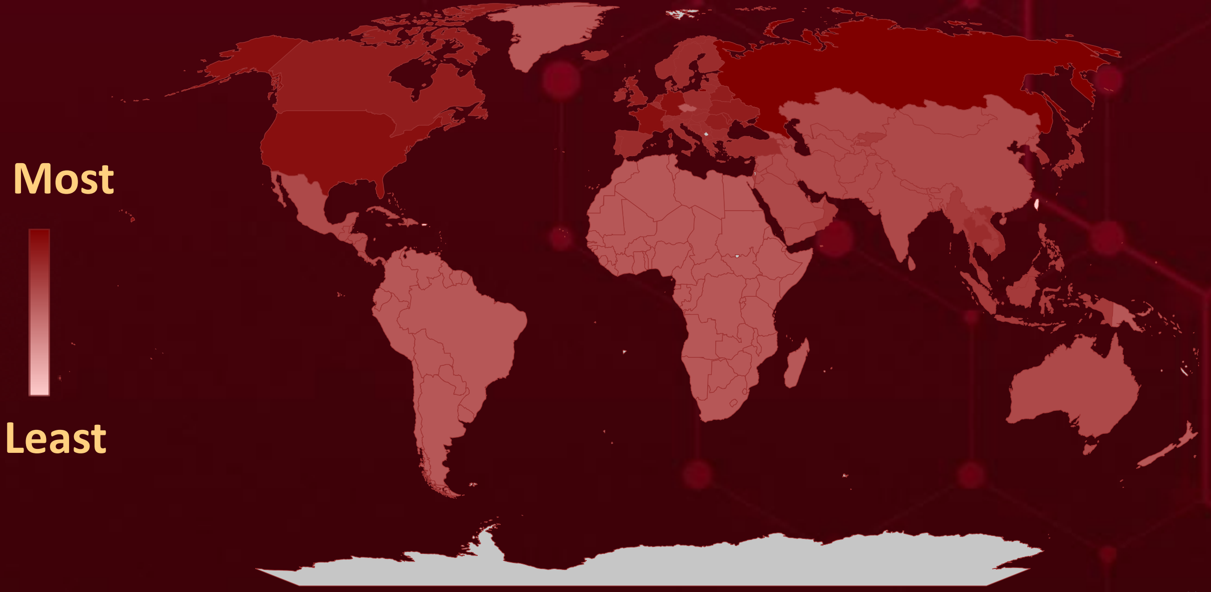
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
TA569	Information theft and espionage	-	-	NetSupport RAT, BurnsRAT	Windows
Kimsuky	Information theft and espionage	North Korea	-	-	-
Venom Spider	Financial gain	Russia	-	RevC2, Venom Loader	-
Secret Blizzard	Information theft and espionage	Russia	-	TinyTurla, TwoDash, Wainscot, CrimsonRAT	-
TA397	Information theft and espionage	-	-	WmRAT and MiyaRAT	Windows
Earth Koshchei	Information theft and espionage	Russia	-	-	-
Cloud Atlas	Information theft and espionage	Russia	-	VBShower, VBCloud, PowerShow er	-
Charming Kitten	nformation theft and espionage	Iran	-	BellaCiao, BellaCPP	Windows

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Microsoft	Application	Microsoft WordPad
		Microsoft Office: 2007 SP3 2010 SP2 2013 SP1 2016
		Microsoft Office: 2007 - 2016 Microsoft Word: 2007 - 2016
	Server	Microsoft Netlogon
	Server	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025
ZYXEL NETWORKS	Firewall	Zyxel ATP series Version 5.00 - 5.38, Zyxel USG FLEX series Version 5.00 - 5.38, Zyxel USG FLEX 50W Version 5.10 - 5.38, Zyxel USG20W-VPN Version 5.10 - 5.38
I-O DATA	Router	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier
STRUTS	Framework	Struts Version 2.0.0 – Struts 2.3.37 (EOL), Struts Version 2.5.0 - Struts 2.5.33, Struts Version 6.0.0 - Struts 6.3.0.2
Cleo	Software	Cleo Harmony (versions upto 5.8.0.21) Cleo VLTrader (versions upto 5.8.0.21) Cleo LexiCom (versions upto 5.8.0.21)

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Software	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16
FORTINET	Application	FortiWLM 8.5: Versions 8.5.0 through 8.5.4 FortiWLM 8.6: Versions 8.6.0 through 8.6.5
paloalto NETWORKS	Firewall	PAN-OS 11.2: Versions below 11.2.3; PAN-OS 11.1: Versions below 11.1.5; PAN-OS 10.2: Versions upto 10.2.8, Versions below 10.2.10- h12 and Versions below 10.2.13-h2; PAN-OS 10.1: Versions upto 10.1.14 and Versions below 10.1.14-h8

Targeted Countries



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Color	Countries
🟥	Russia
🟥	United States
🟥	France
🟥	Germany
🟥	Moldova
🟥	Romania
🟥	Netherlands
🟥	Ukraine
🟥	Canada
🟥	Belarus
🟥	United Kingdon
🟥	Slovenia
🟥	Norway
🟥	Monaco
🟥	Estonia
🟥	Czech Republic (Czechia)
🟥	Finland
🟥	Switzerland
🟥	Austria
🟥	Andorra
🟥	Albania

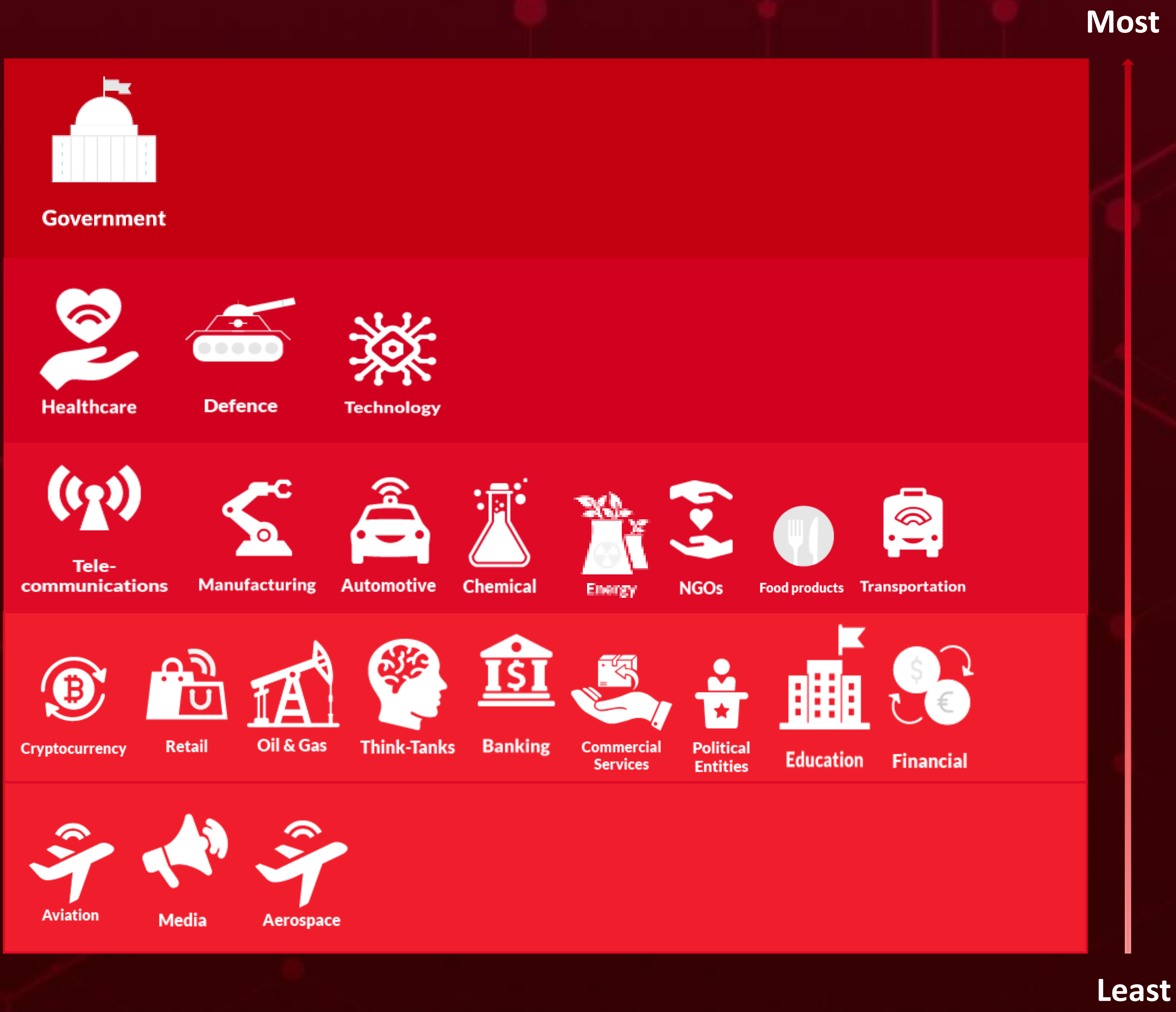
Color	Countries
🟥	Portugal
🟥	Greece
🟥	Serbia
🟥	Holy See
🟥	Spain
🟥	Hungary
🟥	Turkey
🟥	Iceland
🟥	Montenegro
🟥	Ireland
🟥	North Macedonia
🟥	Italy
🟥	Poland
🟥	Japan
🟥	Croatia
🟥	Latvia
🟥	San Marino
🟥	Belgium
🟥	Slovakia
🟥	Bosnia and Herzegovina
🟥	South Korea

Color	Countries
🟥	Lithuania
🟥	Sweden
🟥	Luxembourg
🟥	Thailand
🟥	Malta
🟥	Denmark
🟥	Bulgaria
🟥	Vietnam
🟥	Liechtenstein
🟥	Laos
🟥	Indonesia
🟥	Singapore
🟥	Oman
🟥	Myanmar
🟥	Philippines
🟥	Malaysia
🟥	Israel
🟥	Brunei
🟥	Cambodia
🟥	Kyrgyzstan
🟥	Cyprus
🟥	Lithuania
🟥	Sweden
🟥	Luxembourg

Color	Countries
🟥	Lebanon
🟥	Uzbekistan
🟥	Belize
🟥	Saint Lucia
🟥	Bhutan
🟥	Kazakhstan
🟥	Antigua and Barbuda
🟥	Timor-Leste
🟥	Maldives
🟥	El Salvador
🟥	Georgia
🟥	Saudi Arabia
🟥	Mexico
🟥	Armenia
🟥	Azerbaijan
🟥	State of Palestine
🟥	Bahamas
🟥	Tajikistan
🟥	Mongolia
🟥	Dominica
🟥	Grenada
🟥	Lebanon

Color	Countries
🟥	Nepal
🟥	Barbados
🟥	Haiti
🟥	Cuba
🟥	Nicaragua
🟥	Jamaica
🟥	North Korea
🟥	Jordan
🟥	Bahrain
🟥	Sri Lanka
🟥	Honduras
🟥	Kuwait
🟥	Bangladesh
🟥	Syria
🟥	Pakistan
🟥	Australia
🟥	Panama
🟥	Trinidad and Tobago
🟥	China
🟥	Turkmenistan
🟥	India
🟥	Nepal

Targeted Industries



Most

Government

Healthcare
Defence
Technology

Telecommunications
Manufacturing
Automotive
Chemical
Energy
NGOs
Food products
Transportation

Cryptocurrency
Retail
Oil & Gas
Think-Tanks
Banking
Commercial Services
Political Entities
Education
Financial

Aviation
Media
Aerospace

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	T1588 Obtain Capabilities	T1027 Obfuscated Files or Information	T1036 Masquerading	T1566 Phishing
T1082 System Information Discovery	T1190 Exploit Public-Facing Application	T1588.006 Vulnerabilities	T1041 Exfiltration Over C2 Channel	T1547.001 Registry Run Keys / Startup Folder
T1204.002 Malicious File	T1204 User Execution	T1070 Indicator Removal	T1059.001 PowerShell	T1071 Application Layer Protocol
T1564 Hide Artifacts	T1005 Data from Local System	T1203 Exploitation for Client Execution	T1547 Boot or Logon Autostart Execution	T1083 File and Directory Discovery
T1068 Exploitation for Privilege Escalation	T1105 Ingress Tool Transfer	T1053 Scheduled Task/Job	T1566.001 Spearphishing Attachment	T1033 System Owner/User Discovery

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
SmokeLoader	SHA256	f7544f07b4468e38e36607b5ac5b3835eac1487e7d16dd52ca882b3d021c19b6
Elpaco Ransomware	SHA256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f, e160d7d21c917344f010e58dcfc1e19bec6297c294647a06ce60efc7420d3b13
Helldown Ransomware	SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbbdcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93ddd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1, 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19, cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, 67aea3de7ab23b72e02347cbf6514f28fb726d313e62934b5de6d154215ee733, 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0, 6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd, 9ab19741ac36e198fb2fd912620bf320aa7fdeeeb8d4a9e956f3eb3d2092c92c, ccd78d3eba6c53959835c6407d81262d3094e8d06bf2712fefa4b04baadd4bfe
Termite	MD5	6b06aae5ec596cdbc1b9d4c457fd5f81
	SHA1	a515b7d89676b1401eeb9eb776190a1179c386cf
	SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55
	TOR Address	termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion

Attack Name	TYPE	VALUE
Black Basta	SHA1	a6d653d2887f0ce4029a94616464ad74c4f770fe, 0fbed8d60e2d940882e01a2bf11003f6bd59f883, 22f10e42683501fb2ea6962e44eefd64848aefe7
	SHA256	ec669387150865b59bbf98b41a770235ba4fd632aab33433c2d493460ef52479, 95a6c06ac691bec0ac2140b6590c96488feb8bc6c3ca501d1fe8ee7cbf9d0f8b
PUMAKIT	SHA256	30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f, cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe, 8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03
	Domains	sec[.]opsecurity1[.]art, rhel[.]opsecurity1[.]art
	IPv4	89[.]23[.]113[.]204
Cl0p	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8
	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56
VIPKeyLogger	SHA256	b7d62d77cace855288bf6b463f8ad783316594f90dad78d97a7ea85be58b8bc3, d854f347061d9d7b8a9788ab8633c3f07619e29bd440924507a0147484c217c3
Yokai	SHA256	eaae6d5dbf40239fb5abfa2918286f4039a3a0fcd28276a41281957f6d850456, 3e5cfe768817da9a78b63efad9e60d2d300727a97476edf87be088fb26f06500, 1626ce79f2b96c126cbdb00195dd8509353e8754b1a0ce88d359fa890acd6676, 2852223eb40cf0dae4111be28ce37ce9af23e5332fb78b47c8f5568d497d2611
BellaCPP	MD5	222380fa5a0c1087559abbb6d1a5f889
	SHA1	dccdfc77dd2803b3c5a97af0851efa0aa5bbeeeb
	SHA256	e4e3f09c4257269cef6cfbebc83c8a60376ce5e547080502e3e408a3f9916218
	File name	adhapl.dll

Attack Name	TYPE	VALUE
BellaCiao	MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcdb6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7, 5f4284115ab9641f1532bb64b650aad6, 0fea857a35b972899e8f1f60ee58e450, 20014b80a139ed256621b9c0ac4d7076, 7f0ee078c8902f12d6d9e300dabf6aed, 63647520b36144e31fb8ad7dd10e3d21, 8096e00aa7877b863ef5a437f55c8277, 12ab1bc0989b32c55743df9b8c46af5a, 50dc5faa02227c0aefa8b54c8e5b2b0d, e760a5ce807c756451072376f88760d7, b03c67239e1e774077995bac331a8950, ba69cc9f087411995c64ca0d96da7b69, 051552b4da740a3af5bd5643b1dc239a, edfb8d26fa34436f2e92d5be1cb5901b, 3e86f6fc7ed037f3c9560cc59aa7aacc, ae4d6812f5638d95a82b3fa3d4f92861, 67677c815070ca2e3ebd57a6adb58d2e, 17a78f50e32679f228c43823faabedfd, b9956282a0fed076ed083892e498ac69, 1b41e64c60ca9dfadeb063cd822ab089
OtterCookie	SHA256	d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fcef13ad2106, 7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e, 4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79, 32257fb11cc33e794fdfd0f952158a84b4475d46f531d4bee06746d15caf8236
	Domains	zkservice[.]cloud, w3capi[.]marketing, payloadrpc[.]com
	IPv4	45[.]159[.]248[.]55

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0199	✗	Microsoft Office and WordPad	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	SmokeLoader
Microsoft Office and WordPad Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1204 : User Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗	Microsoft Office: 2007 SP3 2010 SP2 2013 SP1 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*	SmokeLoader, VIPKeyLogger
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203 : Exploitation for Client Execution, T1059 : Command and Scripting Interpreter, T1204 : User Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11667	✗	Zyxel ATP series Version 5.00 - 5.38, Zyxel USG FLEX series Version 5.00 - 5.38, Zyxel USG FLEX 50W Version 5.10 - 5.38, Zyxel USG20W-VPN Version 5.10 - 5.38	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:atp_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:usg_flex_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:usg_flex_50w_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:zyxel:usg20-vpn_firmware:*:*:*:*:*:*:*:*	Helldown Ransomware
Zyxel Multiple Firewalls Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting, T1136 : Create Account	https://www.zyxel.com/us/en-us/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-45841	✗	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*:*:*	-
I-O DATA DEVICE UD-LT1/EX Incorrect Permission Assignment for Critical Resource Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-732	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://www.iodata.jp/support/information/2024/11_ud-lt1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-47133	✗	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*:*:*	-
I-O DATA DEVICE UD-LT1/EX OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://www.iodata.jp/support/information/2024/11_ud-lt1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-52564	✗	UD-LT1 firmware Ver.2.1.8 and earlier UD-LT1/EX firmware Ver.2.1.8 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:i-o_data:ud-lt1:*:*:*:*:*:*:* cpe:2.3:h:i-o_data:ud-lt1_ex:*:*:*:*:*:*:*	-
I-O DATA DEVICE UD-LT1/EX Inclusion of Undocumented Features Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1242	T1059: Command and Scripting Interpreter	https://www.iodata.jp/support/information/2024/11_ud-lt1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46604	✗	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*:*:*	Mauri ransomware, Quasar RAT
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories.data/CVE-2023-46604

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-50623</td><td>✗</td><td rowspan="2">Cleo Harmony (versions upto 5.8.0.21)
Cleo VLTrader (versions upto 5.8.0.21)
Cleo LexiCom (versions upto 5.8.0.21)</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✓</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>CISA KEV</b></td><td rowspan="2">cpe:2.3:a:cleo:vltrader:*:*:*:*:*:*:*:*
cpe:2.3:a:cleo:lexicom:*:*:*:*:*:*:*:*
cpe:2.3:a:cleo:harmomy:*:*:*:*:*:*:*:*</td><td rowspan="2">Cl0p</td></tr>
<tr><td rowspan="3">Cleo Multiple Products Unrestricted File Upload Vulnerability</td><td>✓</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-434</td><td>T1059: Command and Scripting Interpreter; T1105: Ingress Tool Transfer</td><td>https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623 , https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49138	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Common Log File System Driver Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55956	☒	Cleo Harmony (prior to version 5.8.0.24) Cleo VLTrader (prior to version 5.8.0.24) Cleo LexiCom (prior to version 5.8.0.24)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cleo:vltrader:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:lexicom:*:*:*:*:*:*:*:* cpe:2.3:a:cleo:harmomy:*:*:*:*:*:*:*:*	Cl0p
Cleo Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956 , https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53677	⊗	Struts Version 2.0.0 - Struts 2.3.37 (EOL), Struts Version 2.5.0 - Struts 2.5.33, Struts Version 6.0.0 - Struts 6.3.0.2	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:struts:*:*:*:*:*:*:*:*	-
Apache Struts Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://struts.apache.org/download.cgi

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34990	⊗	FortiWLM 8.5: Versions 8.5.0 through 8.5.4 FortiWLM 8.6: Versions 8.6.0 through 8.6.5	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiwlm:*:*:*:*:*:*:*:*	-
Fortinet FortiWLM Relative Path Traversal Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://www.fortiguard.com/psirt/FG-IR-23-144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0802	✗	Microsoft Office: 2007 - 2016 Microsoft Word: 2007 - 2016	Cloud Atlas
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:word:*:*:*:*:*:*	VBShower, VBCloud, PowerShower
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1204 : User Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR

CVE-2024-3393	✗	PAN-OS 11.2: Versions below 11.2.3;
		PAN-OS 11.1: Versions below 11.1.5;
		PAN-OS 10.2: Versions upto 10.2.8, Versions below 10.2.10-h12 and Versions below 10.2.13-h2;
		PAN-OS 10.1: Versions upto 10.1.14 and Versions below 10.1.14-h8
			-

	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks Denial of Service (DoS) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-754	T1498 : Network Denial of Service, T1068 : Exploitation for Privilege Escalation	https://security.paloaltonetworks.com/CVE-2024-3393

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-52046	✗	Apache MINA 2.0 through 2.0.26, Apache MINA 2.1 through 2.1.9, Apache MINA 2.2 through 2.2.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apache:mina:*:*:*:*:*:*	-
Apache MINA Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://mina.apache.org/downloads-mina_2_0.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-2051	✗	D-Link DIR-645 Router	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-645_firmware:*:*:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link DIR-645 Router Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-10891	⊗	D-Link DIR-806 Router	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-806_firmware:-:*:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link DIR-806 Router Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-37056	⊗	D-Link Go-RT-AC750 Router	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:go-rt-ac750_firmware:reva_1.01b03:*:*:*:*:*:*:* cpe:2.3:o:dlink:go-rt-ac750_firmware:revb_2.00b02:*:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link Go-RT-AC750 Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-33112	☒	D-Link DIR-845L router	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:d-link:dir-845l:*:*:*:*:*:*:*:*	FICORA and CAPSAICIN
D-Link DIR-845L router Command Injection Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	EOL

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SmokeLoader (aka Dofoil, Sharik, Smoke)	SmokeLoader can be used to drop other malware on infected systems, but operators can choose additional modules that allow for information-stealing capabilities.	Phishing	CVE-2017-0199 CVE-2017-11882
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft, System compromised and Espionage	Microsoft Office
Loader			**PATCH LINK**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199; https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Helldown	Helldown ransomware utilizes a double extortion approach, encrypting data while simultaneously threatening to expose sensitive information unless the ransom is paid. Although Helldown shares code similarities with LockBit 3.0, it remains a distinct variant and is actively being developed.	Exploitation of vulnerabilities in Zyxel	CVE-2024-11667
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Financial Loss, Data Breaches and Reputation Damage	Zyxel Multiple Firewalls
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.zyxel.com/us/en-us/support/download

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
NetSupport RAT	NetSupport RAT (Remote Access Trojan) is a legitimate remote administration tool often exploited for malicious purposes. Cybercriminals use it to gain control over compromised systems, enabling them to execute commands, transfer files, and monitor activity.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote control and System compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
TA569			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BurnsRAT	BurnsRAT is a malicious Remote Access Trojan (RAT) that allows attackers to control compromised systems remotely. It supports executing commands, transferring files, and interacting with desktops via Remote Desktop Protocol (RDP).	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote control and System compromise	Windows
RAT			
ASSOCIATED ACTOR			PATCH LINK
TA569			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RevC2	RevC2 is a recently discovered information-stealing backdoor malware that leverages WebSockets to communicate with its command-and-control (C2) server. It is capable of stealing cookies and passwords, proxying network traffic, and enabling remote code execution (RCE).	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft and Data exfiltration	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Venom Spider			-

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
Venom	Venom Loader is a sophisticated malware loader designed to deliver and execute additional malicious payloads on compromised systems. It's part of the Venom Spider malware-as-a-service (MaaS) toolkit, a collection of cybercriminal tools offered by threat actors to other cybercriminals.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft and Loads other malware	-
Loader			
ASSOCIATED ACTOR			PATCH LINK
Venom Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Elpaco (aka ELPACO-team)	Elpaco is a new variant of the Mimic ransomware family. Employs advanced tactics like abusing legitimate tools and exploiting vulnerabilities. It's a powerful and evolving threat that uses various techniques to compromise systems and encrypt files.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Financial Loss, Data Breaches and Reputation Damage	-
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
Venom Spider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Termite	Termite Ransomware is a variant of the notorious Babuk ransomware, designed to encrypt targeted files on infected systems. Once executed, it appends the .termite extension to affected files, rendering them inaccessible. Victims also find a ransom note titled "How To Restore Your Files.txt", which provides minimal details about the attack.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt 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
Realst	Realst Stealer is a sophisticated infostealer written in Rust, specifically designed to target macOS users. This malware focuses on exfiltrating sensitive information, including stored passwords, browser data, and cryptocurrency wallets. Realst Stealer can extract credentials from the macOS Keychain, harvest data from popular Chromium-based browsers, and compromise widely used cryptocurrency wallets, posing a significant risk to users' digital assets and personal information.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Black Basta	Black Basta is a ransomware-as-a-service (RaaS) variant that was first identified in April 2022. They employ a double-extortion model, where they not only encrypt the victim's systems but also exfiltrate data. This dual approach increases the pressure on victims to pay the ransom, as they face the threat of data leaks in addition to system inaccessibility.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATE D ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Zbot	Zbot is a notorious malware family that primarily targets Microsoft Windows systems to steal financial data. It operates as a financial services Trojan, using sophisticated techniques like website monitoring and keylogging to capture sensitive banking credentials. The malware records keystrokes, bypassing robust security measures. This capability allows Zbot to steal login information directly as users enter it, compromising accounts and financial transactions with ease.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft	-
ASSOCIATE D 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
DarkGate	DarkGate is a powerful and adaptable malware loader equipped with advanced features, making it a popular tool in the cybercrime landscape. Its capabilities include downloading and executing files directly in memory, operating a Hidden Virtual Network Computing (HVNC) module, logging keystrokes, stealing sensitive information, and escalating privileges on compromised systems. DarkGate leverages legitimate AutoIt files to evade detection, often executing multiple AutoIt scripts as part of its operations.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Steal Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mauri	Mauri ransomware employs AES-256 CTR encryption to lock files, rendering them inaccessible and leaving behind ransom notes. It targets a broad spectrum of file types while deliberately avoiding system-critical paths to maintain operational integrity. In addition to encryption, Mauri ransomware operators use proxy tools like FRP (Fast Reverse Proxy) to expose private network services, such as Remote Desktop Protocol (RDP), to external access.	Exploiting Vulnerability	CVE-2023-46604
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Apache ActiveMQ
ASSOCIATE D ACTOR			**PATCH LINK**
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604

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
Quasar RAT	Quasar RAT is a remote access trojan (RAT) written in .NET, designed to target Windows devices. Known for being open-source and fully functional, it has become a popular tool among attackers due to its accessibility and flexibility. While its open-source nature allows legitimate use, cybercriminals frequently pack the malware to obfuscate its source code and hinder analysis. Once deployed, Quasar RAT enables attackers to gain unauthorized remote control of infected systems. Its capabilities include spying on victims, stealing sensitive information, and deploying additional malware.	Exploiting Vulnerabilities	CVE-2023-46604
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise, Deploy another malware	Apache ActiveMQ
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TinyTurla	TinyTurla is a highly covert backdoor that disguises itself as the legitimate Windows Time service (W32Time). By mimicking the behavior of W32Time, the malware avoids detection while carrying out its malicious activities. TinyTurla replicates the service's legitimate functionalities but adds the capability to upload, execute, and exfiltrate files. It can also download additional malware, making it a versatile tool for attackers.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Secret Blizzard			-

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
TwoDash	TwoDash is a covert malware that combines the characteristics of a trojan and a downloader, enabling it to infiltrate systems undetected. Upon infection, TwoDash collects detailed system information and establishes a connection to a hard-coded command and control (C2) server via port 9443. It proceeds to download and install various programs, including additional malware, onto the compromised device.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader		Downloads other malware	-
ASSOCIATED ACTOR			PATCH LINK
Secret Blizzard			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Wainscot	Wainscot is a backdoor written in Golang, designed to provide attackers with extensive control over compromised systems. Once deployed, it connects to a command-and-control (C2) server and is capable of executing a variety of commands. Key functionalities include launching arbitrary commands, uploading and downloading files, and capturing screenshots from the infected host.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Secret Blizzard			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CrimsonRAT	Crimson RAT once installed, it allows attackers to remotely control infected systems, steal sensitive, and spy on users. The malware can also lock infected computers, take full control, and demand extortion payments.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Secret Blizzard			-

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
PUMAKIT	PUMAKIT is a sophisticated loadable kernel module (LKM) rootkit that uses advanced stealth techniques to hide its presence and communicate with C2 servers. It hooks 18 syscalls and kernel functions through an internal function tracer (ftrace), enabling manipulation of core system behaviors. Key features include privilege escalation via the rmdir() syscall, hiding files and directories, evading detection, and anti-debugging measures. The malware combines a dropper, memory-resident executables, an LKM rootkit, and an SO userland rootkit, activating only under specific conditions.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Rootkit, loader		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cl0p	Clop is a type of ransomware that is known for encrypting a victim's files and appending the ".clop“ extension to them. One distinctive feature of Clop ransomware is the string "Dont Worry C|0P“ that is often included in the ransom notes left behind for the victim. Clop is known to attempt to disable Windows Defender and remove Microsoft Security Essentials from the infected system, aiming to evade detection by security software running in the userspace.	Exploiting Vulnerabilities	CVE-2024-50623 CVE-2024-55956
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	Cleo Harmony, Cleo VLTrader, Cleo LexiCom
ASSOCIATED ACTOR			PATCH LINK
-			https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956 , https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623

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 CVE
VIPKeyLogger	VIPKeyLogger is a newly identified infostealer malware resembling the notorious Snake Keylogger. This malware captures keystrokes, login credentials, and other sensitive system data. To avoid detection by conventional security software, VIPKeyLogger uses advanced obfuscation methods.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Infostealer		Information Theft, Remote Control, System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Yokai	Yokai Backdoor, delivered via a RAR archive containing two Windows shortcut files. Yokai establishes persistence on the compromised system, enabling ongoing communication with a command-and-control (C2) server. In addition to executing commands, the backdoor gathers key system information, such as the hostname and username.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		System Compromise, 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 CVE
WmRAT	WmRAT is a remote access trojan (RAT) developed in C++ that utilizes sockets for communication and offers typical RAT capabilities. It can collect basic host information, upload and download files, capture screenshots, retrieve geolocation data of the target machine, enumerate directories and files, and execute arbitrary commands using cmd or PowerShell.	Spear-phishing emails	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote System Control, Geolocation Tracking, Corporate Espionage	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
TA397			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MiyaRAT	MiyaRAT, written in C++, shares similar functionality with WmRAT. Upon execution, the malware decrypts its hardcoded command-and-control (C2) server and then collects basic system information, which is sent during its initial communication with the C2.	Spear-phishing emails	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote Control Access, Data Exfiltration	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
TA397			

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="3">VBShower</td><td rowspan="7">VBShower is a backdoor used by the Cloud Atlas APT group to facilitate cyberattacks, primarily through phishing emails. It operates by downloading and executing malicious modules, erasing traces of its presence, and communicating with command-and-control servers for further instructions.</td><td>Phishing and Exploit vulnerabilities</td><td>CVE-2018-0802</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Data Theft, System compromise and Espionage</td><td>Microsoft Office and Word</td></tr>
<tr><td><b>TYPE</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Backdoor</td><td rowspan="3">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td></tr>
<tr><td>Cloud Atlas</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="3">VBCloud</td><td rowspan="7">VBCloud is a sophisticated backdoor malware utilized by the Cloud Atlas cybercriminal group, primarily targeting cloud environments. It is delivered through phishing attacks that exploit vulnerabilities in Microsoft Office documents, allowing it to infiltrate systems and exfiltrate sensitive data to cloud storage.</td><td>Phishing and Exploit vulnerabilities</td><td>CVE-2018-0802</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Data Theft</td><td>Microsoft Office and Word</td></tr>
<tr><td><b>TYPE</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Backdoor</td><td rowspan="3">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td></tr>
<tr><td>Cloud Atlas</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerShower	PowerShower is a PowerShell-based malware used by the Cloud Atlas APT group for reconnaissance and as a secondary payload in cyberattacks. It is designed to collect system information, exfiltrate documents, and facilitate the execution of additional malicious modules.	Phishing and Exploit vulnerabilities	CVE-2018-0802
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft and Data Exfiltration	Microsoft Office and Word
ASSOCIATED ACTOR			PATCH LINK
Cloud Atlas			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0802

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BellaCPP	BellaCPP, a C++ variant of the BellaCiao malware family, attributed to the APT actor Charming Kitten. BellaCiao, which first appeared in April 2023, is notable for its stealthy persistence and ability to establish covert tunnels.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Windows
Trojan			
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BellaCiao	BellaCiao is a sophisticated dropper trojan attributed to the Iranian APT group Charming Kitten, designed to deliver additional malicious payloads onto targeted systems. It primarily spreads through phishing emails and exploits vulnerabilities in software such as Microsoft Exchange, aiming to disable security measures like Microsoft Defender.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Windows
Dropper Trojan			
ASSOCIATED ACTOR			PATCH LINK
Charming Kitten			-

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
OtterCookie	OtterCookie is a sophisticated malware used in the Contagious Interview attack campaign, primarily targeting financial data like cryptocurrency wallet keys. It employs advanced techniques such as Socket.IO for real-time communication with its command-and-control servers.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
North Korean Threat Actors			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX	PlugX is a sophisticated remote access Trojan (RAT) that has been used in targeted cyberattacks since 2008, primarily linked to advanced persistent threat (APT) groups operating out of China. Known for its modular design, PlugX allows attackers to gain full control over infected systems, enabling activities such as data theft, monitoring user activity, and executing arbitrary code.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	-
Loader			
ASSOCIATED ACTOR			PATCH LINK
China-linked APT			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rakshasa	Rakshasa is a Hack tool written in Go, specifically designed for multi-level proxying and internal network penetration. The tool is leveraged for advanced cyber-espionage operations, enabling attackers to bypass network defenses and establish covert communication channels within compromised environments.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Multi-level proxying and Data exfiltration	-
Hack tool			
ASSOCIATED ACTOR			PATCH LINK
China-linked APT			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FICORA	The FICORA botnet employs a shell script called "multi" to initiate its attacks. This script uses multiple download methods, to retrieve the FICORA malware, executing and then removing itself to evade detection. Beyond delivery, the script incorporates brute-force capabilities with hard-coded credentials to compromise additional Linux systems, expanding the botnet's reach. Once deployed, FICORA is primed for disruption, conducting distributed denial-of-service (DDoS) attacks through techniques like UDP flooding, TCP flooding, and DNS amplification.	Exploiting Vulnerabilities	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise, DDoS	Multiple D-Link Routers
Botnet			
ASSOCIATED ACTOR			PATCH LINK
-			Patch Link for CVE-2015-2051: https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

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
CAPSAICIN	The CAPSAICIN is a botnet that begins its operations with a downloader script named "bins.sh", designed to retrieve its malicious payload and establish a connection to its command-and-control (C2) server. Upon compromising a system, CAPSAICIN transmits system information back to the C2 server and waits for further instructions. These commands enable it to perform various functions, including launching distributed denial-of-service (DDoS) attacks, making it a versatile and potentially disruptive threat.	Exploiting Vulnerabilities	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2024-33112
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		System Compromise, DDoS	Multiple D-Link Routers
ASSOCIATED ACTOR			PATCH LINK
-			Patch Link for CVE-2015-2051: https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA569	-	Retailers, Service Businesses, Private Users	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	NetSupport RAT, BurnsRAT	Windows
TTPs			
TA0011: Command and Control; TA0003: Persistence; TA0004: TTPs: Privilege Escalation; TA0001: Initial Access; T1059: Command and Scripting Interpreter; T1574.002: DLL Side-Loading; TA0042: Resource Development; T1566.001: Spearphishing Attachment; TA0002: Execution; TA0005: Defense Evasion; TA0009: Collection; T1566: Phishing; T1574: Hijack Execution Flow; T1041: Exfiltration Over C2 Channel; T1218.005: Mshta; T1584: Compromise Infrastructure T1059.007: JavaScript; T1140: Deobfuscate/Decode Files or Information; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1059.005: Visual Basic; T1036: Masquerading; T1204: User Execution; T1123: Audio Capture; T1218: System Binary Proxy Execution; T1059.003: Windows Command Shell; T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Kimsuky (aka Sparkling Pisces, Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394)	North Korea	-	Japan, South Korea, US
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1568: Dynamic Resolution; T1588: Obtain Capabilities; T1588.002: Tool; T1589: Gather Victim Identity Information; T1589.001: Credentials; T1071: Application Layer Protocol; T1204: User Execution; T1036: Masquerading

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Venom Spider (aka GOLDEN CHICKENS)	Russia	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RevC2, Venom Loader	-

TTPs
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1113: Screen Capture; T1090: Proxy; T1059: Command and Scripting Interpreter; T1571: Non-Standard Port; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Pensive Ursa, Blue Python)	Russia	Foreign Affairs, Embassies, Government, Defense, Military, Aerospace, Defense, Education, Embassies, Energy, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail	Worldwide
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	TinyTurla, TwoDash, Wainscot, CrimsonRAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0040: Impact; TA0042: Resource Development; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1203: Exploitation for Client Execution; T1071: Application Layer Protocol; T1071.004: DNS; T1055: Process Injection; T1036: Masquerading; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1012: Query Registry; T1082: System Information Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1078: Valid Accounts; T1570: Lateral Tool Transfer; T1005: Data from Local System; T1105: Ingress Tool Transfer; T1583: Acquire Infrastructure; T1560: Archive Collected Data; T1584: Compromise Infrastructure; T1584.004: Server; T1213: Data from Information Repositories; T1587: Develop Capabilities; T1587.001: Malware; T1083: File and Directory Discovery; T1588: Obtain Capabilities; T1588.002: Tool; T1057: Process Discovery; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA397 (aka Bitter APT, T-APT-17, APT-C-08, Orange Yali)	-	Defense	Turkey
	MOTIVE		
	Information theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	WmRAT and MiyaRAT	Windows
TTPs			
TA0005: Defense Evasion; TA0010: Exfiltration; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0003: Persistence; TA0009: Collection; TA0011: Command and Control; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1041: Exfiltration Over C2 Channel; T1027: Obfuscated Files or Information; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1053.005: Scheduled Task; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1564: Hide Artifacts; T1614: System Location Discovery; T1113: Screen Capture; T1204.002: Malicious File; T1217: Browser Information Discovery; T1056.001: Keylogging; T1056: Input Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Earth Koshchei (aka APT29, 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, Midnight Blizzard, UNC3524, Cranefly, TEMP.Monkeys, Cloaked Ursa, Blue Dev 5, NobleBaron, Solar Phoenix)	Russia	Diplomats, Energy, Telecommunications, IT, Government, Think Tanks, NGOs, Politics, Aerospace, Defense, Banking	Europe, US, Japan, Ukraine, and Australia
	MOTIVE		
	Information theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1566: Phishing; T1204: User Execution; T1552.001: Credentials In Files; T1566.001: Spearphishing Attachment; T1078.003: Local Accounts; T1078: Valid Accounts; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1090: Proxy; T1552: Unsecured Credentials; T1083: File and Directory Discovery; T1018: Remote System Discovery; T1560: Archive Collected Data; T1560.003: Archive via Custom Method; T1005: Data from Local System; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1046: Network Service Discovery; T1570: Lateral Tool Transfer; T1563.002: RDP Hijacking; T1563: Remote Service Session Hijacking; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1036: Masquerading

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">Cloud Atlas (Inception Framework, Oxygen, ATK 116, Blue Odin, The Rocra, Clean Ursa)</td><td>Russia</td><td rowspan="3">-</td><td rowspan="3">Russia, Belarus, Canada, Moldova, Israel, Kyrgyzstan, Vietnam, Turkey</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>-</td><td>VBShower, VBCloud, PowerShower</td><td>-</td></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0006: Credential Access; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control: TA0010: Exfiltration; T1001: Data Obfuscation; T1105: Ingress Tool Transfer; T1564.003: Hide Artifacts: Hidden Window; T1558.003: Steal or Forge Kerberos Tickets: Kerberoasting; T1087: Account Discovery; T1069.002: Permission Groups Discovery: Domain Groups; T1069.001: Permission Groups Discovery: Local Groups; T1615: Group Policy Discovery; T1201: Password Policy Discovery; T1557: : Adversary-in-the-Middle; T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1560: Archive Collected Data; T1566: Phishing; T1204.002: User Execution: Malicious File; T1059.005: Command and Scripting Interpreter: Visual Basic; T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1070.004: Indicator Removal: File Deletion; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery; T1012: Query Registry; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1057: Process Discovery; T1053: Scheduled Task/Job; T1071.001: Application Layer Protocol: Web Protocols</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress)	Iran	-	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	BellaCiao, BellaCPP	Windows
TTPs			
TA0005: Defense Evasion; TA0003: Persistence; TA0010: Exfiltration; TA0002: Execution; TA0011: Command and Control; T1041:Exfiltration Over C2 Channel; T1059.001: PowerShell; T1071.004: DNS; T1071: Application Layer Protocol; T1027: Obfuscated Files or Information; T1543.003: Windows Service; T1543: Create or Modify System Process; T1568.002: Domain Generation Algorithms; T1059: Command and Scripting Interpreter; T1568: Dynamic Resolution			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	T1589.001: Credentials
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	T1590.006: Network Security Appliances
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.002: Tool
		T1588.005: Exploits
	T1587: Develop Capabilities	T1587.001: Malware
	T1584: Compromise Infrastructure	T1584.004: Server
	T1583: Acquire Infrastructure	
	T1586: Compromise Accounts	
TA0001: Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.004: Spearphishing Voice
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
TA0002: Execution	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.005: Visual Basic
		T1059.001: PowerShell
		T1059.007: JavaScript
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1203: Exploitation for Client Execution	
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1559: Inter-Process Communication	
	T1047: Windows Management Instrumentation	
TA0003: Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1136: Create Account	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1556: Modify Authentication Process	
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1505: Server Software Component	

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1055: Process Injection	T1055.012: Process Hollowing
		T1055.002: Portable Executable Injection
	T1068: Exploitation for Privilege Escalation	
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1053: Scheduled Task/Job	T1053.003: Cron
		T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1134: Access Token Manipulation	
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.011: Rundll32
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1036: Masquerading	
	T1140: Deobfuscate/Decode Files or Information	
	T1564: Hide Artifacts	T1564.004: NTFS File Attributes
		T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
	T1562: Impair Defenses	T1562.004: Disable or Modify System Firewall
		T1562.001: Disable or Modify Tools
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1112: Modify Registry	
	T1070: Indicator Removal	T1070.004: File Deletion
	T1055: Process Injection	T1055.002: Portable Executable Injection
	T1556: Modify Authentication Process	
	T1656: Impersonation	
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
		T1553.002: Code Signing
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1620: Reflective Code Loading	
	T1550: Use Alternate Authentication Material	T1055.012: Process Hollowing
		T1550.002: Pass the Hash
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
	T1014: Rootkit	
	T1480: Execution Guardrails	T1480.002: Mutual Exclusion
	T1134: Access Token Manipulation	
TA0006: Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1539: Steal Web Session Cookie	
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
		T1555.001: Keychain
	T1556: Modify Authentication Process	
	T1649: Steal or Forge Authentication Certificates	
	T1558: Steal or Forge Kerberos Tickets	T1558.003: Kerberoasting
	T1056: Input Capture	T1056.001: Keylogging

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1557: Adversary-in-the-Middle	
	T1110: Brute Force	
TA0007: Discovery	T1057: Process Discovery	
	T1135: Network Share Discovery	
	T1083: File and Directory Discovery	
	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1217: Browser Information Discovery	
	T1033: System Owner/User Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1007: System Service Discovery	
	T1482: Domain Trust Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
		T1069.001: Local Groups
	T1012: Query Registry	
	T1614: System Location Discovery	
	T1046: Network Service Discovery	
	T1018: Remote System Discovery	
	T1615: Group Policy Discovery	
	T1201: Password Policy Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1210: Exploitation of Remote Services	
	T1570: Lateral Tool Transfer	
	T1563: Remote Service Session Hijacking	T1563.002: RDP Hijacking
TA0009: Collection	T1123: Audio Capture	
	T1113: Screen Capture	
	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.003: Archive via Custom Method
	T1074: Data Staged	
	T1056: Input Capture	T1056.001: Keylogging
	T1213: Data from Information Repositories	
	T1557: Adversary-in-the-Middle	
	T1115: Clipboard Data	
TA0011: Command and Control	T1132: Data Encoding	T1132.001: Standard Encoding
	T1001: Data Obfuscation	T1001.002: Steganography
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1571: Non-Standard Port	
	T1090: Proxy	
	T1572: Protocol Tunneling	

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1219: Remote Access Software	
	T1105: Ingress Tool Transfer	
	T1071.004: DNS	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1665: Hide Infrastructure	
	T1102: Web Service	
	T1095: Non-Application Layer Protocol	
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0040: Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1491: Defacement	
	T1657: Financial Theft	
	T1498: Network Denial of Service	
	T1565: Data Manipulation	
	T1496: Resource Hijacking	
	T1529: System Shutdown/Reboot	

Top 5 Takeaways

#1

In **December**, there were **eight zero-day** vulnerabilities, with the ‘**One** Celebrity Vulnerability' taking center stage. This featured flaw such as **Zerologon.**

#2

Ransomware activity has seen a sharp rise over the past month, with the **Helldown ransomware** group launching aggressive campaigns against multiple industries. Meanwhile, **Cloud Atlas** deployed a new toolset, exploiting **CVE-2018-0802** via phishing emails. Their attack chain delivers **VBShower** and **PowerShower** backdoors, enabling stealthy system infiltration.

#3

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **FICORA, CAPSAICIN, TinyTurla, TwoDash, Wainscot, SmokeLoader** and **Helldown Ransomware.**

#4

Eight active adversaries were identified across multiple campaigns, targeting the following key industries: **Government, Healthcare** and **Defense.**

#5

Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of 34 attacks. These attacks top impacted **Russia, United States, France** and **Germany.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **20 significant vulnerabilities** and block the indicators related to the **8 active threat actors, 34 active malware,** and **162 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 **20 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 2024)

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
SmokeLoader	SHA256	f7544f07b4468e38e36607b5ac5b3835eac1487e7d16dd52ca882b3d021c19b6
Helldown Ransomware	SHA256	0bfe25de8c46834e9a7c216f99057d855e272eafafdfef98a6012cecbbdcfab, 7cd7c04c62d2a8b4697ceebbe7dd95c910d687e4a6989c1d839117e55c1cafd7, 7731d73e048a351205615821b90ed4f2507abc65acf4d6fe30ecdb211f0b0872, 3e3fad9888856ce195c9c239ad014074f687ba288c78ef26660be93ddd97289e, 2621c5c7e1c12560c6062fdf2eeeb815de4ce3856376022a1a9f8421b4bae8e1, 47635e2cf9d41cab4b73f2a37e6a59a7de29428b75a7b4481205aee4330d4d19, cb48e4298b216ae532cfd3c89c8f2cbd1e32bb402866d2c81682c6671aa4f8ea, 67aea3de7ab23b72e02347cbf6514f28fb726d313e62934b5de6d154215ee733, 2b15e09b98bc2835a4430c4560d3f5b25011141c9efa4331f66e9a707e2a23c0, 6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd, 9ab19741ac36e198fb2fd912620bf320aa7fdeeeb8d4a9e956f3eb3d2092c92c, ccd78d3eba6c53959835c6407d81262d3094e8d06bf2712fefa4b04baadd4bfe
NetSupport RAT	Domains	xoomep1[.]com, xoomep2[.]com, labudanka1[.]com, labudanka2[.]com, gribidi1[.]com, gribidi2[.]com
	SHA256	f4e2f28169e0c88b2551b6f1d63f8ba513feb15beacc43a82f626b93d673f56d
BurnsRAT	URLs	hxxp://193[.]42[.]32[.]138/api/, hxxp://87[.]251[.]67[.]51/api/
RevC2	SHA256	cf45f68219c4a105fffc212895312ca9dc7f4abe37306d2f3b0f098fb6975ec7, 153cd5a005b553927a94cc7759a8909bd1b351407d8d036a1bf5fcf9ee83192e
	URLs	ws[:]//208[.]85[.]17[.]52[:]8082, ws[:]//nopsec[.]org[:]8082/
Venom	SHA256	f93134f9b4ee2beb1998d8ea94e3da824e7d71f19dfb3ce566e8e9da65b1d7a2
	URL	hxxp[:]//170[.]75[.]168[.]151/%computername%/aaa

Attack Name	TYPE	VALUE
Elpaco Ransomware	SHA256	9f6a696876fee8b811db8889bf4933262f4472ad41daea215d2e39bd537cf32f, e160d7d21c917344f010e58dcfc1e19bec6297c294647a06ce60efc7420d3b13
Termite	MD5	6b06aae5ec596cdbc1b9d4c457fd5f81
	SHA1	a515b7d89676b1401eeb9eb776190a1179c386cf
	SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55
	TOR Address	termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion
Realst	SHA256	a0b8789ef3249b5fa8eb3590cd6f183e24273b5886560233025fc9d8de52ce0b, b08740de7bd8d6805ca2c3c8be1db69fbb7aa9bd6aad1c0582881e4196574aa9,fc438c6e231c80c0d5de5b5a194fdba87f88e334414b248047c5e412ed613a6a, 4b93ec3fd49c0111e8a11ac8a0a197f5366cda19732932ce4cb84e024c648a38, 78b2fa0df9fba56ba6a773faa0d280977a1a830fce4f2427935f87de11cb9012, e39cca965dbf7957d04f848572aacfbb736e6aff71e319a788c3f61e52abe795, 2c321b1416fb7226bffd1633a2a053ef3921fef9a1de5c49b71ef9c7b0914b00, 5e6cc2ed3876197561ba60a8d8aa7042d025e997cc1046ea351b5b2bc48f9dd7
Black Basta	SHA1	a6d653d2887f0ce4029a94616464ad74c4f770fe, 0fbed8d60e2d940882e01a2bf11003f6bd59f883, 22f10e42683501fb2ea6962e44eefd64848aefe7
	SHA256	ec669387150865b59bbf98b41a770235ba4fd632aab33433c2d493460ef52479, 95a6c06ac691bec0ac2140b6590c96488feb8bc6c3ca501d1fe8ee7cbf9d0f8b
Zbot	Domains	bigdealcenter[.]world, brownswer[.]com
	SHA1	640640d6651c4ac2f66ed8312084849ad9f0124e, ab1271b4316eb4a5d6ea03b4c24d56cef1e8524a, f09804b59a3aac7c1dd47c7e027182fb54f9a277, f1d299336aac1a1314b36064ffa9ae12ebdb3e4c
	IPv4	45[.]61[.]152[.]154, 185[.]229[.]66[.]224
	SHA256	a9f2c4bc268765fc6d72d8e00363d2440cf1dcbd1ef7ee08978959fc118922c9, 22c5858ff8c7815c34b4386c3b4c83f2b8bb23502d153f5d8fb9f55bd784e764

Attack Name	TYPE	VALUE
DarkGate	IPv4	179[.]60[.]149[.]194
	SHA1	577EFD1534DD2C4133EA2E4B16A21672D257AF72, bccf867716709ce0167cc72f16d4a14f159e459f, 0fdb26c6202acb33eea938da1a492504035ff8c1
	SHA256	4f30d975121d44705a79c4f5c8aeba80d8c97c8ef10c86fee011b99f12b173b4
Mauri	MD5	07894bc946bd742cec694562e730bac8, 25b1c94cf09076eb8ce590ee2f7f108e, 2c93a213f08a9f31af0c7fc4566a0e56, 2e8a3baeaa0fc85ed787a3c7dfd462e7, 3b56e1881d8708c48150978da14da91e
	SHA256	9c87ef43719d6070e186f2be44ffe51b7c6e57728594928915d7b736bfa87b01
Quasar RAT	IPv4:Port	18[.]139[.]156[.]111:4782
TinyTurla	SHA256	e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381, c039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a
	Domains	connectotels[.]net, hostelhotels[.]net
	IPv4	94[.]177[.]198[.]94, 162[.]213[.]195[.]129, 46[.]249[.]58[.]201, 95[.]111[.]229[.]253
TwoDash	SHA256	dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced, 7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912
	IPv4	146[.]70[.]158[.]90, 143[.]198[.]73[.]108, 161[.]35[.]192[.]207, 91[.]234[.]33[.]48
Wainscot	SHA256	e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273, 08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2
	IPv4	130[.]185[.]119[.]198, 176[.]57[.]184[.]97, 173[.]212[.]252[.]2, 209[.]126[.]11[.]251
CrimsonRAT	SHA256	aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c
	IPv4	45[.]14[.]194[.]253, 37[.]60[.]236[.]186, 5[.]189[.]183[.]63

Attack Name	TYPE	VALUE
PUMAKIT	SHA256	30b26707d5fb407ef39ebee37ded7edeea2890fb5ec1ebfa09a3b3edfc80db1f, cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe, 8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03
	Domains	sec[.]opsecurity1[.]art, rhel[.]opsecurity1[.]art
	IPv4	89[.]23[.]113[.]204
Cl0p	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8
	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56
VIPKeyLogger	SHA256	b7d62d77cace855288bf6b463f8ad783316594f90dad78d97a7ea85be58b8bc3, d854f347061d9d7b8a9788ab8633c3f07619e29bd440924507a0147484c217c3
Yokai	SHA256	eaae6d5dbf40239fb5abfa2918286f4039a3a0fcd28276a41281957f6d850456, 3e5cfe768817da9a78b63efad9e60d2d300727a97476edf87be088fb26f06500, 1626ce79f2b96c126cbdb00195dd8509353e8754b1a0ce88d359fa890acd6676, 2852223eb40cf0dae4111be28ce37ce9af23e5332fb78b47c8f5568d497d2611
WmRAT	SHA256	10cec5a84943f9b0c635640fad93fd2a2469cc46aae5e43a4604c903d139970f
MiyaRAT	SHA256	c7ab300df27ad41f8d9e52e2d732f95479f4212a3c3d62dbf0511b37b3e81317
VBShower	Domains	yandesks[.]net, yandisk[.]info, mirconnect[.]info, sber-cloud[.]info, gosportal[.]net, riamir[.]net, web-wathapp[.]com

Attack Name	TYPE	VALUE
VBShower	MD5	f45008bf1889a8655d32a0eb93b8acdd, 4b96dc735b622a94d3c74c0be9858853, 49f8ed13a8a13799a34cc999b195bf16, 3f12bf4a8d82654861b5b5993c012bfa, 3a54acd967dd104522ba7d66f4d86544, 389f6e6fd9dcc84c6e944dc387087a56, 36dd0fbd19899f0b23ade5a1de3c2fec, 2fe7e75bc599b1c68b87cf2a3e7aa51f, 242e86e658fe6ab6e4c81b68162b3001, 21585d5881cc11ed1f615fdb2d7acc11, 1bfb9cba8aa23a401925d356b2f6e7ed, 1af1f9434e4623b7046cf6360e0a520e, 184cf8660af7538cd1cd2559a10b6622, 160a65e830eb97aae6e1305019213558, 016b6a035b44c1ad10d070abcdfe2f66, aa8da99d5623fafed356a14e59acbb90
	SHA1	40bcb307884ad84bc884c1f2b701e680c7ffc151, 3790e6f13b5927f3647bbf606b7d416d2aff8c4f, f6ee2629b0180e1cdc4a9603e7c783035a32d25d, 1deb1ed97dd971cedf81fe13e8dc86c3ef9d9851, cda338eb207311ff14e4f49306a972ba3759f03b, 0db2dcea98298669b2bb3cebeb9e72a66f5c84c2, d7dfda94d354ee218bf06cf232ca47858b0fc7ff, 0cd6b538b3db7c8f48b05ab456ca673bad8068dc, 93dec8070a822b63eb6b23c342e56272642d9128, cf3cf5df1206b14f7d528c5e58d7ff6ace719ed2, 54129ab2bc800982a99bda32002620ec572cc1bf, 6e94c09756b6dcba5ce9ea7e34af19e5e1777de0, c1fcf0db984815dcee8b6323f173ba4097a0fc24, ed492410a934c27b4b1cd81d2cb01190ad24faa6, ce843abe13b0178e0e12dc0719be1cb164b158e4, 7bb42d09cdae0c34592bd4bfe5125836812bd765
	SHA256	75b2e65bebea849d0bd0bab6599f477e6ebd0e74c2ffa960d2360db771e3f583, 1aaf4c0e8653d11adf5d36096130bb3d76384e932a476ae104eefcc0f9823d72, 97497246227ef159a1bedf6ce97c8b81eb9cc86d34f5fbd00d7fe31862b3946d, 678b30bcb599663bc7c26b4dc2ba49ee34048841c83531ca7c7f5ea2e3dee962, aa509fe7b7d6531866c3506e2c006e31926504685e685d93f658e3efb709400e, f482cfe98e589bffd7eee76be5caf4040c69d4c0a8efbd10dcffaefab146ecd4, 9ca81de013b9f9de63c80275fb662510241f97c4d1daab10ab6418a9d0a89cb6, 69b3f4877c7e051dc87d78b8d760e34b6a60000a10ea64351b577d6cb4df8967, 26295b543d1cb6cce1337cc06c1c8a8a0ee30e9aac580710f26bff7d5cc18193, 366f6984d8aa9e78bca46788162f510bbafc10ede3d3ad4c4f53fb42bee00c55,

Attack Name	TYPE	VALUE
VBShower	SHA256	a8bf032dea0fec1c6ef2926edcc03baedcadae149fcbcfb75925a98f290408cf, d9c670f4b5c67958c8f8d705d66c0dbc2ab95e8edc441903e0c68de0aa7b4379, 25230923690d4ce004d0592eac057f8d4ceb942f8334fb9d28d1363271ad3c89, 55f3f668364b3986a2c4ea528d00031c7a0ab67df54cef8affe92a21737f86c9, 81ab65c7b54f501a2e2962346764a6dcb587f32d5ee62b3569a4ba348152fdb9, a5ad86dd7e6b35b45957e9b0986b5fc633a0968d2887b702e1753a469ec57407
VBCloud	Domains	webdav[.]opendrive[.]com, webdav[.]mydrive[.]ch, webdav[.]yandex[.]ru, kim[.]nl[.]tab[.]digital
	MD5	0139f32a523d453bc338a67ca45c224d, 01db58a1d0ec85adc13290a6290ad9d6, 0f37e1298e4c82098dc9318c7e65f9d2, 6fcee9878216019c8dfa887075c5e68e, d445d443ace329fb244edc3e5146313b, f3f28018fb5108b516d802a038f90bde
	SHA1	3f8094e77185af6143eb7dd7ea5c51e9add7f5f1, 10c647af079537c18a1b9f94af596e65a238fcc0, 93bb6307a5dde45d92c8bdc7279d6ff63be8c541, b5b67df4643043aab9533cc1156e44532b4d26c6, 06393cf9bd61e1894dc90e2720f8cbb8778f726f, f5eae20a841a8b44350226522271cc805372dac6
	SHA256	3d55f9a70a1b01432fc0432e5b43ff6c8fa4a8a7a9ed5a787d9cf2a579b12c80, 614e7290bf7974e22e7eac04c1443565ca52e626f9ce4f93f8f33468293c7556, b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d63b08bc4a, 9047d2116b226b35170d1e8a7c81ce0fd25822f6bdf21db39fa3fd28700420a8, 957bbadda00231d45959c3f900d6ac805afbb1cb086192ad68549f3cf0cb8ec2, 5928b83d2626a85231618d6ba169a0133530a71bb71104c948b4b30e45aef0e0
PowerShower	Domains	yandisk[.]info, yandesktop[.]com, web-wathapp[.]com
	MD5	15fd46ac775a30b1963281a037a771b1, 31b01387ca60a1771349653a3c6ad8ca, 389bc3b9417d893f3324221141edea00

Attack Name	TYPE	VALUE
PowerShower	SHA1	ac8ec1e17bd90430113b2c083793682e68e03311, 7c75f00f89fbd1e4977032e945c2468590c60450, 9c60869ae3697662102c8dd54bd45fbf2588d02e
	SHA256	7b0683a60a10657963cbcfcc9d0480e7812a3894ffb3b0d6d92bab0dc2fde0b4, c4f97cd48cc2ca11acc9e49ac18b8763752853beaabf149fe313b295fa01b2d6, a9f53fc9f350446632111b500550567a8273d0f7838d27099c41f523a0a550b9
BellaCPP	MD5	222380fa5a0c1087559abbb6d1a5f889
	SHA1	dccdfc77dd2803b3c5a97af0851efa0aa5bbeeeb
	SHA256	e4e3f09c4257269cef6cfbebc83c8a60376ce5e547080502e3e408a3f9916218
	File name	adhapl.dll
BellaCiao	MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcdb6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7, 5f4284115ab9641f1532bb64b650aad6, 0fea857a35b972899e8f1f60ee58e450, 20014b80a139ed256621b9c0ac4d7076, 7f0ee078c8902f12d6d9e300dabf6aed, 63647520b36144e31fb8ad7dd10e3d21, 8096e00aa7877b863ef5a437f55c8277, 12ab1bc0989b32c55743df9b8c46af5a, 50dc5faa02227c0aefa8b54c8e5b2b0d, e760a5ce807c756451072376f88760d7, b03c67239e1e774077995bac331a8950, ba69cc9f087411995c64ca0d96da7b69, 051552b4da740a3af5bd5643b1dc239a, edfb8d26fa34436f2e92d5be1cb5901b, 3e86f6fc7ed037f3c9560cc59aa7aacc, ae4d6812f5638d95a82b3fa3d4f92861, 67677c815070ca2e3ebd57a6adb58d2e, 17a78f50e32679f228c43823faabedfd, b9956282a0fed076ed083892e498ac69, 1b41e64c60ca9dfadeb063cd822ab089
OtterCookie	SHA256	d19ac8533ab14d97f4150973ffa810e987dea853bb85edffb7c2fcef13ad2106, 7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e, 4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79, 32257fb11cc33e794fdfd0f952158a84b4475d46f531d4bee06746d15caf8236

Attack Name	TYPE	VALUE
OtterCookie	Domains	zkservice[.]cloud, w3capi[.]marketing, payloadrpc[.]com
	IPv4	45[.]159[.]248[.]55
PlugX	SHA256	33cb9f06338a9ea17107abbdc478071bbe097f80a835bbac462c4bb17cd0b798
Rakshasa	SHA256	aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158
CAPSAICIN	URLs	hxxp[://]87[.]11[.]174[.]141/bins[.]sh, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]yak[.]sh, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm5, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm6, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]arm7, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]i586, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]i686, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]m68k, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]mips, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]mipsel, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]ppc, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]sparc, hxxp[://]pirati[.]abuser[.]eu/yakuza[.]x86, hxxp[://]87[.]10[.]220[.]221/bins[.]sh, hxxp[://]87[.]10[.]220[.]221/yakuza[.]sh, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm4, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm5, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm6, hxxp[://]87[.]10[.]220[.]221/yakuza[.]arm7, hxxp[://]87[.]10[.]220[.]221/yakuza[.]i586, hxxp[://]87[.]10[.]220[.]221/yakuza[.]i686, hxxp[://]87[.]10[.]220[.]221/yakuza[.]m68k, hxxp[://]87[.]10[.]220[.]221/yakuza[.]mips, hxxp[://]87[.]10[.]220[.]221/yakuza[.]mipsel, hxxp[://]87[.]10[.]220[.]221/yakuza[.]ppc, hxxp[://]87[.]10[.]220[.]221/yakuza[.]sparc, hxxp[://]87[.]10[.]220[.]221/yakuza[.]x86
	SHA256	8349ba17f028b6a17aaa09cd17f1107409611a0734e06e6047ccc33e8ff669b0, b3ad8409d82500e790e6599337abe4d6edf5bd4c6737f8357d19edd82c88b064, ec87dc841af77ec2987f3e8ae316143218e9557e281ca13fb954536aa9f9caf1, 784c9711eadceb7fedf022b7d7f00cff7a75d05c18ff726e257602e3a3ccccc1, bde6ef047e0880ac7ef02e56eb87d5bc39116e98ef97a5b1960e9a55cea5082b, c7be8d1b8948e1cb095d46376ced64367718ed2d9270c2fc99c7052a9d1ffed7, 4600703535e35b464f0198a1fa95e3668a0c956ab68ce7b719c28031d69b86ff,

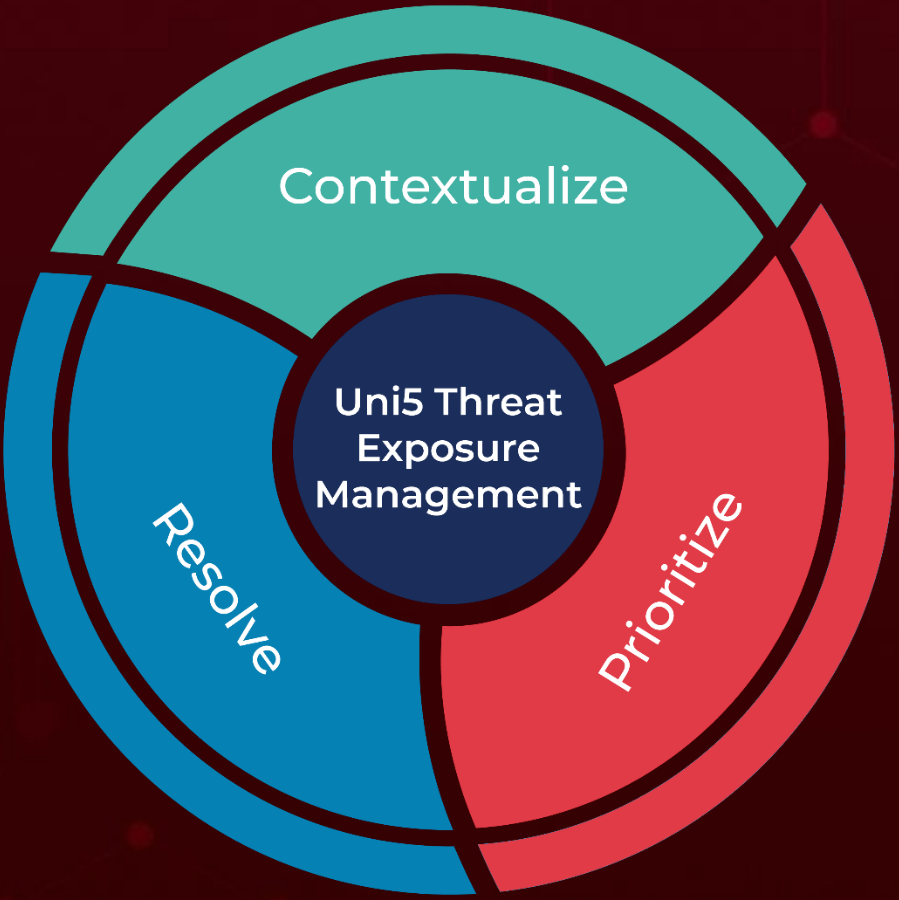
Attack Name	TYPE	VALUE
CAPSAICIN	SHA256	6e3ef9404817e168c974000205b27723bc93abd7fbf0581c16bb5d2e1c5c6e4a, 32e66b87f47245a892b102b7141d3845540b270c278e221f502807758a4e5dee, 540c00e6c0b53332128b605b0d5e0926db0560a541bb13448d094764844763df, b74dbd02b7ebb51700f3c5900283e46570fe497f9b415d25a029623118073519, 148f6b990fc1f1903287cd5c20276664b332dd3ba8d58f2bf8c26334c93c3af5, 464e2f1faab2a40db44f118f7c3d1f9b300297fe6ced83fabe87563fc82efe95, b699cd64b9895cdcc325d7dd96c9eca623d3ec0247d20f39323547132c8fa63b, 1007f5613a91a5d4170f28e24bfa704c8a63d95a2b4d033ff2bff7e2fe3dcffe, 7a815d4ca3771de8a71cde2bdacf951bf48ea5854eb0a2af5db7d13ad51c44ab, d6a2a22000d68d79caeae482d8cf092c2d84d55dccee05e179a961c72f77b1ba, 7ab36a93f009058e60c8a45b900c1c7ae38c96005a43a39e45be9dc7af9d6da8, 803abfe19cdc6c0c41acfeb210a2361cab96d5926b2c43e5eb3b589a6ed189ad, 7b29053306f194ca75021952f97f894d8eae6d2e1d02939df37b62d3845bfdb7, 59704cf55b9fa439d6f7a36821a50178e9d73ddc5407ff340460c054d7defc54, aaa49b7b4f1e71623c42bc77bb7aa40534bcb7312da511b041799bf0e1a63ee7, 1ca1d5a53c4379c3015c74af2b18c1d9285ac1a48d515f9b7827e4f900a61bde
FICORA	SHA256	9b161a32d89f9b19d40cd4c21d436c1daf208b5d159ffe1df7ad5fd1a57610e5, faeea9d5091384195e87caae9dd88010c9a2b3b2c88ae9cac8d79fd94f250e9f, 10d7aedc963ea77302b967aad100d7dd90d95abcdb099c5a0a2df309c52c32b8, 7f6912de8bef9ced5b9018401452278570b4264bb1e935292575f2c3a0616ec4, a06fd0b8936f5b2370db5f7ec933d53bd8a1bf5042cdc5c052390d1ecc7c0e07, 764a03bf28f9eec50a1bd994308e977a64201fbe5d41337bdcc942c74861bcd3, df176fb8cfbc7512c77673f862e73833641ebb0d43213492c168f99302dcd5e3, ac2df391ede03df27bcf238077d2dddcde24cd86f16202c5c51ecd31b7596a68, ca3f6dce945ccad5a50ea01262b2d42171f893632fc5c5b8ce4499990e978e5b,

Attack Name	TYPE	VALUE
FICORA	SHA256	afee245b6f999f6b9d0dd997436df5f2abfb3c8d2a8811ff57e3c21637207d62, ec508df7cb142a639b0c33f710d5e49c29a5a578521b6306bee28012aadde4a8
	URLs	hxxp[://]103[.]149[.]87[.]69/multi, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arc, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm5, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm6, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]arm7, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]m68k, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]mips, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]mipsel, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]powerpc, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]sh4, hxxp[://]103[.]149[.]87[.]69/la[.]bot[.]sparc

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 3, 2025 • 4:00 AM

More at www.hivepro.com