Date of Publication
May 2, 2024

Hive Pro

HiveForce Labs

MONTHLY THREAT DIGEST

Vulnerabilities, Attacks, and Actors

APRIL 2024

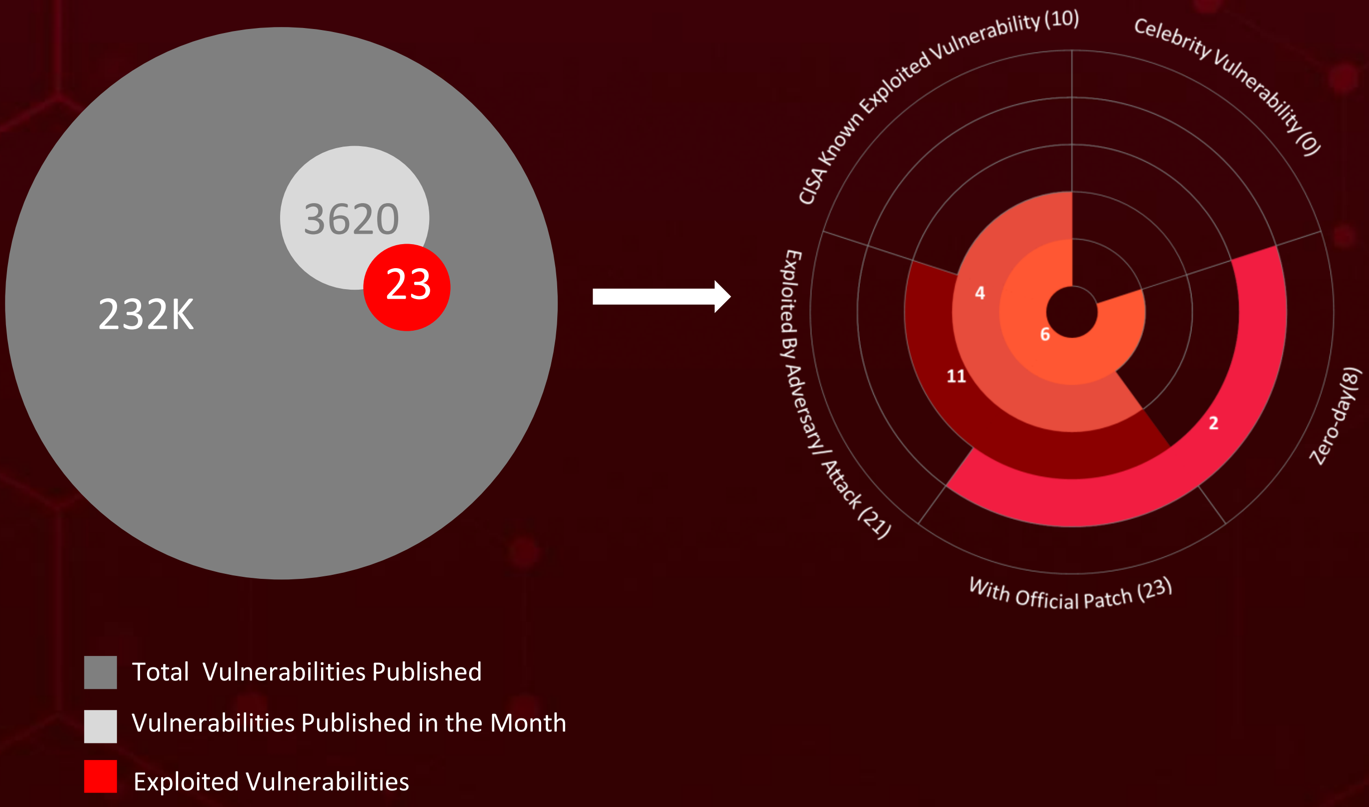
Table Of Contents

Summary

In April, the cybersecurity landscape witnessed a surge in attention due to the discovery of **eight zero-day** vulnerabilities. Notably, one of these vulnerabilities (**CVE-2024-3400**) in Palo Alto Networks PAN-OS was exploited by the **UTA0178** group, allowing unauthenticated attackers to execute code with root privileges, leading to full device control.

During the same period, ransomware attacks experienced a noticeable uptick, with strains such as **LockBit 3.0**, **KageNoHitobito, DoNex,** and **Akira** 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, **fifteen** adversaries were active across diverse campaigns. **STORM-1849**, a group of state-affiliated operatives, has masterminded **ArcaneDoor**, an intricately crafted cyber espionage endeavor. Since November 2023, this operation has strategically aimed at governmental and critical infrastructure networks on a global scale, leveraging two zero-day vulnerabilities present in Cisco ASA and FTD firewalls. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

SteganoAmor campaign

TA558 hacking group employs steganography to conceal malicious code within images

0-Day in Palo Alto

CVE-2024-3400 is a critical flaw in Palo Alto Networks PAN-OS, allowing unauthenticated attackers to execute code with root privileges, leading to full device control

Sync-Scheduler

Infostealer, developed in C++, has emerged as a significant threat, hidden within Office document files

XZ-Utils backdoored

A backdoor (CVE-2024-3094) in XZ Utils library poses supply chain threat to multiple Linux distributions, allowing attackers to manipulate data

Akira Ransomware

As of January 1, 2024, the ransomware group has affected more than 250 organizations and declared around $42 million USD in ransomware earnings

CVE-2022-38028

A critical vulnerability in Windows Print Spooler exploited by APT28 to deliver GooseEgg malware

Connect:fun cyber campaign

targeting organizations with vulnerable Fortinet FortiClient EMS systems, exploiting CVE-2023-48788 for remote access.

Muddy Water

The Iranian threat actor, has added a new C2 infrastructure named **DarkBeatC2** to its arsenal

In April 2024, a geopolitical cybersecurity landscape unfolds, revealing the **United States, Pakistan, Australia, New Zealand,** and **Israel** as the top-targeted countries

Highlighted in **April 2024** is a cyber battleground encompassing the **Government**, **Finance**, **Technology**, **Education**, and **Transportation** sectors, designating them as the top industries

Threat Landscape

23 Vulnerabilities

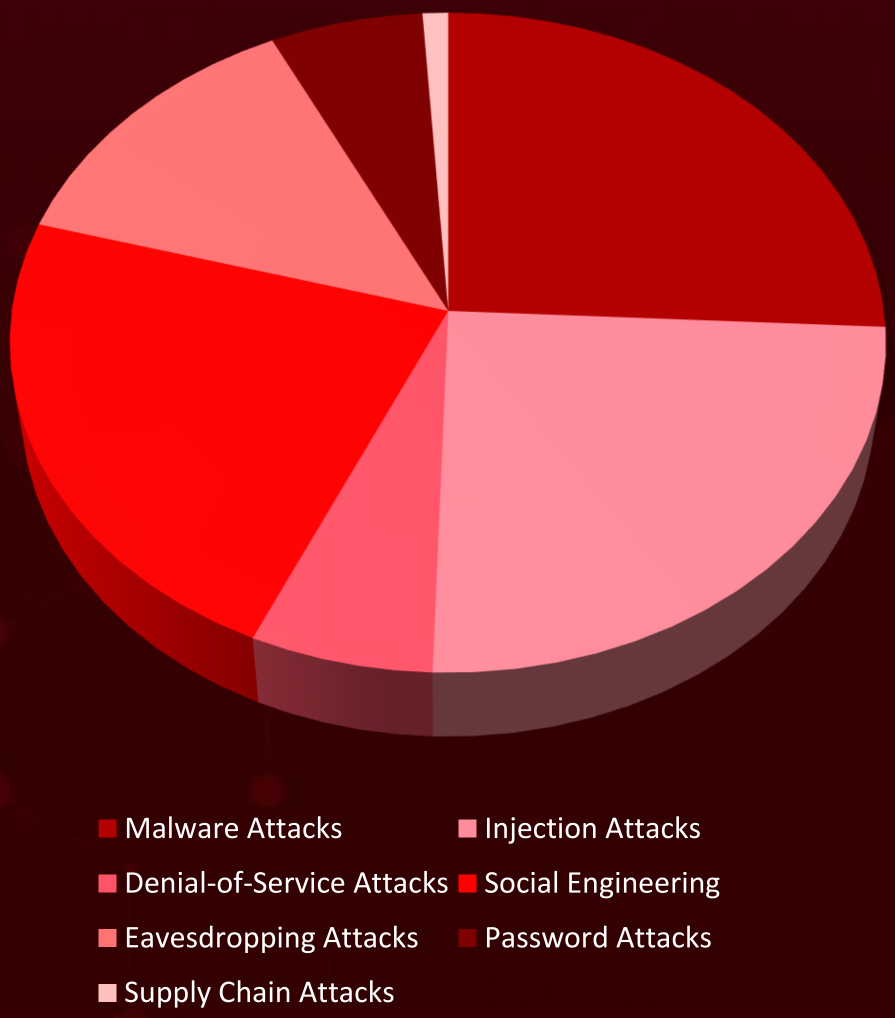
221 MITRE ATT&CK TTPs

24 Industries

15 Adversaries

232 Countries

34 Attacks



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-3094	XZ Utils Embedded Malicious code	XZ Utils	✗	✗	✓
CVE-2024-2879	WordPress LayerSlider SQL Injection Vulnerability	WordPress LayerSlider	✗	✗	✓
CVE-2024-20720	Adobe OS Command Injection Vulnerability	Adobe Commerce	✗	✗	✓
CVE-2024-3273	D-Link NAS Remote Code Execution Vulnerability	D-Link NAS	✗	✓	✓
CVE-2024-26234	Microsoft Windows Proxy Driver Spoofing Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2024-29988	Microsoft Windows SmartScreen Prompt Security Feature Bypass Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2023-45590	Fortinet FortiClient Remote Code Execution Vulnerability	Fortinet FortiClient	✗	✗	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓
CVE-2023-48788	Fortinet FortiClientEMS SQL Injection Vulnerability	Fortinet FortiClientEMS	✗	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-28254	OpenMetadata OS Command Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28255	OpenMetadata Improper Authentication Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28847	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28253	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-28848	OpenMetadata Code Injection Vulnerability	OpenMetadata	✗	✗	✓
CVE-2024-20295	Cisco Integrated Management Controller CLI Command Injection Vulnerability	Cisco Integrated Management Controller	✗	✗	✓
CVE-2022-38028	Microsoft Windows Print Spooler Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-20353	Cisco ASA and FTD Denial of Service Vulnerability	Cisco ASA and FTD	✓	✓	✓
CVE-2024-20359	Cisco ASA and FTD Privilege Escalation Vulnerability	Cisco ASA and FTD	✓	✓	✓
CVE-2024-4040	CrushFTP VFS Sandbox Escape Vulnerability	CrushFTP VFS	✓	✓	✓
CVE-2024-27956	WordPress Automatic Plugin SQL Injection Vulnerability	WordPress Automatic Plugin	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2020-3259	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco ASA and FTD	✗	✓	✓
CVE-2023-20269	Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	Cisco Adaptive Security Appliance and Firepower Threat Defense	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Atomic Stealer	Stealer	-	macOS	-	Malicious ads, fake software updates
Realst stealer	Stealer	-	-	-	Disguised as fake blockchain games
UNAPIMON	Loader	-	Windows and VMware	-	Phishing
SYNC-SCHEDULER	Stealer	-	-	-	-
RotBot	RAT	-	Windows	-	Phishing
XClient stealer	Stealer	-	Windows	-	Phishing
Latrodectus	Downloader	-	-	-	Phishing email
Nitrogen	Dropper	-	-	-	Malvertising
Raspberry Robin	Worm	-	Windows	-	Social engineering and malvertising
LazyStealer	Stealer	-	-	-	Phishing
Rhadamanthys	Stealer	-	Windows	-	Phishing
PrintSpoofer	Tool	-	Redis	-	Exploiting Redis services
DarkBeatC2	Backdoor	-	-	-	Social engineering
UPSTYLE	Backdoor	CVE-2024-3400	Linux	✓	Exploiting vulnerabilities
LockBit 3.0	Ransomware	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
AgentTesla	RAT	CVE-2017-11882	Microsoft Office	✓	Phishing
FormBook	Stealer	CVE-2017-11882	Microsoft Office	✓	Phishing
Remcos	RAT	CVE-2017-11882	Microsoft Office	✓	Phishing emails, exploit kits, and watering hole attacks
LokiBot	Stealer	CVE-2017-11882	Microsoft Office	✓	Phishing
Guloader	Downloader	CVE-2017-11882	Microsoft Office	✓	Phishing
SnakeKeylogger	Keylogger	CVE-2017-11882	Microsoft Office	✓	Phishing
Xworm	RAT	CVE-2017-11882	Microsoft Office	✓	Phishing
JsOutProx	RAT	-	Windows	-	Phishing
FatalRAT	RAT	CVE-2017-11882	Microsoft Office	✓	Phishing
Carbanak	Backdoor	-	-	-	Phishing
Waterbear	Backdoor	-	-	-	-
CR4T	Backdoor	-	-	-	-
Cryptbot	Stealer	-	-	-	Phishing
LummaC2	Stealer	-	-	-	Phishing
Rhadamanthys	Stealer	-	-	-	Phishing
GooseEgg	Loader	CVE-2022-38028	Windows	✓	Exploiting vulnerabilitie s
KageNoHitobit o	Ransomwar e	-	-	-	-

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
DoNex	Ransomware	-	-	-	-
Akira	Ransomware	CVE-2020-3259 CVE-2023-20269	-	✓	Exploiting vulnerabilitie s

Adversaries Summary

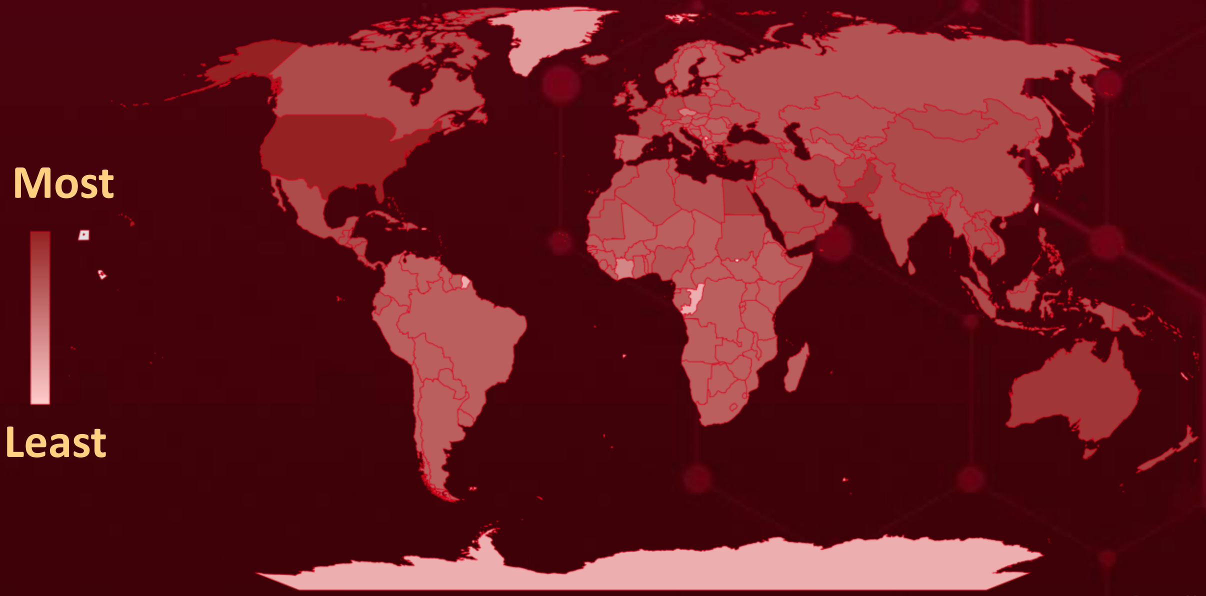
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Earth Freybug	Espionage and Financial gain	China	-	UNAPIMON	Windows and VMware
CoralRaider	Financial gain	Vietnam	-	RotBot, XClient stealer, Cryptbot, LummaC2 and Rhadamanthys	Windows
TA577	Financial Gain	-	-	Latrodectus	-
TA547	Financial Gain, Financial Crime	-	-	Rhadamanthys	Windows
TA578	Financial Gain	-	-	Latrodectus	-
Lazy Koala	Information Theft and Espionage	-	-	LazyStealer	-
Muddy Water	Information theft and espionage	Iran	-	DarkBeatC2	-
SOLAR SPIDER	Financial Gain	-	-	JsOutProx RAT	Windows

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
TA558	Financial Gain	-	CVE-2017-11882	AgentTesla, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm	-
FIN7	Information theft and espionage, Financial gain	Russia	-	Carbanak	-
Earth Hundun	Information theft and espionage	China	-	Waterbear backdoor	-
ToddyCat	Information theft and espionage	China	-	-	-
APT28	Information theft and espionage	Russia	CVE-2022-38028	GooseEgg	Microsoft Windows Print Spooler
STORM-1849	Espionage	-	CVE-2024-20353, CVE-2024-20359	-	Cisco ASA Software and FTD Software
Muddling Meerkat	-	China	-	-	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
XZ Utils	Software	XZ Utils or liblzma Versions and Fedora
WordPress	Application	WordPress LayerSlider
Adobe	Ecommerce platform	Adobe Commerce
D-Link	Network-connected storage drives	D-Link NAS
Microsoft	Operating system	Microsoft Windows
	Application	Microsoft Office
FORTINET	Endpoint security software	Fortinet FortiClient
	Unified Endpoint Management (UEM) software	Fortinet FortiClientEMS
paloalto NETWORKS	Operating system	Palo Alto Networks PAN-OS
Open Metadata	Application	OpenMetadata
CISCO	Baseboard Management Controller	Cisco Integrated Management Controller CLI
	Firewalls	Cisco ASA and FTD, Cisco Adaptive Security Appliance and Firepower Threat Defense

Targeted Countries

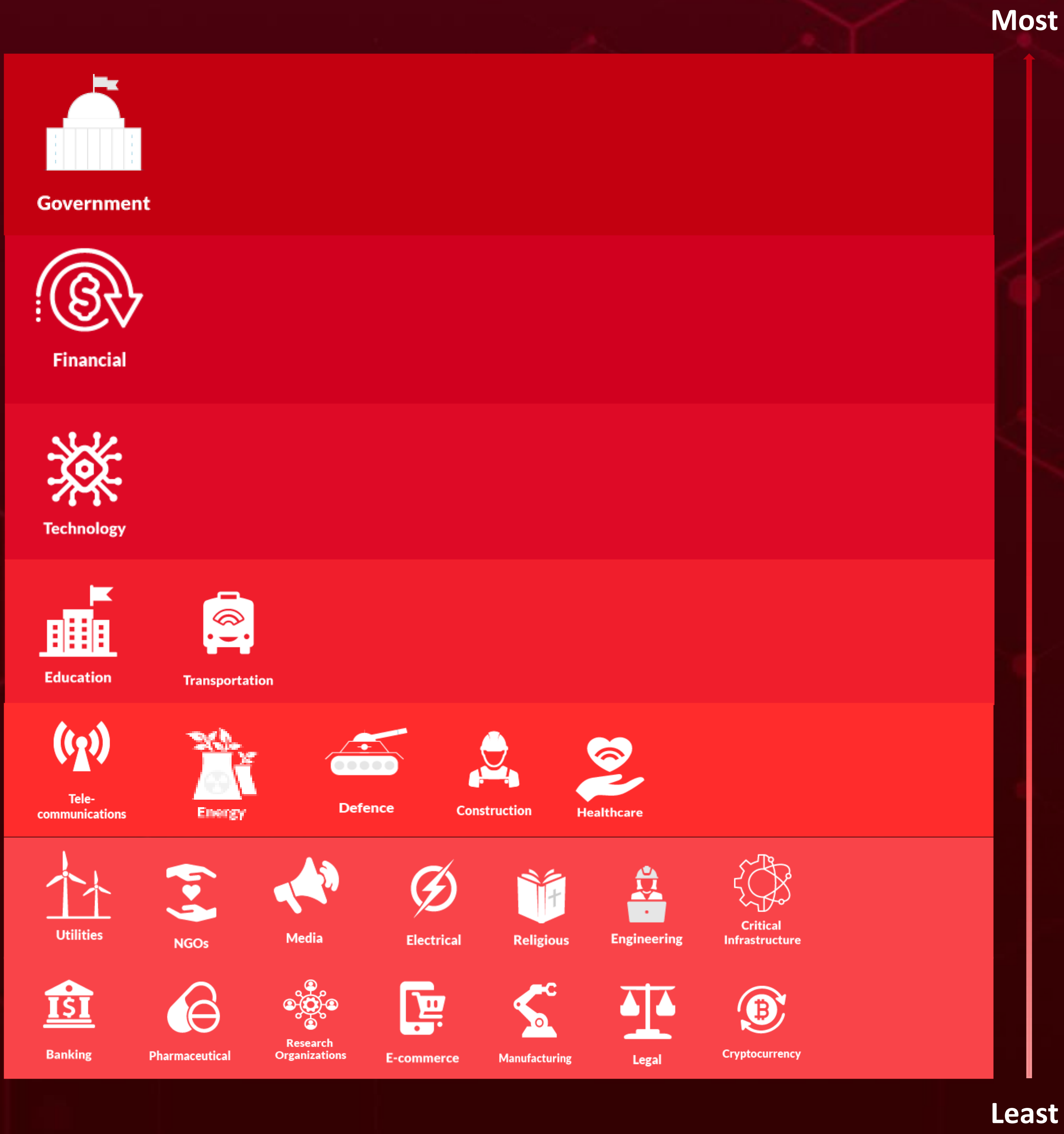


Powered by Bing

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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
🟥	United States	🟥	Dominica	🟥	Costa Rica	🟥	Canada	🟥	Kazakhstan
🟥	Pakistan	🟥	United Arab Emirates	🟥	India	🟥	Laos	🟥	Russia
🟥	Australia	🟥	Dominican Republic	🟥	Cyprus	🟥	Sri Lanka	🟥	Belarus
🟥	New Zealand	🟥	Oman	🟥	Indonesia	🟥	Lebanon	🟥	Tajikistan
🟥	Israel	🟥	Antigua and Barbuda	🟥	Mongolia	🟥	Thailand	🟥	Kyrgyzstan
🟥	Papua New Guinea	🟥	Samoa	🟥	Iran	🟥	Vietnam	🟥	Morocco
🟥	Egypt	🟥	El Salvador	🟥	Nepal	🟥	Trinidad and Tobago	🟥	Libya
🟥	Tuvalu	🟥	China	🟥	Iraq	🟥	Malaysia	🟥	Netherlands
🟥	Fiji	🟥	Armenia	🟥	Nicaragua	🟥	Cuba	🟥	Luxembourg
🟥	Palau	🟥	Micronesia	🟥	Afghanistan	🟥	Maldives	🟥	North Korea
🟥	Japan	🟥	France	🟥	Belize	🟥	United Kingdom	🟥	Djibouti
🟥	Philippines	🟥	Belgium	🟥	Jamaica	🟥	Barbados	🟥	Poland
🟥	Solomon Islands	🟥	Germany	🟥	Panama	🟥	Mexico	🟥	Malta
🟥	Tonga	🟥	Bhutan	🟥	Bahamas	🟥	Jordan	🟥	Georgia
🟥	Turkey	🟥	Grenada	🟥	Cambodia	🟥	Yemen	🟥	Mauritania
🟥	Kiribati	🟥	Qatar	🟥	Bahrain	🟥	Myanmar	🟥	Sudan
🟥	Marshall Islands	🟥	Guatemala	🟥	Saint Lucia	🟥	Somalia	🟥	Azerbaijan
🟥	Vanuatu	🟥	Singapore	🟥	Bangladesh	🟥	Norway	🟥	Tunisia
🟥	Nauru	🟥	Haiti	🟥	Saudi Arabia	🟥	Italy	🟥	Ecuador
🟥	South Korea	🟥	Syria	🟥	Kuwait	🟥	Ukraine	🟥	Uzbekistan
🟥	Brunei	🟥	Honduras	🟥	Canada	🟥	Algeria	🟥	Monaco
				🟥	Laos	🟥	Nigeria	🟥	Ireland
				🟥	Sri Lanka			🟥	Hungary

Targeted Industries



Most

Government

Financial

Technology

Education

Transportation

Tele-communications

Energy

Defence

Construction

Healthcare

Utilities

NGOs

Media

Electrical

Religious

Engineering

Critical Infrastructure

Banking

Pharmaceutical

Research Organizations

E-commerce

Manufacturing

Legal

Cryptocurrency

Least

TOP 25 MITRE ATT&CK TTPS

T1059	Command and Scripting Interpreter
T1588	Obtain Capabilities
T1566	Phishing
T1588.006	Vulnerabilities
T1036	Masquerading
T1082	System Information Discovery
T1027	Obfuscated Files or Information
T1204	User Execution
T1059.001	PowerShell
T1190	Exploit Public-Facing Application
T1555	Credentials from Password Stores
T1041	Exfiltration Over C2 Channel
T1574.002	DLL Side-Loading
T1204.002	Malicious File
T1057	Process Discovery
T1203	Exploitation for Client Execution
T1566.001	Spearphishing Attachment
T1071	Application Layer Protocol
T1071.001	Web Protocols
T1083	File and Directory Discovery
T1204.001	Malicious Link
T1105	Ingress Tool Transfer
T1068	Exploitation for Privilege Escalation
T1055	Process Injection
T1573	Encrypted Channel

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Atomic Stealer	SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d,
	IPv4	194.169.175[.]117
UNAPIMON	SHA256	62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2
Raspberry Robin	SHA256	98ad6aad996e4005389ea7e4782a4a082c1e83a8a20ad07bb3a3eed4047b3603, 9303b89abe2c0393e78991f74a90d9202a2f14dc267367277da7af705733eb32, 229c6b0dc9298a6868a24aad6cf3c8b08feb97f809f2d67fb6dc2e71ebee876b, 78ae67f650400ef6db9a85aa3d10ab7684f789e587ef33420a352a9b53916364, dd576545834e9c439491d62a8a6d9578a58693cef9f5cd2783fc80f49275dac8, fbdbe211e66792f3cefc50da6b3b88d82d497be1cd25f4654d4d122c0ed10a42, a3de553cae9671bd94aae75f76f8de2dd9abb41780d25f012debf7761a579ea9, 479d1cb582c03c679cb23ccb6b5dd1611822f59f311a6cdc82bd6eef5f53da14, d5dd3f1dd787746403843100c8dec9c70c20d8098071aafc5bfeef20b95fd93f, b4566c3cbfa193ad6dc7173d8b5d93734f06d940085110f6a2c7812524c2c236, 752ccebfcf2d63d44bf3073b2f30e83758aa0ae26d3bdca59de6e53e6d33b19e, a81176e32b8d73fbbd11d1a1da32789c8b18cf6aa79e1b4cae8ed031b7e9dbbf, 99d1e9839922063d3655583d541ac6908000222cd847c95c919a27c9d2b01301

Attack Name	TYPE	VALUE
GooseEgg	SHA256	c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5, 6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f
PrintSpoofer	MD5	dbdcbacbc74b139d914747690ebe0e1c, b26b57b28e61f9320cc42d97428f3806
	URL	hxxp://35.185.187[.]24/PrintSpoofer.exe
DarkBeatC2	IPv4	45.66.249[.]226, 137.74.131[.]19, 164.132.237[.]68, 95.164.61[.]64, 95.164.46[.]54, 91.225.218[.]210, 95.164.38[.]68, 45.140.147[.]81, 80.71.157[.]130, 103.35.190[.]203, 95.164.46[.]253
UPSTYLE	SHA256	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
	MD5	0c1554888ce9ed0da1583dbdf7b31651
	SHA1	988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9
JsOutProx	MD5	118b6673bd06c8eb082296a7b35f8fa5, 1bd7ce64f1a7cf7dc94b912ceb9533d0, 3a2104953478d1e60927aa6def17e8e7, 3d46a462f262818cada6899634354138, 66514548cdffab50d1ea75772a08df3d, 6764dbc4df70e559b2a59e913d940d4b, 72461c94bd27e5b001265bbccc931534, 81b9e7deb17e3371d417ad94776b2a26, 89a088cd92b7ed59fd3bcc7786075130, 9c9df8fbcef8acd1a5265be5fd8fdce9, bea8cf1f983120b68204f2fa9448526e, d22f76e60a786f0c92fa20af1a1619b2, efad51e48d585b639d974fcf39f7ee07, f1858438a353d38e3e19109bf0a5e1be

Attack Name	TYPE	VALUE
FatalRAT	SHA256	8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d
Carbanak	SHA256	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
	MD5	87aa5f3f514af2b9ef28db9f092f3249
Rhadamanthys	Domain	indscpm[.]xyz
	IPv4:Port	94[.]131[.]104[.]223:443
	SHA256	B9AD234ABEB1490F2C2D28DD2387F0575BA5128EBB799741B1F3179622204175, 7FAEB3F847830A2C52322565D8E73E07000003CCB54310790E10756CD3B2FF6B, C7CA2F9065557A6D8FB0C02C75804D386B77FFCA4466678B201C09E916AFA096, A432BF6943599E53A12D5615F91FE3D636A6820073B60A7068FA9508849806B4, 30B5B1D6877DF251F4007725DF4E043F704D80A55B4EBD7C952B4F24B7806712, 8404CB4A740D169256E49E3A22B2AF1A61B2606E71CDCA4F39DEECCD5D461C91, 138C86D9C22182DC809F2747D012D792ED391A84081E513C7C93D8786801D5F7, B579DF3A8607CB6B251EE319BDC8C1005CA3A6ED1E360EEDF2433B3F6151D856, 1D8E82D9ABDA58C9F4A0DEF2940E9F75921E2DCE89A07B337A075CA363176CD4, 4130CE135FBFAB00618F261A0397E88479D2F61E1ED0D09EBCDE525439774F3E, CC830FF08B6C66FB562A8E90C9512CADD6DBE715EB31D09E7D6AFCC0E9FBEE68, 70DEBCE3A545CACCA8B0BDB6008945852084B36E9160424FB63479C2991DCADE, A4B6A1619CF4FF65770BE120CC415DE1E8897C2378610171F3C48FF0FA38E9FE, 00DD5C97E86646DF73973BA24085EBB32DB19DE258F37ED50B5C333087BB6B5C, DF65E93CDDF79B31B474F39477AA3038CB666965311676096D9E02A5B5CF7523, 233A2666A23AB1BAE19296EE7F66CE3CDF6284DB1CA4CAAEB121530126419B42, D5B6CFE15A5BF959152889D8FF4FC220F0C055327C57A83C4877316AF50D3A4D,

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3094	⊗	XZ Utils or liblzma Versions 5.6.0,5.6.1 Fedora : Versions 40, 41(Rawhide)	-
	ZERO-DAY		
	⊗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:tukaani:xz-utils:*:*:*:*:*:*:*	-
XZ Utils Embedded Malicious code	⊗		
	CWE ID	**ASSOCIATED TTPs**	**WORKAROUND**
	CWE-506	T1195.001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Downgrade XZ Utils to a stable version before 5.6.0, such as XZ Utils 5.4.6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-2879	⊗	LayerSlider Version 7.9.11 – 7.10.0	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.9.11:*:*:*:*:*:*:* cpe:2.3:a:layerslider_plugin:layerslider_plugin:7.10.0:*:*:*:*:*:*:*	-
WordPress LayerSlider SQL Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190 : Exploit Public-Facing Application, 1505 : Server Software Component	https://www.wordfence.com/threatintel/vulnerabilities/wordpressplugins/layerslider/layerslider-7911-7100-unauthenticated-sql-injection

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20720	⊗	Adobe Commerce: 2.3.7 - 2.4.6-p3, Magento Open Source: 2.4.4 - 2.4.6-p3	Unknown
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*:*:*	Stripe payment skimmer
Adobe OS Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/magento/apsb24-03.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3273	✗	DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013 DNS-325 Version 1.01 DNS-327L Version 1.09, Version 1.00.0409.2013 DNS-340L Version 1.08	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:d-link:dns-320l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-325:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-327l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-340l:*:*:*:*:*:*:*:*	skid.x86 (Mirai variant)
D-Link NAS 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=SAP10383

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-26234	✗	Windows: 10 - 11 23H2 Windows Server: 2008 – 2022 23H2	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Proxy Driver Spoofing Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-284	T1090: Proxy	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29988	✗	Windows: 10 - 11 23H2 Windows Server: 2019 – 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows SmartScreen Prompt Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-45590	✗	FortiClientLinux version 7.2.0, 7.0.6 through 7.0.10 and 7.0.3 through 7.0.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:*:*:*	-
Fortinet FortiClient Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://www.fortiguard.com/psirt/FG-IR-23-087

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400	✗	Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 <11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	UTA0218
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	UPSTYLE
Palo Alto Networks PAN-OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48788	✗	FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*:*:*	Connect:fun Campaign
Fortinet FortiClientEMS SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗	Microsoft Office: 2007 SP3 2010 SP2 2013 SP1 2016	TA558
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*	AgentTesla, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203 : Exploitation for Client Execution, T1059 : Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28254	✗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-j86m-rrpr-g8gw

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28255	⊗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*	-
OpenMetadata Improper Authentication Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190 : Exploit Public-Facing Application, T1068 : Exploitation for Privilege Escalation	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-6wx7-qw5p-wh84

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28847	⊗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-8p5r-6mvv-2435

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28253	⊗	OpenMetadata versions prior to 1.3.1	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-7vf4-x5m2-r6gr

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28848	⊗	OpenMetadata versions prior to 1.2.4	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:open-metadata:openmetadata:*:*:*:*:*:*:*:*	-
OpenMetadata Code Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-5xv3-fm7g-865r

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20295	⊗	Cisco Integrated Management Controller: 3.2.6 - 4.12 Enterprise NFV Infrastructure Software: 3.12 - 3.13 Cisco 5000 Series Enterprise Network Compute System: All versions Catalyst 8300 Series Edge Universal CPE: All versions UCS C-Series Rack Servers in standalone mode: All versions UCS E-Series Servers: All versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:integrated_management_controller:*:*:*:*:*:*:*:*:*	-
Cisco Integrated Management Controller CLI Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059.008: Network Device CLI, T1059 : Command and Scripting Interpreter	https://www.cisco.com/c/en/us/support/index.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2022-38028]()	✗	Microsoft Windows Print Spooler	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	GooseEgg
Microsoft Windows Print Spooler Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-38028

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-20353]()	✗	Cisco ASA Software and FTD Software	STORM-1849
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	-
Cisco ASA and FTD Denial of Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-835	T1498: Network Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20359	✗	Cisco ASA Software or FTD Software	STORM-1849
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	-
Cisco ASA and FTD Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4040	✗	CrushFTP	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*:*	-
CrushFTP VFS Sandbox Escape Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1336	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.crushftp.com/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27956	✗	WordPress Automatic plugin	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:automatic_plugin:*:*:*:*:*:*:*:*	-
WordPress Automatic Plugin SQL Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://wpscan.com/vulnerability/53a51e79-a216-4ca3-ac2d-57098fd2ebb5/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-3259	✗	Cisco Adaptive Security Appliance (ASA): 9.5 - 9.13 Cisco Firepower Threat Defense (FTD): 6.2.3 - 6.5.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*	Akira ransomware
Cisco ASA and FTD Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1082 : System Information Discovery, T1190: Exploit Public-Facing Application	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20269	✗	WordPress Automatic plugin	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:automatic_plugin:*:*:*:*:*:*:*:*	Akira rasnomware
Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863, CWE-288	T1068: Exploitation for Privilege Escalation, T1110 : Brute Force	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atomic Stealer	Atomic Stealer, also known as AMOS (Atomic macOS Stealer), is a malicious program that targets macOS devices. It's classified as a stealer, a type of malware designed to extract and steal sensitive information from infected computers.	Malicious ads, fake software updates	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	macOS
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Realst stealer	Realst stealer malware is a type of information-stealer malware that targets macOS devices. It is designed to steal a variety of sensitive information from infected computers.	Disguised as fake blockchain games	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		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
UNAPIMON	UNAPIMON is a straightforward DLL malware written in C++, designed to prevent monitoring of child processes. It achieves this by hooking into the CreateProcessW function and unhooking critical API functions in child processes, thereby allowing malicious activities to go undetected.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Evasion of Security Measures and Financial loss	Windows and VMware
ASSOCIATED ACTOR			**PATCH LINK**
Earth Freybug			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SYNC-SCHEDULER	The Sync-Scheduler Infostealer, developed in C++, has emerged as a significant threat, hidden within Office document files. This malicious software boasts sophisticated anti-analysis features, allowing it to swiftly terminate operations upon detecting any analytical environment.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		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
RotBot	RotBot malware is a variant of the QuasarRAT client, a malicious remote access tool (RAT) designed for stealing information and granting remote access to attackers.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data Theft and Remote Access	Windows
ASSOCIATED ACTOR			PATCH LINK
CoralRaider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XClient stealer	XClient is a dangerous stealer malware targeting Windows users. It can steal a wide range of information including login credentials, browser data, social media information, financial data, and even cryptocurrency holdings. XClient spreads through phishing campaigns and can have severe consequences for victims, leading to identity theft, privacy breaches, and financial losses.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			PATCH LINK
CoralRaider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrintSpoofer	PrintSpoofer, a tool for privilege escalation, leveraging PowerShell's "invoke-webrequest" command. This tool exploits the SeImpersonatePrivilege to escalate user privileges and is employed in attacks targeting vulnerable services like web servers or database service providers.	Exploiting Redis services	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage, Financial Loss	Redis
Tool			
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
Latrodectus	Latrodectus, a newly emerged malware believed to be an evolution of the IcedID loader, has been detected in malicious email campaigns since November 2023. It is suspected that the creators of IcedID are behind Latrodectus. Latrodectus functions as an emerging downloader, equipped with advanced sandbox evasion capabilities.	Phishing email	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		System Compromise, Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
TA577 and TA578			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nitrogen	Nitrogen malware strains through fake advertisements posing as installations for well-known system tools like FileZilla or PuTTY. Using a DLL sideloading technique, the malware executes a malicious DLL file by launching a legitimate program.	Malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		System Compromise, Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Raspberry Robin</td><td rowspan="6">The Raspberry Robin malware campaign, active since March 2024, employs malicious Windows Script Files (WSFs) to disseminate its malware. The Raspberry Robin employs a spectrum of anti-analysis and virtual machine (VM) detection mechanisms. The final payload remains dormant until the malware discerns that it is operating on a genuine end-user device rather than within a sandbox environment.</td><td>Social engineering and malvertising</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Information Theft, Espionage</td><td>Windows</td></tr>
<tr><td>Worm</td><td><b>PATCH LINK</b></td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">LazyStealer</td><td rowspan="6">A cybercriminal group known as Lazy Koala orchestrated a string of successful attacks. Despite the simplicity of their methods, the malware they deployed, named LazyStealer, demonstrated remarkable effectiveness. The stolen data is either sold or repurposed for subsequent attacks, often aimed at corporate internal systems.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Information Theft, Espionage</td><td rowspan="2">-</td></tr>
<tr><td>Information Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>Lazy Koala</td><td>-</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
Rhadamanthys	TA547, a financially motivated cybercriminal group in the recent attack campaign employed Rhadamanthys information stealer. The Rhadamanthys malware is directly downloaded into the system's memory. This technique, known as a fileless attack, bypasses traditional disk-based detection methods, making it more challenging to identify and prevent.	Phishing email	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Information Theft, System Compromise, Espionage and Financial Loss	Windows
ASSOCIATED ACTOR			PATCH LINK
TA547			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkBeatC2	DarkBeatC2, a malicious backdoor by Iranian hackers MuddyWater, infects systems through social engineering. It uses PowerShell scripts to silently load a hidden component (DLL) that grants remote access. This technique leverages legitimate functions for stealthy control of compromised devices.	Social engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Remote Control and Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
UPSTYLE	Upstyle, a custom Python-based backdoor. Designed to grant attackers remote control, it facilitates additional commands and potentially establishes persistence on the compromised firewall.	Exploiting vulnerabilities	CVE-2024-3400
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	Palo Alto Networks PAN-OS
ASSOCIATED ACTOR			PATCH LINK
UTA0218			https://security.paloaltonetworks.com/CVE-2024-3400

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
JsOutProx RAT	JsOutProx RAT is a Windows Trojan. Deceptive emails with attachments or website links trick users into downloading it. Once installed, attackers can steal your data, mess with your system, or install even worse malware. It's especially fond of targeting banks and financial institutions.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data breaches, financial losses, and data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
SOLAR SPIDER			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Agent Tesla	The Agent Tesla malware, classified as a remote access trojan (RAT), demonstrates remarkable proficiency in infiltrating systems to extract sensitive information like keystrokes and login credentials from web browsers and email clients.	Phishing	CVE-2017-11882
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data Theft	Microsoft Office
ASSOCIATED ACTOR			PATCH LINK
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos	Remcos, a legitimate remote access tool, is misused by attackers for total system control. It hides, escalates privileges, and persists on reboot. Phishing emails, exploit kits, and watering hole attacks are common delivery methods.	Phishing emails, exploit kits, and watering hole attacks	CVE-2017-11882
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote Control and Data Theft	Microsoft Office
ASSOCIATED ACTOR			PATCH LINK
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LokiBot	LokiBot, an information-stealing Android malware, targets your bank accounts. It lurks in seemingly harmless apps, stealing login details and bypassing two-factor authentication. Once LokiBot infiltrates your device, it can steal messages, spy on calls, and even grab your contacts.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Financial Loss and Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FormBook	FormBook, identified in 2016, is an infostealer malware. It infiltrates systems to pilfer diverse data like browser-cached credentials, screenshots, and keystrokes. Moreover, it functions as a downloader, facilitating the retrieval and execution of further malicious files.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Guloader	Guloader malware acts like a secret agent, dropping off harmful payloads on your device. This sophisticated downloader, first spotted in late 2019, uses a variety of tricks to evade detection. It encrypts its malicious code, disguises itself within legitimate processes, and even alters its behavior if it suspects it's being analyzed.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Deploys other malware and Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SnakeKeylogger	SnakeKeylogger, a sly keylogger and data thief, slithers past defenses, stealing your keystrokes, screenshots, and clipboard data. It uses email, FTP, and even Telegram to send this intel to attackers, putting your online accounts, privacy, and finances at risk.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Keylogger		Data Theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Xworm	XWorm, marketed as a malware-as-a-service, operates as a remote access trojan (RAT) with a comprehensive toolkit for hacking. It can extract sensitive information and files from compromised computers, seize control of MetaMask and Telegram accounts, and monitor user actions.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data breaches, financial losses, and identity theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
TA558			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LockBit 3.0	LockBit 3.0 ransomware also known as LockBit Black, that encrypts your data and might steal it too, threatening to leak it if you don't pay. Known for its evasive tactics, it targets enterprises and operates as a RaaS service.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FatalRAT	FatalRAT, a Remote Access Trojan, initiated a targeted phishing campaign primarily targeting cryptocurrency enthusiasts, especially those utilizing the Exodus platform. This campaign strategically deploys FatalRAT alongside additional malware such as Clipper and Keylogger, specifically focusing on Chinese-speaking individuals and organizations.	Phishing emails	CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data breaches, financial losses, and data theft	Microsoft Office
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Carbanak	Carbanak Backdoor also known as Anunak, is a sophisticated backdoor equipped with data theft functionalities and a modular design. Its capabilities encompass keylogging, desktop video recording, VNC access, HTTP form interception, file system manipulation, file transfer, TCP tunneling, HTTP proxying, OS sabotage, theft of POS and Outlook data, and reverse shell functionality.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7			-

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
Waterbear	Waterbear has undergone more than 10 iterations since 2009, featuring a diverse range of measures to counter debugging, sandboxing, and conventional antivirus efforts. Waterbear employs a genuine executable to facilitate the loading of its proprietary DLL file.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
Earth Hundun			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CR4T	The CR4T Backdoor is crafted with the main objective of providing attackers with access to a command-line console on the victim's system. Moreover, it enables the downloading, uploading, and alteration of files. This backdoor empowers attackers to run command lines on victims' machines, facilitating malicious actions such as file manipulation and data extraction.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Upload Files, data manipulation	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cryptbot	CryptBot represents a common type of infostealer that specifically targets Windows systems. Its primary function is to pilfer sensitive data from compromised computers, including credentials from web browsers, cryptocurrency wallets, browser cookies, and credit cards. Additionally, it captures screenshots of the infected system.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	
ASSOCIATED ACTOR			**PATCH LINK**
CoralRaider			-

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
LummaC2	LummaC2 is a widely known information stealer notorious for its efforts to gather data from victims' devices. Its initial exfiltration stage involves establishing a connection to the C2 server. If it fails to receive an "OK" response from any of the designated C2 servers, the malware will terminate the process. The subsequent step involves extracting information from compromised machines.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
CoralRaider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys	Rhadamanthys is an information stealer coded in C++ that surfaced in August 2022. It focuses on acquiring credentials for email accounts, FTP servers, and online banking services.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
CoralRaider			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GooseEgg	GooseEgg is a launcher application with the ability to carry out multiple malicious actions, operating with SYSTEM-level permissions. These actions include remote code execution and lateral movement within compromised networks.	Exploiting Vulnerabilities	CVE-2022-38028
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Code Execution	Windows
ASSOCIATED ACTOR			PATCH LINK
APT28			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-38028

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
KageNoHitobito	KageNoHitobito ransomware is specifically engineered to encrypt files solely on the local drive, excluding networked drives from its encryption process. Encrypted files are marked with a ".hitobito" extension.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt data	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DoNex	DoNex ransomware employs encryption mechanisms on both local drives and network shares, as indicated by the settings of <local_disks> and <network_shares> being set to true. Affected files have a victim ID appended as a file extension, and their file icons are altered by the ransomware.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira	The Akira ransomware group has become notorious for its malicious activities, having accrued a staggering $42 million through unauthorized means by infiltrating the networks of over 250 victims as of January 2024.	Exploiting Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Microsoft 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.

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Earth Freybug	China	-	Worldwide
	MOTIVE		
	Espionage and Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	UNAPIMON	Windows and VMware
TTPs			
TA0004: Privilege Escalation, TA0043: Reconnaissance, T1574: Hijack Execution Flow, T1106: Native API, T1053.005: Scheduled Task, T1053: Scheduled Task/Job, T1592: Gather Victim Host Information, T1574.002: DLL Side-Loading, T1190: Exploit Public-Facing Application, T1059.001: PowerShell, T1059: Command and Scripting Interpreter, T1082: System Information Discovery, T1574.006: Dynamic Linker Hijacking, T1036: Masquerading, T1547.001: Registry Run Keys /Startup Folder, T1547: Boot or Logon Autostart Execution, T1489: Service Stop			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA577 (aka Hive0118)	-	All	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Latrodectus downloader	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0040: Impact; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1055: Process Injection; T1497: Virtualization/Sandbox Evasion; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA547 (aka SCULLY SPIDER)	-	All	Germany
	MOTIVE		
	Financial Gain, Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Rhadamanthys	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA578	-	All	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	Latrodectus downloader	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0040: Impact; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1055: Process Injection; T1497: Virtualization/Sandbox Evasion; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Lazy Koala	-	Government, Financial, Medical, and Educational Institutions	Russia, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Armenia
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	LazyStealer	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1204.002: Malicious File; T1204: User Execution; T1140: Deobfuscate/Decode Files or Information; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1567: Exfiltration Over Web Service; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.006: Python; T1055: Process Injection; T1211: Exploitation for Defense Evasion; T1027: Obfuscated Files or Information; T1212: Exploitation for Credential Access

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, Boggy Serpens, Yellow Nix)	Iran	-	Israel
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	DarkBeatC2	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1036: Masquerading; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1071: Application Layer Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
SOLAR SPIDER	-	Financial Services, Banking	APAC and MENA regions
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	JsOutProx RAT	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and: Control; TA0010: Exfiltration; T1036: Masquerading; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1055: Process Injection; T1027: Obfuscated Files or Information; T1212: Exploitation for Credential Access; T1056: Input Capture; T1082: System Information Discovery; T1567: Exfiltration Over Web Service; T1657: Financial Theft; T1566: Phishing; T1567.001: Exfiltration to Code Repository			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TA558	-	Industrial sector, service sector, public sector, electric power industry, counstruction, Transportation companies, Sports, Information Technology, Education, Religious organizations, Finance, Pharmaceutical industry	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2017-11882	AgentTesla, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1566: Phishing; T1566.001: Spearphishing Attachment; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1132: Data Encoding; T1132.001: Standard Encoding; T1071: Application Layer Protocol; T1071.002: File Transfer Protocols; T1217: Browser Information Discovery; T1056: Input Capture; T1125: Video Capture; T1123: Audio Capture; T1033: System Owner/User Discovery; T1555: Credentials from Password Stores; T1204: User Execution; T1204.003: Malicious Image			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)	Russia	Automotive	USA
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Carbanak Backdoor	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1027: Obfuscated Files or Information; T1021.004: SSH; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1057: Process Discovery; T1059.001: PowerShell; T1069.002: Domain Groups; T1082: System Information Discovery; T1087.002: Domain Account; T1090: Proxy; T1124: System Time: Discovery; T1204.002: Malicious File; T1222.001: Windows File and Directory Permissions Modification; T1543.003: Windows Service; T1562.004: Disable or Modify: System Firewall; T1564.001: Hidden Files and: Directories; T1566.002: Spearphishing Link; T1566: Phishing; T1571: Non-Standard Port; T1583.001: Domains; T1608.005: Link Target; T1569.002: Service Execution			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Earth Hundun (aka BlackTech, Circuit Panda, Radio Panda, Palmerworm, TEMP.Overboard, T-APT-03, Red Djinn, Manga Taurus)	China	Technology, Research, Government, Construction, Financial, Healthcare, Media	China, Hong Kong, Japan, Taiwan, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Waterbear backdoor	-

TTPs
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1129: Shared Modules; T1106: Native API; T1574.002: DLL Side-Loading; T1547.012: Print Processors; T1027.001: Binary Padding; T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1497.003: Time Based Evasion; T1622: Debugger Evasion; T1083: File and Directory Discovery; T1016.001: Internet Connection Discovery; T1049: System Network Connections Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1012: Query Registry; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1071.001: Web Protocols; T1573: Encrypted Channel; T1132.002: Non-Standard Encoding

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
STORM-1849 (aka UAT4356)	-	Government, Critical Infrastructure, Telecommunication, Energy	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-20353, CVE-2024-20359	-	Cisco ASA Software and FTD Software
TTPs			
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1037: Boot or Logon Initialization Scripts; T1040: Network Sniffing; T1041: Exfiltration Over C2 Channel; T1055: Process Injection; T1059: Command and Scripting Interpreter; T1070.004: File Deletion; T1071.001: Web Protocols; T1102.003: One-Way Communication			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
ToddyCat	China	Defense, Government, Telecommunications	Afghanistan, India, Indonesia, Iran, Kazakhstan, Kyrgyzstan, Malaysia, Pakistan, Russia, Slovakia, Taiwan, Thailand, UK, Uzbekistan, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0010: Exfiltration; TA0011: Command and Control; T1027: Obfuscated Files or Information; T1105: Ingress Tool Transfer; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1057: Process Discovery; T1211: Exploitation for Defense Evasion; T1068: Exploitation for Privilege Escalation; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1090: Proxy; T1124: System Time Discovery; T1204.002: Malicious File; T1029: Scheduled Transfer; T1007: System Service Discovery; T1562.004: Disable or Modify System Firewall; T1564.001: Hidden Files and Directories; T1053: Scheduled Task/Job; T1055: Process Injection; T1059: Command and Scripting Interpreter; T1021.004: SSH			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
CoralRaider	Vietnam	Computer service call center organizations and civil defense service organizations	U.S., Nigeria, Pakistan, Ecuador, Germany, Egypt, the U.K., Poland, the Philippines, Norway, Japan, Syria and Turkey
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	RotBot, XClient stealer, Cryptbot, LummaC2 and Rhadamanthys	Windows

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1059.007: JavaScript; T1204: User Execution; T1204.002: Malicious File; T1104: Multi-Stage Channels; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1112: Modify Registry; T1083: File and Directory Discovery; T1140: Deobfuscate/Decode Files or Information; T1041: Exfiltration Over C2 Channel; T1055: Process Injection; T1036: Masquerading; T1027: Obfuscated Files or Information; T1608: Stage Capabilities; T1608.001: Upload Malware; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1555: Credentials from Password Stores; T1217: Browser Information Discovery; T1105: Ingress Tool Transfer

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT28 (aka Sofacy , Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard,BlueDelta,TA422, Fighting Ursa,Blue Athena)	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Energy, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Saudi Arabia, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2022-38028	GooseEgg	Microsoft Windows Print Spooler
TTPs			
TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0002: Execution; TA0007: Discovery; TA0042: Resource Development; TA0008: Lateral Movement; TA0005: Defense Evasion; T1112: Modify Registry; T1559.001: Component Object Model; T1559: Inter-Process Communication; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1588: Obtain Capabilities; T1083: File and Directory Discovery; T1588.006: Vulnerabilities; T1588.005: Exploits; T1584: Compromise Infrastructure; T1555: Credentials from Password Stores; T1068: Exploitation for Privilege Escalation; T1574.006: Dynamic Linker Hijacking; T1574: Hijack Execution Flow			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Muddling Meerkat	China	All	All
	MOTIVE		
	-		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-
TTPs			
TA0042: Resource Development; TA0043: Reconnaissance; TA0040: Impact; T1594: Search Victim-Owned Websites; T1584: Compromise Infrastructure; T1584.002: DNS Server; T1584.003: Virtual Private Server; T1584.001: Domains; T1584.005: Botnet; T1595: Active Scanning; T1595.002: Vulnerability Scanning; T1596: Search Open Technical Databases; T1593: Search Open Websites/Domains; T1498: Network Denial of Service			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1115: Clipboard Data	
	T1123: Audio Capture	
	T1584: A136:A151Compromise Infrastructure	
	T1560: Archive Collected Data	
	T1557: Adversary-in-the-Middle	
	T1113: Screen Capture	
	T1530: Data from Cloud Storage	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0043: Reconnaissance	T1592: Gather Victim Host Information	
	T1590: Gather Victim Network Information	
	T1593: Search Open Websites/Domains	
	T1594: Search Victim-Owned Websites	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1596: Search Open Technical Databases	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
		T1583.008: Malvertising
	T1587: Develop Capabilities	T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.005: Link Target
	T1650: Acquire Access	
	T1588: Obtain Capabilities	T1588.005: Exploits
	T1584: Compromise Infrastructure	T1584.001: Domains
		T1584.002: DNS Server
		T1584.003: Virtual Private Server
		T1584.004: Server
		T1584.005: Botnet

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1659: Content Injection	
	T1189: Drive-by Compromise	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1078: Valid Accounts	T1078.003: Local Accounts
TA0002: Execution	T1203: Exploitation for Client Execution	
	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	
	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
		T1059.008: Network Device CLI
TA0011: Command and Control		T1071.001: Web Protocols
	T1090: Proxy	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
	T1659: Content Injection	
	T1219: Remote Access Software	
TA0006: Credential Access	T1003: OS Credential Dumping	
	T1056: Input Capture	T1056.001: Keylogging
	T1212: Exploitation for Credential Access	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.005:Password Managers
		T1555.003: Credentials from Web Browsers
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.003: NTDS
	T1557: Adversary-in-the-Middle	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
		T1567.001: Exfiltration to Code Repository
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1537: Transfer Data to Cloud Account	
	T1029: Scheduled Transfer	
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
TA0040: Impact	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1657: Financial Theft	
	T1489: Service Stop	
	T1486: Data Encrypted for Impact	
	T1496: Resource Hijacking	
	T1490: Inhibit System Recovery	

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1036: Masquerading	
	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	T1564.001:Hidden Files and Directories
	T1622: Debugger Evasion	
	T1550: Use Alternate Authentication Material	
	T1014: Rootkit	
	T1134: Access Token Manipulation	
	T1220: XSL Script Processing	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
	T1562: Impair Defenses	T1562.001:Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
TA0007: Discovery	T1007: System Service Discovery	
	T1033: System Owner/User Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1124: System Time Discovery	
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1622: Debugger Evasion	
	T1518: Software Discovery	
	T1046: Network Service Discovery	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	T1069.001: Local Groups
	T1069: Permission Groups Discovery	T1069.001: Local Groups
	T1482: Domain Trust Discovery	

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	T1021.004: SSH
		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

Top 5 Takeaways

#1

In **April**, **eight zero-day** vulnerabilities were identified across various platforms, including **XZ Utils**, **Palo Alto Networks, WordPress, Microsoft, Adobe, D-Link, Cisco, Open Metadata** and **Fortinet**. These vulnerabilities were actively exploited in attacks by adversaries.

#2

Throughout the month, ransomware strains including **LockBit 3.0, KageNoHitobito, DoNex,** and **Akira** actively targeted victims.

#3

Numerous malware families have been observed targeting victims in the wild. These include **Rhadamanthys, PrintSpoofer, DarkBeatC2, UPSTYLE, LockBit 3.0,** and **AgentTesla.**

#4

There were a total of **15** active **adversaries** identified across multiple campaigns. Their focus was directed toward the following key industries: **Government, Finance, Technology, Education,** and **Transportation**

#5

In the **ArcaneDoor** cyber-espionage campaign, the state-sponsored threat actor named **STORM-1849** exploited two Cisco zero-day vulnerabilities in firewall devices. They targeted government network perimeters, deploying two custom-built backdoors as part of their operations.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **23 significant vulnerabilities** and block the indicators related to the **15 active threat actors, 34 active malware,** and **221 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 **23 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 (APRIL 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 🔴⚔ 🔴👽					

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
Atomic Stealer	SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d,
	IPv4	194.169.175[.]117
XClient Stealer	SHA256	4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643
Rotbot	SHA256	e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f, 0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0, 28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f, d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e, de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4, 020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34, 1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3, 93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c,
UNAPIMON	SHA256	62ad0407a9cce34afb428dee972292d2aa23c78cbc1a44627cb2e8b945195bc2
Agent Tesla	SHA256	8ba55cc754638714764780542eefd629c55703ecf63ae20d5eb65b8c14d3e645, 87709f72683c5ffc166f348212b37aadb7943b5653419f2f0edf694fb50f1878, 691761d401a6650872d724c30b7ef5972e3792e9a2ba88fdca98b4312fb318d8

Attack Name	TYPE	VALUE
Realst stealer	SHA256	6574315524dde9a8c47d7f1ba411fb5fa6421721c24a629c72ce8cd32c0d1b34, 6344fb8cd00b8e94671144c2877dbb337e8e98648f43e7954fa3fa01b4ae3357
SYNC-SCHEDULER stealer	URL	http[:]//syncscheduler[.]com/r3diRecT/redirector/proxy[.]php
	SHA256	2027a5acbfea586f2d814fb57a97dcfce6c9d85c2a18a0df40811006d74aa7e3, 203d60fe1ebbfafc835e082774ee56088273d9455fb12ac1de2c1be410cceeec, 6e4a4d25c2e8f5bacc7e0f1c8b538b8ad61571266f271cfdfc14725b3be02613, 316e01b962bf844c3483fce26ff3b2d188338034b1dbd41f15767b06c6e56041
	IPv4	146[.]70[.]157[.]120
Latrodectus	URLs	hxxps://mazdakrichest[.]com/live/, hxxps://riverhasus[.]com/live/, hxxps://peermangoz[.]me/live/, hxxps://aprettopizza[.]world/live/, hxxps://nimeklroboti[.]info/live/, hxxps://frotneels[.]shop/live/, hxxps://arsimonopa[.]com/live, hxxps://lemonimonakio[.]com/live, hxxps://fluraresto[.]me/live/, hxxps://mastralakkot[.]live/live/, hxxps://postolwepok[.]tech/live/, hxxps://trasenanoyr[.]best/live/, hxxps://miistoria[.]com/live, hxxps://plwskoret[.]top/live, hxxps://sluitionsbad[.]tech/live/, hxxps://grebiunti[.]top/live/, hxxps://zumkoshapsret[.]com/live/, hxxps://jertacco[.]com/live/
	SHA256	fc21a125287c3539e11408587bcaa6f3b54784d9d458facbc54994f05d7ef1b0, 465f931e8a44b7f8dff8435255240b88f88f11e23bc73741b21c20be8673b6b7, 9e7fdc17150409d594eeed12705788fbc74b5c7f482a64d121395df781820f46, 53b0d542af077646bae5740f0b9423be9fb3c32e04623823e19f464c7290242f, 9fad77b6c9968ccf160a20fee17c3ea0d944e91eda9a3ea937027618e2f9e54e,

Attack Name	TYPE	VALUE
Latrodectus	SHA256	d8b902568386f588fb2d42a77cd39062ada13c9a3fed0adf20ab6510f3b4a681, 805b59e48af90504024f70124d850870a69b822b8e34d1ee551353c42a338bf7, d855daede0b97277d68e04c73ef0f2a36690faa77539914aa7948ee045427042
Nitrogen	URL	amplex-amplification[.]com/wp-includes/FileZilla_3.66.1_win64.zip, newarticles23[.]com/wp-includes/putty-64bit-0.80-installer.zip, support[.]hosting-hero[.]com/wp-includes/putty-64bit-0.80-installer.zip, mkt.geostrategy-ec[.]com/installer.zip
	SHA256	ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281, 2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945, 033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf
	IPv4	94.156.65[.]98, 94.156.65[.]115
Raspberry Robin	Domains	chroococcoid.sbs, polyideism.sbs, ophthalmomyositis.sbs, quarrelers.sbs, counterboring.sbs, brittlebush.sbs, noematachograph.sbs, hemimetabolism.sbs, spendthriftiness.sbs, misalienate.sbs, smartville.sbs, refractorily.sbs, syllabication.sbs, uninsolvent.sbs, mammaterijekasumy.sbs, dechlorinatingdermatropic.sbs, axiologies.sbs, okruzihealdsburg.sbs, halsalkalindivvies.sbs, squeezably.sbs, contretemps.sbs, indulgement.sbs, viandelarkishness.sbs,

Attack Name	TYPE	VALUE
Raspberry Robin	Domains	cunyguddlefrodina.sbs, audiovisuals.sbs, perrputtnomi.sbs, azoospermia.sbs, metriconetimeagley.sbs, dundeelieflydeflect.sbs, juniorstwosometogt.sbs, nametagsweatseyelike.sbs, glubeulaufuggy.sbs, bootedpindusvalenba.sbs, rockerstalbertcerate.sbs, biltongpumpsiecrumrod.sbs, jossesdialykreamer.sbs, ingressfloor-walker.sbs, freamingrafttwoway.sbs, craighleserapic.sbs, acid-fastlindbom.sbs, annuelertimes.sbs, kepfoipnjw.sbs, semantical.sbs, dominieunflaming.sbs, urvkwwqhjb.sbs, undefinitely.sbs, 294unmendaciously.sbs, oilproofing.sbs, sphere-born.sbs, 294anacamptometer.sbs, proconsulships.sbs, unthematically.sbs, hockersmixtecsquier.sbs, arctiidkwatumaindwelt.sbs, curricular.sbs, buxbaumiaceae.sbs, subextensibleness.sbs, unconstrainedness.sbs, anguilliform.sbs
	SHA256	553b9eaa741adfb9073638e001d369441a802b406d3bca50436aea1df5b16da5, 4c87daaa84c41706156d370603602147988262229f5dedd6c46c821d879409509, 4e93fb810189d3e1df1d0ef0f30642b8891e4140301a4aaaf5cb93955588734d, 0b369277901fff2ac52bf04e366318aa9018e7ea570779f476b2a0e676c9db83, ca6f46bdfd14021c102d4e4d95597a20bb9685628b4067b9ba85f18644ad6cdb,

Attack Name	TYPE	VALUE
Raspberry Robin	SHA256	98ad6aad996e4005389ea7e4782a4a082c1e83a8a20ad07bb3a3eed4047b3603, 9303b89abe2c0393e78991f74a90d9202a2f14dc267367277da7af705733eb32, 229c6b0dc9298a6868a24aad6cf3c8b08feb97f809f2d67fb6dc2e71ebee876b, 78ae67f650400ef6db9a85aa3d10ab7684f789e587ef33420a352a9b53916364, dd576545834e9c439491d62a8a6d9578a58693cef9f5cd2783fc80f49275dac8, fbdbe211e66792f3cefc50da6b3b88d82d497be1cd25f4654d4d122c0ed10a42, a3de553cae9671bd94aae75f76f8de2dd9abb41780d25f012debf7761a579ea9, 479d1cb582c03c679cb23ccb6b5dd1611822f59f311a6cdc82bd6eef5f53da14, d5dd3f1dd787746403843100c8dec9c70c20d8098071aafc5bfeef20b95fd93f, b4566c3cbfa193ad6dc7173d8b5d93734f06d940085110f6a2c7812524c2c236, 752ccebfcf2d63d44bf3073b2f30e83758aa0ae26d3bdca59de6e53e6d33b19e, a81176e32b8d73fbbd11d1a1da32789c8b18cf6aa79e1b4cae8ed031b7e9dbbf, 99d1e9839922063d3655583d541ac6908000222cd847c95c919a27c9d2b01301, 07b19580d9c5febb2b7d1da395022ca790372104bc99b35a8b18d506dfa2f9c0, 8921a869a93b4e9cec50b66b81793af67c2664aec5028c48738bae03f7026560, 981e56f56ab9c3dc81deed819ad3cd7367b8d44449a1ebbf1aad5033f2bd4547, 068f7a941ca655d71dd894c1564a24bbe9d67a6aa9e60b0692f558512e28c3a4, f2e1130b4baf1dc611fdde8029234348b4df69d5ebe32edc540e6fe1caaadd0a
LazyStealer	MD5	4f060c5c6813e269f01e6cba1d3ac4cd, 641932b66490630005dde2aef405e5e9, 882d63c5ff749f232a3ce70a36c95b83, fe245cf57be8b3daf8cdb3882de99f35, 8e233b0250d85ae63076af45ee829c55, 032a586d08e7f31e2aedbec61d5d0f62, 8cb819b48958540fac07244188508156, 2d51a6620c976e1d736448082338e0b1, 763eb39787756744b4062336eb945750,

Attack Name	TYPE	VALUE
LazyStealer	MD5	5b84b516760773c538647bc6e4d26d37, 1dedf5772ea1126b79b5e22ca10cefd3, 0f5727bada96b3b62573bba51538e9e3, c3242bce783d5fa0ab0ce645f1283c64, 1cff5f65c85d8cf614beedf8fd5112d7, 98914403f428abeea89c94e0b7edaaa9
	SHA1	4f0a1831d4d8c09f46e8f5fbe8b17b024daa6eee, 9bad63eab92144b8a365428aa68531c80fc2da0f, cd1f89f3d56df6a775d8694c1cbf588961dc7f06, 40789ef406772e52a0dfc86509cc7617fa8b54a3, ec14cf28fe8764d4f285b95ee7001af49ff0af68, 51ad91409698d8f4017defbd0a382cce9e69ed6f, 1f204cfb02df849f935c296a5e4b2f120bfa563b, 755ade0ddaceaabe9577d22a240e0430375f502f, 7685dd23d64fa94bb8d2d54dd2e104fbe5379ec5, 3e497222f9bc13d43d6a3e5fbdcae3474b3d2d22, 140968b7004aca9785a0a1f0a6712322db22fd6c, 6f54d068423cee9b2cf5ef50b4348025f983e220, 845be44fb0d663636e500187d7d394714e562e08, c10637e35dfe326bd2c9a92f432d483f2f7591bd, 9866dfedbd311ed2f838ec56947cdf4ccabe8634
	SHA256	9fd197b7402285ed2a75dac9a5ce3ef499a58342fd0dcefe1c40443a12bc6832, e419a8158c6fe326dc7ab16dbd5f3b2723dffe8c9561fe835bb16f62a8fa61f5, a6e68f3066424daae4a54b2e0b01a4474a9a381469ae69daae6fef9a1626fa6d, 1db3d0ac68515b5c9876634605ba8492ba558f7df435bff2b20a74239107f3ec, 5ecdf5efe2a74db93450f2b35e942b91ee6dd1b0f545c04810d2794b748b1dea, 9fc75a6a17238ec3833dce0605b334c03fd84363f56313a5bf58d57ff286a9f9, 7d3733513e0645e66009e3d677af76653baa75c8ddf0d126aa0f270b56183272, 216f4e858f84269bee999fdc29dafbd79ec2270575e19a8626e25d5fe72a8f25, 8246e66ff043374477c06a612602f6e8a2cb487a33d8b046357a6c4870648ed1, ef6fb63259eac9f7642e468726a042f5a29576bf9f846b96fa6ded8bf145b64c, f2a8088f1a634e62a2d0e5b2d6427d67fae640bf03dd04c8571006e1f31d7992, bfa3718f6492dd337c127ccdbd8033b503ca089699ddbff3ac5c45f5f95f01e8,

Attack Name	TYPE	VALUE
LazyStealer	SHA256	1549114ea6d86198d29f79a009218ca991aa17d215a84b90e3c91ef3268180e4, 864a38b028d5b9e41fa0d4eee7cfa3a284d0ab9874b42cc4d50f1e2b2e26e1e5, 18e00bb5dee23815a89067258b11ef13d6327bcb3555d70596c906d4875ed8c2
Rhadamanthys	Domain	indscpm[.]xyz
	IPv4:Port	94[.]131[.]104[.]223:443
PrintSpoofer	MD5	dbdcbacbc74b139d914747690ebe0e1c, b26b57b28e61f9320cc42d97428f3806
	URL	hxxp://35.185.187[.]24/PrintSpoofer.exe
DarkBeatC2	MD5	3dd1f91f89dc70e90f7bc001ed50c9e7, Bede9522ff7d2bf7daff04392659b8a8, 32bfe46efceae5813b75b40852fde3c2, b7d15723d7ef47497c6efb270065ed84
	IPv4	45.66.249[.]226, 137.74.131[.]19, 164.132.237[.]68, 95.164.61[.]64, 95.164.46[.]54, 91.225.218[.]210, 95.164.38[.]68, 45.140.147[.]81, 80.71.157[.]130, 103.35.190[.]203, 95.164.46[.]253
UPSTYLE	SHA256	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
	MD5	0c1554888ce9ed0da1583dbdf7b31651
	SHA1	988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9

Attack Name	TYPE	VALUE
LockBit 3.0	SHA256	07926e060b7083bbe639b36e9c79cce23404ba9dcaa58c190ee40d7d415ff96f, 707bb3b958fbf4728d8a39b043e8df083e0fce1178dac60c0d984604ec23c881, 5e006f895382525e762a33e5dd5e8416bef56ae859f5e96f820cfba5c4c11226, c9dd51d4295c33e1df0d275669a1de9e1de374a51eb88d7f7b1a1e65f49f7794, 72a18c1e65869e5fce28667ce2b9069f9c180f4af3437193a12566fa1aa9d1a1, f7d05c0e9430ba0621020caad12fa1e8e62acb3bda349cd03240c1938ce7a887, 4dfa2dcbcfe39550255fcf5daaa4ee3b74e7ea3a32666c91c100fb6b8508544b, b2c3beda4b000a3d9af0a457d6d942ec81696f3ed485f7cf723b18008a5f3d10, e81d18241b9af3d08b7a8e98148d690489eaf8891ec7b00e932d9efccbc41860, 2d2a9923c2676d5950473cb9ecb0d4c0db55035ca7540ef5717d8cae2733ac5e, be05716fd6f750c771974985de80d71892e1842c8a760038888ff5008cb6f3e0, 988f9936c4990bc9769bade8353ce321983afb83026295a6b70537e5f1151040, 54e75fae8ee8ffbbee075c7694a7fbb1ed838030d36e9e9c4e454010229e230d, b7147a76c6695b750a84de55d4569f71f694b33aeefeef5daa09318ebabd9a24
AgentTesla	SHA256	C54A3C60BC528E8594C813C61A2F929666E0F22A3CA837612B9CD48442721853, 97A6F1686F456A126C4FD823B01DF49814C71DBF4E2F3458CE9C62F89DE17719, D86EAA75FDBC0D2DE5B239974B02038200247B981ECC99074E86B5AD51A5906A, 02A2A2779ECD2CD887B97930A56FA5C8977A0D8FEC04D06BF3FB65ACB418FE9F, CA528EB30885238A7E594075C68AFE244602E2438DA103C98DDD81CBDEAFFA2E, 091982DE7843B6D35B392A9526B3ABF94B6A89A0455FA3F1FF1A18AB823C307D, CBA91CA10CE9EC62E5785A3F2004655540054A281CB76A4FCE46B56441B2A119, 1B01030333E0A08D7D9E66C2D57C34DEB54704E8769C52149D543100A5BF86B8,

Attack Name	TYPE	VALUE
AgentTesla	SHA256	2091183DB00054D0DC8504468CDF15C10F9A4172DD36AFA1D18123E59155DCDC, CD4F4252279410BC08AB3F37CB032A87C0C98077C4FC9981266A9964C37274A9, 34DD266B2EC7F77DAE04BDCD14E82B0CF977E0C6CC689A1C8A49737BB18A86BE, 8694E70E25489684DD115CACC569DCEC2D1AACF86D97C395B7475DB75F7C711F, D85278C4099B913C69779C4B69A0C85CBB0D7CBE72AE9A324B798A0FD2E02FB7, F36D42A5E7745D82D8ABC396CF0B91784B3C0ED6B82CFCAC3B77D1D8F61BCF2B, C1BF99CC27B4632A1916CA5AF4D8946A38E1D29CA0CF5AF7EAB237C5DAC930FB, 308BBA46BFCB12039B06105BEF71AFCCD82ACB7DF7658A8A4497C1955C67EE5D, 8AD61CAE616332A206292501D56A552330901422E52FC09EB6FD7D85820C3E15, 9E2F5BAD6ACB0454F71026526CB9D5D78985EF6E566B433B04BA7ABA5B277DDB, A830EABA9888A6FA0A3CBF85DA3636F1C41AE7A0372CBC5CFAB0EFD197894FC9, F74C6A3DEF1CED2A6E4BC81FEC1B4F062EBA67CE271CA4A47271631986A6D1C3
Formbook	SHA256	50413921860A4F9DB3C3AB95C68154E9FFD12726C64A4A46D141499FCF448288, C4333322E47F6528C43A77936DEA4BCF9230A3EC68C527D931D3C1C8F6232BAF, 2EA01DEF771F0E57B541D4819DD9A543C5ADB3A4452C6F5C03EAC2C49C542BFA, 7C614154B6EC07D9D05E17100DA1B4223A07A5BE73F8002D0290B722B4C379C9, AA48EAF5253F8378F5E6DB8325D90E229E3D836080083C6269DE0969AF2854BA, 4E538F7F6D63185FC67C4DF0B3697709F3D420821C2E7B423FBE62C684C7F9AF, 26EE13CEB4C1B409A14DE72D0CF8E1F3B0CB4D92A416B8618CFF800DF7762FB1, C892E597C34DB8FD7F3B96CD87A613F34AC3CDC710BF8F82A86E7D98AEB90C25, 27B3F0E015EDCC476C4A71A0AEEDFB5E1FC711E56CA0027C4AA2B13D4078036C, 0948B592B85131C65EE3FA422E8E05BB2AF509B5BE7F59FA88AC6D0E5AD0743C,

Attack Name	TYPE	VALUE
Formbook	SHA256	609E38239C20A1B1A2A1D773E18E467FB8097DCB2F398580C8780FC27D1DF443, 0A8CE026714E03E72C619307BD598ADD5F9B639CFD91437CB8D9C847BF9F6894, 37AE91A0976D913BC1A194207829DC5460AFD7B12D4EE22A69129772D151F156, 8AEE0E7501795514AB18F454EB754FBA95090A590A7F1128EB1EA52DBABAB134, D79A768E106B5C09D20E48704AEB15F5ACCEA32C5E05D1693FF26F0D3A45374D, D4D5A21A5EA9100F99E0D037AF48B705F809C571D6F444C94715D0204EA7A8EF, 2423D7CB2BE18902BCDB5C9C5AE88B32F9F4D97C920A429AAF4AE1FF70D70B01, B780B2FB9E38BCC285F93125E548C0E7B896FB20A26400F20293C3C6634EBE2D, 3FED057E15C7C7AD6539672E9DAD14FC272B22C7DC21AB6BA73544A50EB2E5D6, 571114066B38641901A6A70CF10FC8C0D64167B09C220C19ACAD7D15505455C0
Ramcos	SHA256	6FF46BDE6F6AB139C685F220E33230D1C064A6E62F68047F3E97BC8F04727E1E, 2E5B8A1ED53E25C5DDD9B7CD97B86627BAF197A7E3893909BCF33360BEDA2F71, D72B9F4910CBE10F8D1B3EEB7096F26412FCE2B735C9929C354D8F20265ABA50, 593CF342A669FCB1BFF594BD8CE85FC112BC19D42F7FCB0932C9AC5CDF70D0D9, D0947156CDD5831F8F4CEDE0B54E7A0B0D43EEAFC4F85532032A406F65736A69, 9E6406269FE3E1F7A309E3EE01E4770D6F5C7ABD2DEAD9AFC7EDDFEDCDB04295, 16ED067E08AF1F57D826FC97D438A03DD9E69FBD191F64B241654635ACAE3277, 4143A027AF3C078D252C462F6101CC1B4B849402280371D9279E6FA62EE6CF75, 91741818480B13EAAC1D5547B488142FE2DF86B8EB51B62B31ACBFD5FEF53F47, 1035DBC121B350176C06F72311379B230AAF791B01C7091B45E4C902E9ABA3F4, B2D5E15268CB130C995118E17AFA1198CA19604A20B91F1907A7EF18210DB30F, 1EC10BE5E16B3BF64560B88F44D02A4BD759E6F7D19F1BDFC6AA8AD2015371AB,

Attack Name	TYPE	VALUE
Ramcos	SHA256	B201D9C6A3A0C85ACBF87DF1BDC9D1377F389867E7807B7CECE516B9AD6EFA7B, 9137A41DDF1827FBC839DD16CF40CEEC512BEC3465CBA4A691D0FC543686A03A, BAD6DC695EC91155FBF548D43E3039C1B694DB28C1A713B81ECC2D59674635CB, BDAEB27128A9D6DBCD93B0844D57E6DE8A03EC3B53B1380F41523EC35AD6AF18, 4F138CD5C06D63316037E0622FA6C9E91A6798C78A45730777296C332DC4B98C, 45E734BC929BDEFEAA6F09BA766B8EF86CA2AF2B8534CA756420E6C5A39413F3, 7BCDC2E607ABC65EF93AFD009C3048970D9E8D1C2A18FC571562396B13EBB301
LokiBot	SHA256	40B9D6C7BD8BBDC15EF53C7067C6282A37B1AFE5796F721ADEB42E2E606521FF, 6255A5B13CA4D4C4CA7A43EADA557F7F248B124690BA49E11535E1C6496EFFD8, 861AC33701D696AA03435C2A6A6985C76EE1A38AB86CAD1C21CDBD15237A35DD, 5DB6A8DFAFD6956BEAF4127500CD5232D78D70165A1775FA1DA58277A43327ED, A5748DCF451F0661BDB05C9075327BD7EA6CB654B05140F4F2DD0B169AC26BC8, 3DDAE440455EE0723B4035FD75927DB44A82F22056C2657FADC125BFF94172BA, C16A14B36E6F0FDD1D74867149808CEBBDA3D2BC713359C98A781BA856FA8246, A725AC3C18D2E27DC053DFCA8284030D4280DEBFE9EA66523CC7AEAC491A4C48, A4B40080FE1EE2FA7A916BE8D7738DAB8F934F1D0367AF6462FA1F0DDD1BAB40, 130B3179FAF1683E10847BCF542AF95829A6509C99B409FEC11B5B040C345094, 237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D, 63F63156E794305B1847F85AEA00C20690BBFE942A27ACF718F5DA3B51EFCA37, 5929347CDE36BD71909DFC96BF2278A424054A21466C3DA91B58467B2D7D6D91, 677094197476508F5E6D59632ACE2106FC0A07435850F1541FF69BE9E939C7BF, A66799C33360147031E8A33775C723CC426256FA2BEC9773B8802FFB33D32AA5,

Attack Name	TYPE	VALUE
LokiBot	SHA256	5E0A6BF1CB4D379D238D51CDAB8BD64B47C10C2921F3F2CB1F6DA2B33C8AC332, 93A26C45838C0147B6227526EF8ABAD9CFABB115300E703C0C169CA7D3A7D77E, B744BAE65129D2D9980029A4D55B4552C79A28A5AFA89B48E0A383B96078231A, 630821BFAE07B41945A9EBF48D20EABDB4AD0E7B74CC58606E45597287A48738, A1CDE47A700A9372C2DE3C0566C895812DC3D9B7DD77E14C282C2E00611B436C
Guloader	SHA256	2582A3D44619CF80599337232301B2A1C06B706B397CB45718F15A0311871578, A50C71D12A6C7DEA4F7B1494A592FF459A42EA2511F82328ACB04DEB65E0861B, C637A1D9397AED930B59ED64B88233432B601BF7F2A2934AD2DE0A243DB30983, C3F62B8F93B8EA82168EB60074369A55855D637798D246182A3FE0E40F70DCC7, 6EEEB05646DC1C6DB8F8FB818A3148548100334EC73108506E5434E5F18B8888, C21E99F913EF55751C39FF7A605335CC0C3598D70CAEE0D40193C70A8DA2B9DB, 89ED1483ADE890ADA1D088CA1C76A378ED83043FE2DFC877B69788A5857B375C, EA7EED758FFF9ABB8044BFFA0BF0A0FE8865A10EA1124D245A9F1B39725429AC, 8596299CDDDE8AA075B0CE5CCA5AF805BBBD1CFA1FC6D54319060369FFAB275D, 2C92015C742474E9A12B6AF28085F85A0DD10F76E4882F8B51693253291A8B23, 7B53347CFFA39B9146236CBCDCBF2C40BE98CA5CB360BBE07E1F10B20E391B49, 3C6D1AEAC47CA58D37C43AF7C826E5D5727B33F0171D15708A3B9D602D2B5A10, 920E040D64758438D2BA1514B29A497C8D7C0822D19C8B9F9DF24D1A03583983, 676146162491E834C2F073B6B5499416C93141AE4D6B817D0F2D5E41EBBB581F, 75DCA4592067755F34E2ECA369ECA24BFBDE194A2F870FB79CD26B42046AAD98, F8A1D6FC26EE5CFEC7E2BB4FA4AAC2A4F4FA57DDF10589D60202E89A592223F0, 504A1971A4AD0A3006F67DF485B92EF5F0BEF5510ADF777E24DE9437C28CAB48,

Attack Name	TYPE	VALUE
Guloader	SHA256	C8E32720B969178C753329B176A0CC34AF8ED2317DCE003CFE52E55D3E07E81E, 4365FF3C93EE1FAA413AB7CF6838884C449053479D3039E995A6CDFE590125E4, 26D95099636E212FCCB35C4865A6AAEE393079698B6C3A6F0A07EF2960A845B0
SnakeKeylogger	SHA256	3B50796D11C0837412A2D9205F28604EF9C02EA436E33F9CB46AC3B99E1BBC37, 061EE3375DC3333D8C4266E773535E516206935D4F7DBBC3F0319D253840213D, F8C1925693A82D8A544BEDCF975160A6CBD8A0D0E2A463E402402D8D28AD6E8D, 1624A0E8F86CF5331CCF66FD830A96827FC0B3DD842ABB268996D2387F2ED4BE, 07A1258C5EF18D86C00F843408AA21667C7817B8E7D1EAD1A5411856D0D21ED7, 36E9496A87CA35BF4D8D4D8E800BC82371D6DB67B8B19ED0C0C37FBC66EF8A5B, B932E7EC61F1CC9B3C858A55EB883ACCF378580572077C2676ADCF2A0AA8DDE1, E417867AC84D86D4B244788731D9C840FF0537640665083D293D077633F0628E, 53F9DACF7CCBE8AF215F3CB912F7C2ABB468505D5C1430137C82C4B60997C424, 2D00AFFF6535A1FAFD100B518B45019EC4645AFB3C105670F71CEB6CDF552814, 4ADA7E83E7FFA97F90588475D5C9356A9F1003E1CC7721D227CA0609EF23E9DC, D156D6626E85584270B990B2B53C325A53BE473E21C6FD32E1AC4E50301EE165, 7DB30520CDE8D37F8875299B1182C0E56A0A47D995117C1BE330D08B4DE86666, 2F320096233E8420996FF654C26C078472BBE2BC115FD5D4D6139E0819A58457, 225C1D3377CFF7773455E55202057E9E95C537C33016D26BB832333797277E49, F315D7D883A82CE0B007F7F2B899047B781FA2CB5B05952E146AB679C8C64717, 9A327BC3EF2E083620C9AE2E7A6363E720D8ABB5A4FC3C4EAFA91A34D1C5E2F4, 82452545022D3ACA5B5453B044F6E1A5C0837DBF340E42B1E75C047B555F9BC4,

Attack Name	TYPE	VALUE
SnakeKeylogger	SHA256	EBD92BDD8BEAFB2436B1B084EBFA7686BD53F73E305AA368D9EAA53A7C96C78F, 3D499CCCCF5F8EC92BE049BB72964B0762B5DA99FF7E0280F77284DF6E042B4E
Xworm	SHA256	C0BD1EBDF30196EFE9F0F562DCCCC143ECE619994CA14170E88F87AD402CDFFA, CD9CA4735E5100ABF0163B9E2E7F63B35CD3DC0BA791E0540E15C94A13470289, F9D7569C8A07239001E8EB6E8915D922821F53A37328C67F390D64B8D594623D, E1DE5491FBADA68CDBFF98F68ED645BF8FDF62F21CF792FCA7CC556EF2D30A9F, AC009DA131ECC35C95B484248FCD3091F607D71F26F7421699B2A8C907B1EE04, B6F7B52A5A37CDC6A4EF74557EA182E006CDDBFD81CAA55FF0154F032C643B16, FB6030901766855BD7C744C8B3718248014F53C72562191FE6BAC6468D48B476, 096E33B9B0B4F843A7EA0259F75B4370F00AB90F3807EB89D5F0117DA762900D, C39365657B596C0E0D5599D177EC383659D23D24D1E529FCF2EEEF2C8F82E5F0, B6D964C8820A2827075248FB5F78E6D108E86CED610F854B7BF79BA0511B0E6D, D2AE6FC3637DAE75AA818C5EAAE687AF4989CD9B2312D6375A182AC1E3DE8FD5, 820BB1A31F421B90EA51EFC3E71CC720C8C2784FB1E882E732E8FAFB8631A389, F79EA17E2928C9D73D8733366AB1DFFA64F3B26275219EACA2E83C2F76C96161, 87B77954F60BEA9EEBAC32548459D1024998C92B6606E6CE9CBAB0FACC746751, EEF14366A8910998A21B02BBC3180C87A110D6900897E918EE5810A0DBA6FDF0, B079DD50E4CD9788F984A1F1018984D71D03990C44FBE3089EBE0A595DA4E98A, D22FAFFE39DE72108CB34407C0F6555069AE9E5D7D0C26F839370558F44BCA9A, 70BA57FB0BF2F34B86426D21559F5F6D05C1268193904DE8E959D7B06CE964CE, C9A766B2570F5F059A4A1222AF829AA099CB7E5E47F3CC6A6DFDA9A80611E3A0, CD829068822B91CC8BA0CB929CC82FC8CA94897A87C73A154D4469983CCB7643

Attack Name	TYPE	VALUE
JsOutProx	MD5	118b6673bd06c8eb082296a7b35f8fa5, 1bd7ce64f1a7cf7dc94b912ceb9533d0, 3a2104953478d1e60927aa6def17e8e7, 3d46a462f262818cada6899634354138, 66514548cdffab50d1ea75772a08df3d, 6764dbc4df70e559b2a59e913d940d4b, 72461c94bd27e5b001265bbccc931534, 81b9e7deb17e3371d417ad94776b2a26, 89a088cd92b7ed59fd3bcc7786075130, 9c9df8fbcef8acd1a5265be5fd8fdce9, bea8cf1f983120b68204f2fa9448526e, d22f76e60a786f0c92fa20af1a1619b2, efad51e48d585b639d974fcf39f7ee07, f1858438a353d38e3e19109bf0a5e1be
FatalRAT	SHA256	8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d
Carbanak	SHA256	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
	MD5	87aa5f3f514af2b9ef28db9f092f3249
Waterbear	SHA256	e669aaf63552430c6b7c6bd158bcd1e7a11091c164eb034319e1188d43b5490c, 0da9661ed1e73a58bd1005187ad9251bcdea317ca59565753d86ccf1e56927b8, ca0423851ee2aa3013fe74666a965c2312e42d040dbfff86595eb530be3e963f, 6dcc3af7c67403eaae3d5af2f057f0bb553d56ec746ff4cb7c03311e34343ebd, ab8d60e121d6f121c250208987beb6b53d4000bc861e60b093cf5c389e8e7162, a569df3c46f3816d006a40046dae0eb1bc3f9f1d4d3799703070390e195f6dd4, e483cae34eb1e246c3dd4552b2e71614d4df53dc0bac06076442ffc7ac2e06b2, c97e8075466cf91623b1caa1747a6c5ee38c2d0341e0a3a2fa8fcf5a2e6ad3a6, 6b9a14d4d9230e038ffd9e1f5fd0d3065ff0a78b52ab338644462864740c2241
Cryptbot	SHA256	BACA9D0FDDDE0E897A98070E87D0529FB4FCD5BCD1F3584BB43281E61EE68352, 245C2379816C8AB8C0C83050DC7DA5375FC724788E6844540CF2BA537F6B727B, D80B49455C86BB748C2B4D006443E73FB107F4CDFEE298991BB526BF9A6FA464,

Attack Name	TYPE	VALUE
Cryptbot	SHA256	D4036C235FCA73A67732D884564991184B7A8EA148784F0CD70FA07ADBD8E160, B840500C7985E9A0DB4AFAF55F633A1F0FC4A1F52344791B13E14B8FAFC8FFAB, 1DDBD0850493C851AB3503B8AF24118E2F4C0441A997436D13FB5596F96178EB, E8221B90D1CCC9761383DE1DAF68F7025FE9D38A4C5BFB6EF8DE71C525D53FE9, E41202C14467AC53D72BE5754802CE73A07C605C7159D4F65E0B9CDA1E36A836, 183F842CE161E8F0CCE88D6451B59FB681AC86BD3221AB35BFD675CB42F056AC, 91A270A7E220EAD2D197732A5C0F08F1186AD7EF53BDB11749FF014AFC5FFE48, EBCD03FB51CF4AB8CD5636F1894276886E64014F3AB8C0468A9E528073931F08, 24336A3C69F863981DF13CC9C2CC8FE002D642962FC1D12C87062A8E5D273889, F4D74FDB147B02ED456DA86058C56F78708FD386EF6B893795BC44A8AFA42E9C, F667AB33B49D8B8389E116A05849032CC2E78A7578B12CDD07ED89A931C3C464, B4CAEA526BAC33E9A0F02A6CD303A5EFC557C21CB44814C096C755E4C1AF0C98, F971BC6B48B1B12ABE708F9CFA090E8A22111B689549F46B6010E30153B1467E, BDCE60E92616F204631EBAC6D57C74FD2214C9591C6FAA2A76150C6AC15C6AC0, F5525DA97ACAB586AD247CCC199D0D6FA6487F9B7F4BB66E36FAF52BE1A8D9F1, CB3B9C473954B995C70BE161F1332AAE47E1E0BDD5BE80DDFE7AF9B76CECB7A2
KageNoHitobito	SHA256	8939bfe20bc6476806d22c8edfcaba5c36f936b893b3de1c847558502654c82f, 1940fcdb2561c2f7b82f6c44d22a9906e5ffec2438d5dadfe88d1608f5f03c33, 506e8753dd5ca1c8387be32f26367e26f242b7c65e61203f7f926506c04163aa, 8a10e0dc4994268ea33baecd5e89d1e2ddabef30afa09961257a4329669e857a, bec9d2dcd9565bb245f5c8beca4db627390bcb4699dd5da192cc8aba895e0e6a

Attack Name	TYPE	VALUE
LummaC2	SHA256	65E1A8E550DF1000EB91A7B679CF586EFAB0F24385B810F50349D50EB80AE806, 5ECAFA1ECBC54D9A7B0E2E5C646578057215A246AEEC2132FE7605A078AA43EC, D0E7A341FE199DBABB5F0798DBA0564E9B60E4736A405C46EAFC7232CC10DC40, 8A80210B1F6382CDBFF2AFC0C9A30092FC13687A33F293E36A9DBC0263A45101, A90294B602B51FFF7B04E72DEEB3E88FB200272321C939F00E13BDE1D49FF1A3, 257BCB2BAC99FE5E876857EC4511CADA759E7F515DE629E43CBB0F839575E7FC, 8BFDD127054E1EE93F58148677961929BB9265BB6BA9648F517118C1DFCA6504, 78785AB759DD61F4A9FB561FAEF90234FB0A78696523D1DF53312C7A3EFF99FE, A4EA760306249B07D5AF054B5FC82D5FD9DCAB5E5CB6EAB3C8E8EB9132EBF882, 3D1D2E2B702D493DDAAD5D7DEB780EE227EB24438E68B499839A4722E212F8FB, 1BE53A1BC4D191E139AFB7C053B8F54AF43C0338FF1EEE40CD1486DFE5B787B1, D0130399FD404226AE5B90897E8E3AFFE29B7D34081EE1BF11ECB3750CA342C5, D932EE10F02EA5BB60ED867D9687A906F1B8472F01FC5543B06F9AB22059B264, E4D5B043F5C9E0894A5F4A21C93CD7347A609A900DA8F56F55A0DD84269E81F1, CE00C5433FB2481534577E90B23E61B164654AD41C5A0F14BA59735ED637E326, 4DC5588AC49FA183824AB585B69A491FD45D1D3B2B01F052ADC5062B356E7434, 984A58B77A8657D009B7867D392F320F65BB8CB72B63D9960A90F5A94721F8FB, 43D0CFCE7AB2B0C2F6F89F0FA93083F46F290047CEF0F75A0AE3A0B8742D84D8, DE6C4C3DDB3A3DDBCBEA9124F93429BF987DCD8192E0F1B4A826505429B74560, 77460056386F07D96908455241B15091C3EDECD9FD55FBF6CE7F3A061C7AC5CD
Rhadamanthys	SHA256	B9AD234ABEB1490F2C2D28DD2387F0575BA5128EBB799741B1F3179622204175, 7FAEB3F847830A2C52322565D8E73E07000003CCB54310790E10756CD3B2FF6B,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	C7CA2F9065557A6D8FB0C02C75804D386B77FFCA4466678B201C09E916AFA096, A432BF6943599E53A12D5615F91FE3D636A6820073B60A7068FA9508849806B4, 30B5B1D6877DF251F4007725DF4E043F704D80A55B4EBD7C952B4F24B7806712, 8404CB4A740D169256E49E3A22B2AF1A61B2606E71CDCA4F39DEECCD5D461C91, 138C86D9C22182DC809F2747D012D792ED391A84081E513C7C93D8786801D5F7, B579DF3A8607CB6B251EE319BDC8C1005CA3A6ED1E360EEDF2433B3F6151D856, 1D8E82D9ABDA58C9F4A0DEF2940E9F75921E2DCE89A07B337A075CA363176CD4, 4130CE135FBFAB00618F261A0397E88479D2F61E1ED0D09EBCDE525439774F3E, CC830FF08B6C66FB562A8E90C9512CADD6DBE715EB31D09E7D6AFCC0E9FBEE68, 70DEBCE3A545CACCA8B0BDB6008945852084B36E9160424FB63479C2991DCADE, A4B6A1619CF4FF65770BE120CC415DE1E8897C2378610171F3C48FF0FA38E9FE, 00DD5C97E86646DF73973BA24085EBB32DB19DE258F37ED50B5C333087BB6B5C, DF65E93CDDF79B31B474F39477AA3038CB666965311676096D9E02A5B5CF7523, 233A2666A23AB1BAE19296EE7F66CE3CDF6284DB1CA4CAAEB121530126419B42, D5B6CFE15A5BF959152889D8FF4FC220F0C055327C57A83C4877316AF50D3A4D, F62527A0F56252621A8C7C18E0F5131BB53B4A5312DBA42B4188B52345CC94A2, F9D387135A7A4E49EB96FC29D3DA8F412D870417BF684B5E8AE91C4A1FBCC6D5, DF66FE18BA387CAA8CB295C5F35BB0A8D208DDADEA7A05CEF77090CC09A681B1
GooseEgg	SHA256	c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5, 6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f
DoNex	SHA256	0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca, 6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40, b32ae94b32bcc5724d706421f915b7f7730c4fb20b04f5ab0ca830dc88dcce4e

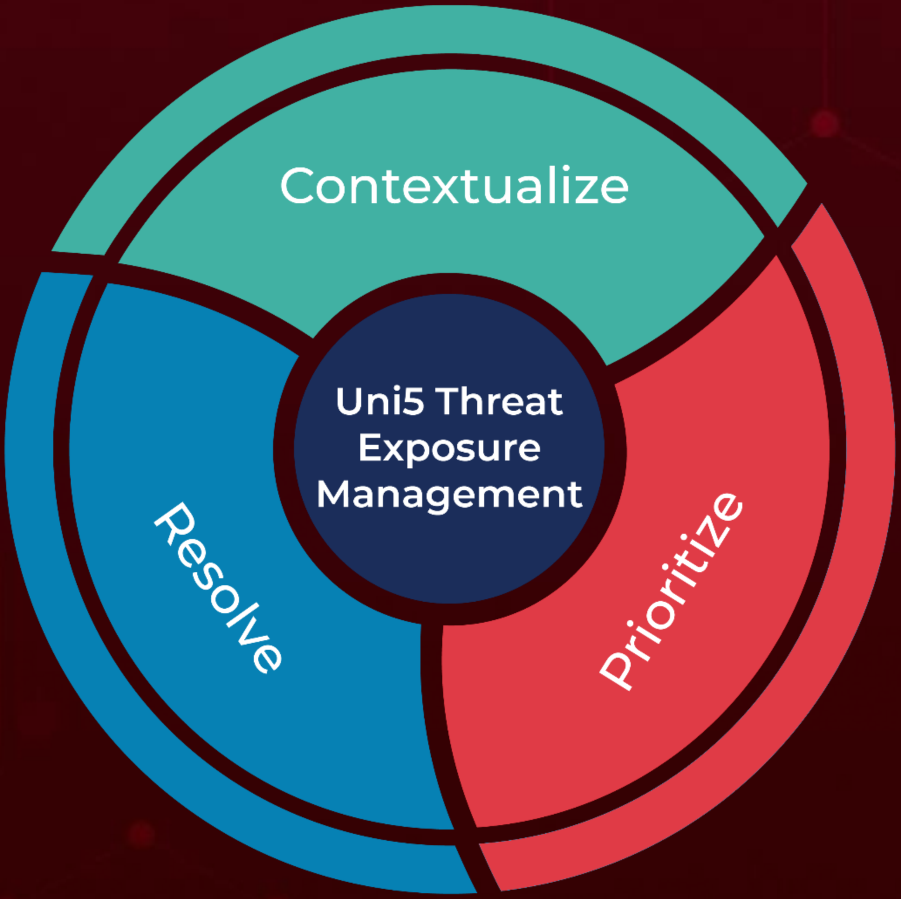
Attack Name	TYPE	VALUE
Akira Ransomware		d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386, aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9, 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4, 36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c, 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75, 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c, ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc, dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198, 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07, 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c, 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065, 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83, 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be, 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a, 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d, C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0, aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d, 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88, 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32,

Attack Name	TYPE	VALUE
Akira Ransomware		8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694, 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0, 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43, 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5, 5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2, 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562, 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84, fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64, e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1, 3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4,
	MD5	7a647af3c112ad805296a22b2a276e7c

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

May 2, 2024 • 6:30 AM

More at www.hivepro.com