

Date of Publication
August 1, 2024



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JULY 2024

Table Of Contents

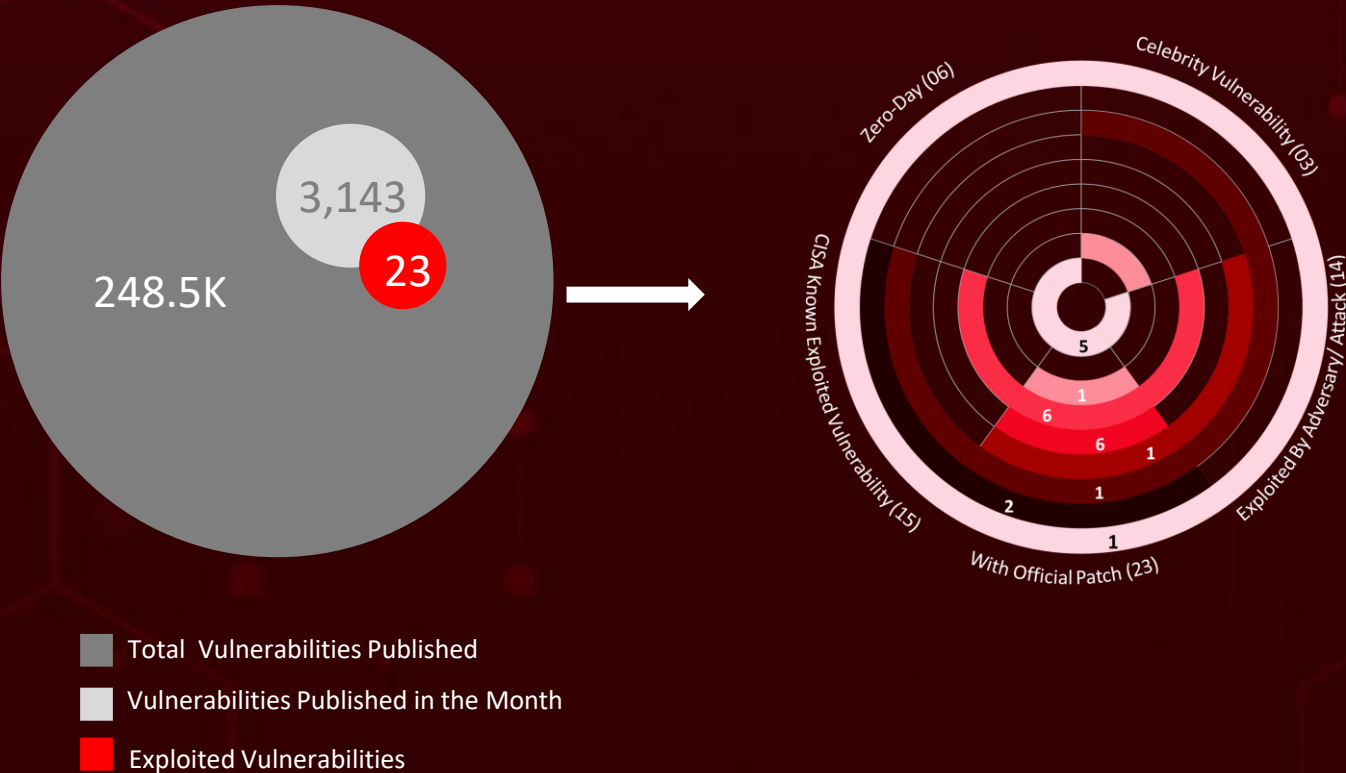
<u>Summary.....</u>	03
<u>Insights.....</u>	04
<u>Threat Landscape.....</u>	05
<u>Celebrity Vulnerabilities</u>	06
<u>Vulnerabilities Summary.....</u>	09
<u>Attacks Summary.....</u>	11
<u>Adversaries Summary.....</u>	14
<u>Targeted Products.....</u>	16
<u>Targeted Countries.....</u>	18
<u>Targeted Industries.....</u>	19
<u>Top MITRE ATT&CK TTPs.....</u>	20
<u>Top Indicators of Compromise (IOCs).....</u>	21
<u>Vulnerabilities Exploited.....</u>	24
<u>Attacks Executed.....</u>	38
<u>Adversaries in Action.....</u>	52
<u>MITRE ATT&CK TTPS.....</u>	63
<u>Top 5 Takeaways.....</u>	67
<u>Recommendations.....</u>	68
<u>Hive Pro Threat Advisories.....</u>	69
<u>Appendix.....</u>	70
<u>Indicators of Compromise (IoCs).....</u>	71
<u>What Next?.....</u>	78

Summary

In July, the cybersecurity arena garnered significant attention following the identification of six zero-day vulnerabilities. Additionally, a supply chain attack impacted 100,000 web services globally due to a **polyfill** flaw. Two critical regression vulnerabilities, **regreSSHion** with OpenSSH and **CVE-2024-41110** with Docker Engine, were reported; these vulnerabilities had been fixed earlier, but the fixes were not carried forward to subsequent versions. Later in the month, critical flaws were discovered in **ServiceNow**, which were exploited to allow unauthorized users to execute code remotely. These flaws are being exploited as part of a broader global reconnaissance campaign targeting various sectors, including finance, healthcare, and technology.

During this same timeframe, there was a marked increase in ransomware attacks, with variants such as **Eldorado ransomware**, **EstateRansomware**, **ShadowRoot Ransomware**, **Play ransomware** aggressively targeting victims. As ransomware tactics become increasingly sophisticated, it is imperative for organizations to bolster their defenses by implementing comprehensive backup and disaster recovery strategies. Furthermore, training employees to detect and prevent phishing attacks remains essential.

Concurrently, **eleven** threat actors were engaged in various campaigns. **Void Banshee**, APT group, has been targeting North America, Europe, and Southeast Asia's Education sector by exploiting the **CVE-2024-38112**, and deploying the **Atlantida stealer** for information theft and financial gains. Additionally, a newly emerged cyber threat actor, **CRYSTALRAY** uses advanced tools and tactics to steal credentials and deploy cryptocurrency miners.



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

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

CVE-2024-21412 flaw in Microsoft SmartScreen leveraged to deploy Lumma and Meduza Stealer, to collect sensitive information

Polyfill.io Supply Chain Attack
Impacts 100,000 Websites, Redirecting Users to Malicious Sites

EvilVideo Flaw
a serious threat to Telegram users, potentially compromising their security and privacy

Play ransomware
has introduced a Linux variant that specifically targets VMware ESXi environments

CVE-2024-38112
a Windows MSHTML flaw exploited by Void Banshee to deploy the Atlantida stealer, which is used for information theft and financial gain

MuddyWater
has expanded its arsenal with BugSleep malware, a backdoor that is continuously being developed and enhanced

regreSSHion

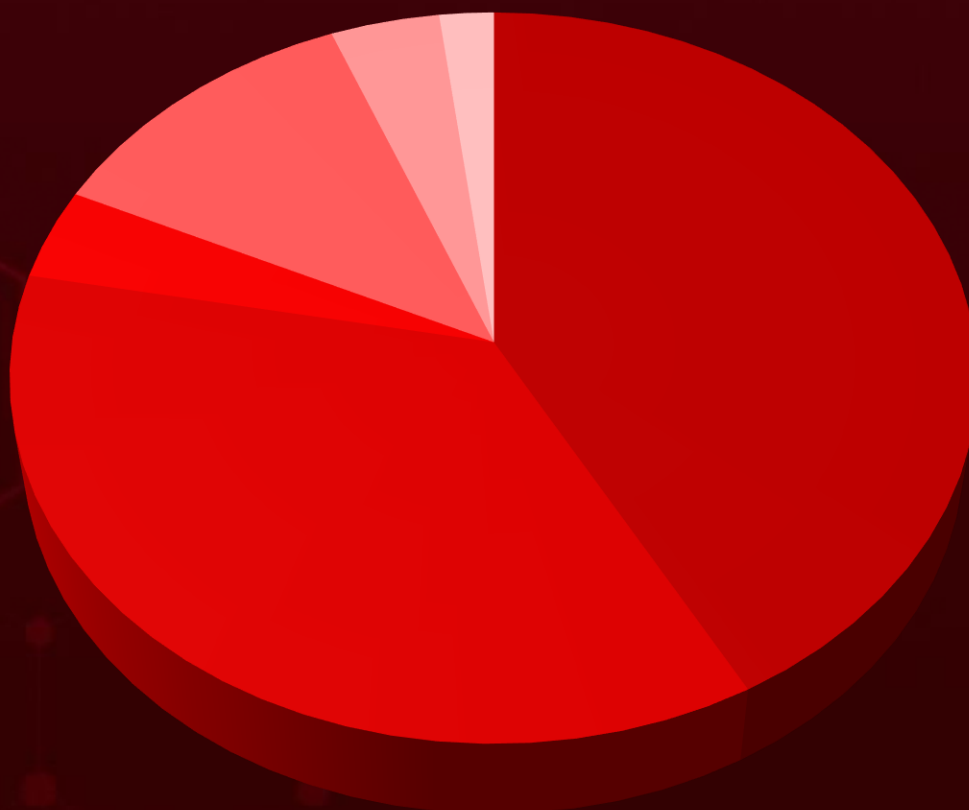
Flaw in OpenSSH, allows RCE with root privileges on glibc-based Linux systems

MerkSpy

A spyware clandestinely monitors and harvest data from victim's system leveraging Microsoft MSHTML flaw



Threat Landscape





- Malware Attacks
- Supply Chain Attacks
- Password Attack
- Social Engineering
- Injection Attacks
- Denial-of-Service Attack



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-6387</u>		OpenSSH versions earlier than 4.4p1 OpenSSH versions from 8.5p1 to before 9.8p1	-
	CISA KEY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:openssh:openssh:*:*:*:*:*:*:*	-
regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-364	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.openssh.com/ftp.html https://www.openssh.com/releasenotes.html !


































CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-34102</u>		Adobe Commerce and Magento Open Source	-
	CISA KEY		
			AFFECTED CPE
NAME			-
CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-611	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter T1606: Forge Web Credentials	https://experienceleague.adobe.com/en/docs/commerce-operations/release/notes/security-patches/2-4-7-patches , https://experienceleague.adobe.com/en/docs/commerce-operations/upgrade-guide/modules/upgrade

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>		Apache Log4j2	Andariel
	CISA KEV		
NAME		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)		cpe:2.3:a:apache:log4j:*:*:*:*:*:*	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware
		CWE ID	ASSOCIATED TTPs
	CWE-917	T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-20399	Cisco NX-OS Software CLI Command Injection Vulnerability	Cisco NX-OS Software			
CVE-2024-6387	regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)	OpenSSH server			
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Microsoft MSHTML			
CVE-2017-3506	Oracle WebLogic Server OS Command Injection Vulnerability	Oracle WebLogic Server			
CVE-2023-21839	Oracle WebLogic Server Unauthenticated RCE Vulnerability	Oracle WebLogic Server			
CVE-2023-2071	FactoryTalk View Machine Edition Remote Code Execution Vulnerability	FactoryTalk View Machine Edition			
CVE-2023-29464	FactoryTalk Linx Denial-of-Service and Information Disclosure Vulnerability	FactoryTalk Linx			
CVE-2024-21412	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows Internet Shortcut Files			
CVE-2024-5441	WordPress Modern Events Calendar Plugin Arbitrary File Upload Vulnerability	Modern Events Calendar, Modern Events Calendar Lite			
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V			
CVE-2024-38112	Windows MSHTML Platform Spoofing Vulnerability	Windows MSHTML			
CVE-2022-44877	CWP Control Web Panel OS Command Injection Vulnerability	CWP Control Web Panel			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2021-3129	Laravel Ignition File Upload Vulnerability	Laravel Ignition			
CVE-2019-18394	Ignite Realtime Openfire Server-Side Request Forgery (SSRF) vulnerability	Ignite Realtime Openfire through 4.4.2			
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication			
CVE-2024-36401	OSGeo GeoServer GeoTools Eval Injection Vulnerability	GeoServer			
CVE-2024-34102	CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)	Adobe Commerce and Magento Open Source			
CVE-2024-36991	Splunk Enterprise Path Traversal Vulnerability	Splunk Enterprise			
CVE-2024-41110	Docker Engine AuthZ Plugin Bypass Vulnerability	Docker Engine			
CVE-2024-4879	ServiceNow UI Macros Jelly Template Injection Vulnerability	ServiceNow UI Macros			
CVE-2024-5178	ServiceNow SecurelyAccess API Input Validation Vulnerability	ServiceNow SecurelyAccess API			
CVE-2024-5217	ServiceNow GlideExpression Script Input Validation Vulnerability	ServiceNow GlideExpression			
CVE-2021-44228	Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2			

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
dllFake	Information Stealer	-	Notezilla, Copywhiz, and RecentX	-	Trojanized software products
MerkSpy	Spyware	CVE-2021- 40444	Microsoft Windows		Exploiting Vulnerability
WINELOADER	Backdoor	-	-	-	Spear Phishing
RootSaw	Dropper	-	-	-	Spear Phishing
VaporRage	Downloader	-	-	-	Spear Phishing
XMRig	Cryptominer	CVE-2017-3506 CVE-2023-21839	Oracle WebLogic Server		Exploiting vulnerabilities
PureCrypter	Downloader	CVE-2017-3506 CVE-2023-21839	Oracle WebLogic Server		Exploiting vulnerabilities
Nim Downloader	Downloader	-	-	-	Social Engineering
Donut	Framework	-	-	-	Social Engineering
Silver	Trojan	-	-	-	Social Engineering
Mekotio	Banking Trojan	-	-	-	Social Engineering
Eldorado ransomware	Ransomware	-	-	-	-
Lumma	Stealer	CVE-2024-21412	Microsoft Windows Internet Shortcut Files		Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Meduza Stealer	Stealer	CVE-2024-21412	Microsoft Windows Internet Shortcut Files		Exploiting Vulnerabilities
ViperSoftX	Stealer	-	-	-	Pirated software and torrents
Kematian	Stealer	-	-	-	Phishing
EstateRansomware	Ransomware	CVE-2023-27532	Veeam Backup & Replication		Abusing Fortinet VPN Service
BugSleep Backdoor	Backdoor	-	-	-	Phishing
ShadowRoot Ransomware	Ransomware	-	-	-	Social Engineering
Atlantida Stealer	Stealer	CVE-2024-38112	Windows MSHTML		Exploiting Vulnerabilities
9002 RAT	RAT	-	-	-	Phishing
Jellyfish	Loader	-	-	-	Phishing
Play ransomware	Ransomware	-	-	-	Valid credentials or Phishing
Coroxy	Backdoor	-	-	-	Dropped via other malware
Braodo	Information Stealer	-	-	-	Spear Phishing
Demodex Rootkit	Rootkit	-	-	-	Exploiting zero-day vulnerabilities in Internet-facing applications or Spear phishing campaigns

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Rhadamanthys	Stealer	-	-	-	Phishing
RisePro	Stealer	-	-	-	Phishing
RedLine	Stealer	-	-	-	Phishing






Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Velvet Ant	Information Theft, Espionage	China	CVE-2024-20399	-	Cisco NX-OS Software
APT29	Espionage and Information theft	Russia	-	WINELOADER, RootSaw, VaporRage	-
8220 Gang	Financial Gain	China	CVE-2017-3506 CVE-2023- 21839	XMRig Cryptominer, PureCrypter loader	Oracle WebLogic Server
CloudSorcerer	Information theft and espionage	-	-	-	-
CRYSTALRAY	Information theft and espionage	-	CVE-2022-44877 CVE-2021-3129 CVE-2019-18394	-	CWP Control Web Panel, Laravel Ignition, Ignite Realtime Openfire
MuddyWater	Information theft and espionage	Iran	-	BugSleep Backdoor	-
Void Banshee	Information Theft & Financial Gainer	-	CVE-2024-38112	Atlantida Stealer	Windows MSHTML
APT17	Information theft and espionage	China	-	9002 RAT	-
GhostEmperor	Information Theft, Espionage	China	-	Demodex Rootkit	-
Stargazer Goblin	Information theft, Financial gain	-	-	Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine	-

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Andariel	Espionage and Information theft, Financial gain	North Korea	CVE-2021-44228	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Prefit, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimos2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware	Apache Log4j2



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Network OS	Cisco NX-OS Software MDS 9000 Series Multilayer Switches Nexus 3000 Series Switches Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Switches in standalone NX-OS mode
	Software	OpenSSH versions earlier than 4.4p1 OpenSSH versions from 8.5p1 to before 9.8p1
 Microsoft	Operating system	Windows: 8.1 - 10 S Windows Server: 2008 - 2019 2004 Microsoft Internet Explorer: 11
	Operating system	Windows Server: before 2022 10.0.20348.2582 Windows: before 11 23H2 10.0.22631.3880
	Browser Engine	Windows MSHTML
	Web Browser	Microsoft Internet Explorer: 11 - 11.1790.17763.0 Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582
	Web Server	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2
	OT Software	FactoryTalk View Machine Edition: 12.0 - 13.0
		FactoryTalk Linx: 6.20

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Web Framework	WordPress Modern Events Calendar, Modern Events Calendar Lite
	Administration Tool	CWP Control Web Panel
	Web Framework	Laravel Ignition
	Messaging Application	Ignite Realtime Openfire through 4.4.2
	Backup Software	Veeam Backup & Replication
	Server	OSGeo GeoServer
	eCommerce platform	Adobe Commerce and Magento Open Source
	SIEM	Splunk Enterprise Versions 9.2.0 to 9.2.1, 9.1.0 to 9.1.4, 9.0.0 to 9.0.9
	Container	Docker Engine
	Software	ServiceNow Now Platform
	Web Server	Apache Log4j2

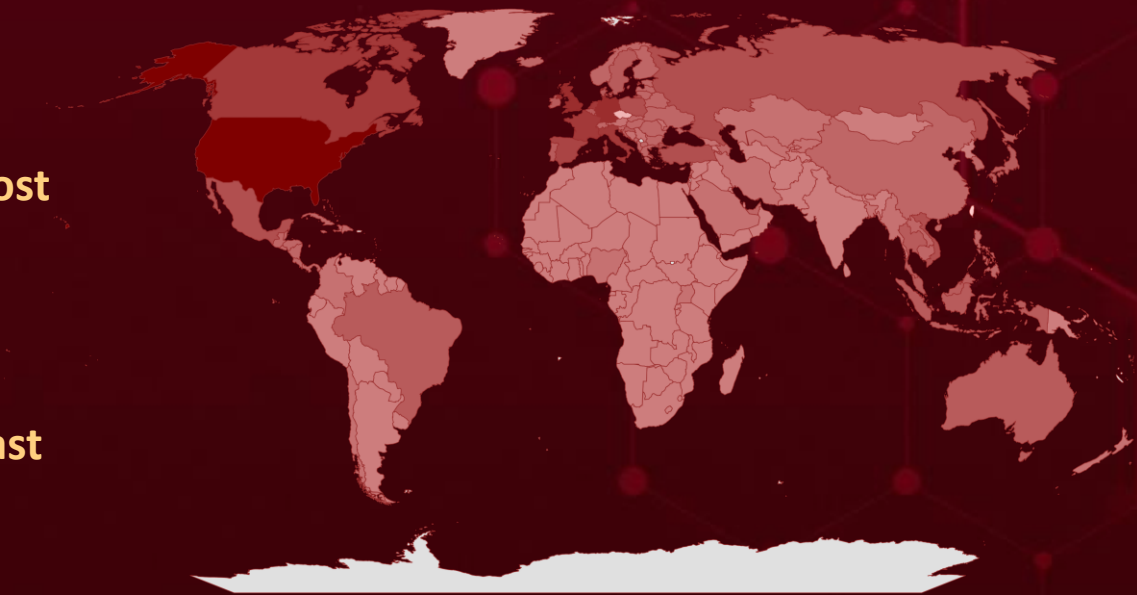


Targeted Countries

Most



Least



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

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	United States		Australia		Albania		Laos		Liechtenstein
	Germany		Brazil		Belarus		United Arab Emirates		Austria
	United Kingdom		Luxembourg		Israel		New Zealand		Malta
	Netherlands		Japan		Norway		Uganda		Moldova
	France		Indonesia		Brunei		Saudi Arabia		Nigeria
	Canada		Slovakia		Philippines		Georgia		Seychelles
	Italy		Panama		Jamaica		Monaco		Jersey
	Singapore		Finland		Cuba		Andorra		Eritrea
	Spain		Grenada		Bulgaria		Czech Republic (Czechia)		Kenya
	Russia		Romania		Barbados		Bangladesh		Bolivia
	Poland		Guatemala		Latvia		Bosnia and Herzegovina		Kiribati
	Vietnam		El Salvador		Dominica		Iran		South Sudan
	Mexico		Haiti		Lithuania		Uzbekistan		Kuwait
	Turkey		Greece		Slovenia		Chile		Eswatini
	Malaysia		Honduras		Cambodia		Myanmar		Guadeloupe
	Sweden		Bahamas		Dominican Republic		Kazakhstan		Yemen
	Portugal		Hungary		Azerbaijan		Cyprus		Abkhazia
	Ireland		Saint Lucia		Switzerland		Kyrgyzstan		Sao Tome & Principe
	Croatia		Iceland		China		San Marino		Guernsey
	Denmark		South Korea		Trinidad and Tobago		Colombia		Solomon Islands
	Belgium		Belize		Montenegro		Serbia		Guinea
	Thailand		Estonia		Ukraine		Timor-Leste		State of Palestine
					Costa Rica				
					Nicaragua				

Targeted Industries

Most



Government



Transportation



Education



Healthcare



Financial



Tele-communications



Media



Aerospace



Pharmaceutical



Technology



Business Services



Energy



Legal



Defence



Real Estate



Professional Services



Retail



Manufacturing



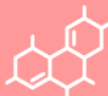
Agriculture



Construction



Logistics



Biotechnology



Critical Infrastructure



Utilities



Banking



Chemical



Travel



Think-Tanks



NGOs



E-commerce



Engineering



Insurance

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1588

Obtain Capabilities

T1204

User Execution

T1588.00

6
Vulnerabilities

T1190

Exploit Public-Facing Application

T1566

Phishing

T1083

File and Directory Discovery

T1082

System Information Discovery

T1027

Obfuscated Files or Information

T1071

Application Layer Protocol

T1041

Exfiltration Over C2 Channel

T1204.00

2
Malicious File

T1036

Masquerading

T1053

Scheduled Task/Job

T1059.00

1
PowerShell

T1068

Exploitation for Privilege Escalation

T1005

Data from Local System

T1070

Indicator Removal

T1053.00

5
Scheduled Task

T1055

Process Injection

T1566.00

2
Spearphishing Link

T1203

Exploitation for Client Execution

T1555

Credentials from Password Stores

T1562

Impair Defenses

T1057

Process Discovery



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>MerkSpy</u>	SHA256	92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08, 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a, 0ffadb53f9624950dea0e07fcffcc31404299230735746ca43d4db05e4d708c6, dd369262074466ce937b52c0acd75abad112e395f353072ae11e3e888ac132a8, 569f6cd88806d9db9e92a579dea7a9241352d900f53ff7fe241b0006ba3f0e22, 6cdc2355cf07a240e78459dd4dd32e26210e22bf5e4a15ea08a984a5d9241067
<u>PureCrypter</u>	SHA256	397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3, 5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2cd80e99, 5d649c5aa230376f1a08074aee91129b8031606856e9b4b6c6d0387f35f6629d, 7a5b8b448e7d4fa5edc94dcb66b1493adad87b62291be4ddcbd61fb4f25346a8, a7c006a79a6ded6b1cb39a71183123dcaaaa21ea2684a8f199f27e16fcb30e8e, be18d4fc15b51daedc3165112dad779e17389793fe0515d62bbcf00def2c3c2d, c846e7bbbc1f65452bdca87523edf0fd1a58cbd9a45e622e29d480d8d80ac331, efc0b3bfcec19ef704697bf0c4fd4f1cfb091dbfee9c7bf456fac02bcffcfe df, f950d207d33507345beeb3605c4e0adfa6b274e67f59db10bd08b91c96e8f5ad
	MD5	0d8b1ad53fddacf2221409c1c1f3fd70, 0ede257a56a6b1fbd2b1405568b44015, 14e4bfe2b41a8cf4b3ab724400629214, 17f512e1a9f5e35ce5761dba6ccb09cb, 18e9cd6b282d626e47c2074783a2fa78, 1d3c8ca9c0d2d70c656f41f0ac0fe818, 2499343e00b0855882284e37bf0fa327, 2964ce62d3c776ba7cb68a48d6afb06e, 2fa290d07b56bde282073b955eae573e, 3f92847d032f4986026992893acf271e, 5420dcbae4f1fba8afe85cb03dcd9bfc, 61259b55b8912888e90f516ca08dc514,




Attack Name	TYPE	VALUE
<u>PureCrypter</u>	MD5	71b4db69df677a2acd60896e11237146, 754920678bc60dabeb7c96bfb88273de, 765f09987f0ea9a3797c82a1c3fced46, 785bfaa6322450f1c7fe7f0bf260772d, 8503b56d9585b8c9e6333bb22c610b54, 8ef7d7ec24fb7f6b994006e9f339d9af, a478540cda34b75688c4c6da4babf973, ae158d61bed131bcfd7d6cecdccde79b, b4fd2d06ac3ea18077848c9e96a25142, b5c60625612fe650be3dcbe558db1bbc, b6c849fcdcdca6c6d8367f159047d26c4, bbd003bc5c9d50211645b028833bbeb2 c3b90a10922eef6d635c6c786f29a5d0, c9ca95c2a07339edb13784c72f876a60, d70bb6e2f03e5f456103b9d6e2dc2ee7, dbcaa05d5ca47ff8c893f47ad9131b29, de94d596cac180d348a4acdeeeaaa9439, eaaf20fdc4a07418b0c8e85a2e3c9b27, f1c29ba01377c35e6f920f0aa626eaf5, f34d5f2d4577ed6d9ceec516c1f5a744, f4eebe921b734d563e539752be05931d, fa4ffa1f263f5fc67309569975611640, fdd4cd11d278dab26c2c8551e006c4ed
<u>XMRig</u>	SHA256	f4d1b970bc9e5d319c5432be9e3863b5a20bf26e557c8cea6f3949d f0012cf01, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c 7d4f7b912b, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b 66a2d7d3e, f34fc824a6c655bd6320b7818acdad9a5a570b88dd46507fdf73cd2 54af9b19f, 621a9f892436647a492e3877502454d1783dc0cf4e4ba9f3f459a8c 2ac7e6d97, f63921129822475dd132a116b11312ebbb0cdc8b54f188aabeb7cf7 a8c9065fd, 05e1988f56fe199f7e401c8f4d6ee50bb26ab34fb3f96c22de959c7e 5f92de77, d0cf7388253342f43f9b04da27f3da9ee18614539efdc2d9c4a0239a f51ddbe4, 09ec3bf64600d1fedbd11bb3ebb705a0f541d1310f5f8690de70d37 648fcd4b4
<u>Eldorado Ransomware</u>	SHA256	1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0a b9f27b, 7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122 ae66dd, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d967 36174a7,




Attack Name	TYPE	VALUE
<u>Eldorado Ransomware</u>	SHA256	b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de, dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33, 8badf1274da7c2bd1416e2ff8c384348fc42e7d1600bf826c9ad695fb5192c74, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7
	MD5	9d1fd92ea00c6eef88076dd55cad611e, 315a9d36ed86894269e0126b649fb3d6
	TOR Address	hxxp[:]//dataleakypypu7uwbIm5kttv726l3iripago6p336xjnbstkjwrlnli d[.]onion
	Email	russoschwartz[at]onionmail[.]org
	IPv4	173[.]44[.]141[.]152
<u>ViperSoftX</u>	SHA256	814297c47c67c82c4700ed0f099d558b8ac45e91cbb72d44a46c2e2a0c6b11aa, fef939b4a90ee28e2cffe1d8f0dcfc0d5dd174b0321e2a2c6cd46c65b7b79a2d, 779323771d4ebd97de44bdb9cb03e40156182b2012acfd444a4787902b0f1f35, 4d1ef869c4bddeccc318939ea2651ce5a3fc2e369ba44a2e24cb9b102ef2be19, d55aaa430ea18f3b85ccbfe2f34ce14b9b88d348d83e6c41d3aaea456b69b869
<u>EstateRansom ware</u>	SHA1	cb704d2e8df80fd3500a5b817966dc262d80ddb8, 2c56e9beea9f0801e0110a7dc5549b4fa0661362, 5e460a517f0579b831b09ec99ef158ac0dd3d4fa, 107ec3a7ed7ad908774ad18e3e03d4b999d4690c
<u>Atlantida Stealer</u>	SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750, 2b6c8aa2ac917d978dfec53cef70eaca36764a93d01d93786cc0d84da47ce8e6, 385ebe3d5bd22b6a5ae6314f33a7fa6aa24814005284c79edaa5bdcf98e28492, 2ebf051f6a61fa825c684f1d640bfb3bd79add0afc6f698660f83f22e6544cba, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1e4cdab0
	IPv4	185[.]172[.]128[.]95
<u>Play Ransomware</u>	SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30
	IPv4	108[.]61[.]142[.]190 , 45[.]76[.]165[.]129, 149[.]248[.]2[.]42
	URL	hxxp[:]//108[.]61[.]142[.]190/FX300[.]rar, hxxp[:]//108[.]61[.]142[.]190/1[.]dll[.]sa, hxxp[:]//108[.]61[.]142[.]190/64[.]zip, hxxp[:]//108[.]61[.]142[.]190/winrar-x64-611[.]exe, hxxp[:]//108[.]61[.]142[.]190/PsExec[.]exe, hxxp[:]//108[.]61[.]142[.]190/host1[.]sa









Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-20399</u>		MDS 9000 Series Multilayer Switches, Nexus 3000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode	Velvet Ant
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:h:cisco:nx-os:*:*:*:*:*:*	-
Cisco NX-OS Software CLI Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1059.008: Network Device CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-6387</u>		OpenSSH versions earlier than 4.4p1 OpenSSH versions from 8.5p1 to before 9.8p1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openssh:openssh:*:*:*:*:*	-
regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-364	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.openssh.com/ftp.html https://www.openssh.com/releases.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-40444</u>		Windows: 8.1 - 10 S Windows Server: 2008 - 2019 2004 Microsoft Internet Explorer: 11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10-*:*:*:*:* cpe:2.3:o:microsoft:windows_server-*:*:*:*:*	MerkSpy
Microsoft MSHTML Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter, T1059.003: Windows Command, T1203: Exploitation for Client Execution, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-3506</u>		Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	8220 Gang (aka Water Sigbin)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:weblogic_server:-:*:*:*:*:*	XMRig Cryptominer, PureCrypter loader
Oracle WebLogic Server OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190 Exploit Public-Facing Application	https://www.oracle.com/security-alerts/cpuapr2017.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-21839</u>		Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	8220 Gang (aka Water Sigbin)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:weblogic_server:-:*:*:*:*:*	XMRig Cryptominer, PureCrypter loader
Oracle WebLogic Server Unauthenticated RCE Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter, T1190 Exploit Public-Facing Application	https://www.oracle.com/security-alerts/cpujan2023.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-2071</u>		FactoryTalk View Machine Edition: 12.0 - 13.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:rockwellautomation:factorytalk_view:*:*:*:*:machine:*:*:*:cpe:2.3:h:rockwellautomation:panelview_plus:-:*:*:*:*:*:*	-
FactoryTalk View Machine Edition Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter T1129: Shared Modules	https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1645%20.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-29464</u>		FactoryTalk Linx: 6.20	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:rockwellautomation:factorytalk_linx:6.20:*:*:*:*:*:*	-
FactoryTalk Linx Denial-of-Service and Information Disclosure Vulnerability		cpe:2.3:a:rockwellautomation:factorytalk_linx:6.30:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1498: Network Denial of Service	https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1652.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-21412</u>		Microsoft Windows Internet Shortcut Files	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:arm64:* cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:x64:* cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:x86:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	Lumma and Meduza Stealer
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204: User Execution T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-5441</u>		Modern Events Calendar, Modern Events Calendar Lite	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:modern_events_calendar_plugin:modern_events_calendar_plugin:*:*:*:*:*:*	-
WordPress Modern Events Calendar Plugin Arbitrary File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://webnus.net/modern-events-calendar/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38080</u>		Windows Server: before 2022 10.0.20348.2582 Windows: before 11 23H2 10.0.22631.3880	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:wind ows:*.~*~*~*~*~*~*~*~*~*	-
Windows Hyper- V Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:wind ows_server:*.~*~*~*~*~*~*~*~*~*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38112</u>		Microsoft Internet Explorer: 11 - 11.1790.17763.0 Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:inter net_explorer:- ~*~*~*~*~*~*~*~*~*	-
Windows MSHTML Platform Spoofing Vulnerability		cpe:2.3:o:microsoft:wind ows:*.~*~*~*~*~*~*~*~*~*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-668	T1204: User Execution T1204.002: Malicious File	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-44877</u>		CWP Control Web Panel	CRYSTALRAY
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:centoswebpanel:centos_web_panel:*:*:*:*:*:*	-
CWP Control Web Panel OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application T1059.004: Unix Shell	CWP users are advised to update their versions to 0.9.8.1147 or higher.




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-3129</u>		Laravel Ignition	CRYSTALRAY
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:facade:ignition:*:*:*:*:*:*	-
Laravel Ignition File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/master/cves/2021/CVE-2021-3129.yaml




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-18394</u>		Ignite Realtime Openfire through 4.4.2	CRYSTALRAY
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*	-
Ignite Realtime Openfire Server-Side Request Forgery (SSRF) vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application T1590: Gather Victim Network Information	https://github.com/igniterealtime/Openfire/pull/1497




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-27532</u>		Veeam Backup & Replication	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_&_replication:*:*:*:*:*:*	EstateRansomware
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1212: Exploitation for Credential Access	https://www.veeam.com/kb4424




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38112</u>		Windows MSHTML	Void Banshee
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*	Atlantida Stealer
Microsoft Windows MSHTML Platform Spoofing Vulnerability		cpe:2.3:o:microsoft:windows:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	
	CWE-668	T1204: User Execution T1218: System Binary Proxy Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-36401</u>		GeoServer	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:geoserver:geoserver:*:*:*:*:*	-
OSGeo GeoServer GeoTools Eval Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	
	CWE-95	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv , https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-34102</u>		Adobe Commerce and Magento Open Source	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:*:*:*:*:* cpe:2.3:a:adobe:magento:*:*:open_source:*:*:* cpe:2.3:a:adobe:commerce_webhooks:*:*:*:*:*:*:*	-
CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)		ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter T1606: Forge Web Credentials	https://experienceleague.adobe.com/en/docs/commerce-operations/release-notes/security-patches/2-4-7-patches , https://experienceleague.adobe.com/en/docs/commerce-operations/upgrade-guide/modules/upgrade




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-36991</u>		Splunk Enterprise Versions 9.2.0 to 9.2.1, 9.1.0 to 9.1.4, 9.0.0 to 9.0.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:splunk:splunk:*:*:*:*: enterprise:*:*:*	-
Splunk Enterprise Path Traversal Vulnerability		cpe:2.3:o:microsoft:windows:- :*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	
	CWE-35	T1083: File and Directory Discovery	https://docs.splunk.com/Documentation/Splunk/9.2.2/ReleaseNotes/MeetSplunk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-41110</u>		Docker Engine: Versions Prior to and v19.03.15, Versions Prior to and v20.10.27, Versions Prior to and v23.0.14, Versions Prior to and v24.0.9, Versions Prior to and v25.0.5, Versions Prior to and v26.0.2, Versions Prior to and v26.1.4, Versions Prior to and v27.0.3, Versions Prior to and v27.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RAN SOMWARE
NAME	CISA KEY	cpe:2.3:a:docker:docker_engine:*:*:*:*:*	-
Docker Engine AuthZ Plugin Bypass Vulnerability			
	CWE ID		PATCH LINKS
	CWE-187 CWE-444 CWE-863	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities	https://github.com/docker/compose/releases/tag/v2.29.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4879</u>		ServiceNow Now Platform	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	-
ServiceNow UI Macros Jelly Template Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1287	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-5178</u>		ServiceNow Now Platform	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	-
ServiceNow SecurelyAccess API Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1588: Obtain Capabilities, T1083: File and Directory Discovery	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648312

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-5217</u>		ServiceNow Now Platform	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:servicenow:service now:*.~.*.*.*.*.*.*	-
ServiceNow GlideExpression Script Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1059: Command and Scripting Interpreter, T1588: Obtain Capabilities	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
<u>CVE-2021-44228</u>		Apache Log4j2	Andariel	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*.*.*:*.~*~*~*~*	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware	
Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)				
	CWE ID		ASSOCIATED TTPs	PATCH LINK
	CWE-917		T1059: Command and Scripting Interpreter	https://logging.apache.org/log4j/2.x/security.html

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
dllFake	The dllFake information-stealing malware, which has been circulating since at least January 2024, can steal browser credentials and cryptocurrency wallet information, log clipboard contents and keystrokes, and download and execute additional payloads on infected Windows hosts.	Trojanized software products	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Information Theft, Resource Hijacking	Notezilla, Copywhiz, and RecentX
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MerkSpy	MerkSpy is a surveillance spyware designed to covertly monitor and collect information from a victim's computer without their knowledge or consent. It can record activities such as keystrokes, browsing behavior, and personal information, often transmitting this data to a third party for espionage or theft.	Exploiting Vulnerability	CVE-2021-40444
TYPE		IMPACT	AFFECTED PRODUCTS
Spyware		Information Theft, Compromise Infrastructure	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444

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
<u>WINELOADER</u>	The new modular backdoor WINELOADER features a modular design, where encrypted modules are downloaded from the C2 server. This backdoor employs techniques such as re-encryption and zeroing out memory buffers to protect sensitive data in memory and evade memory forensics solutions.	Spear Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
APT 29			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RootSaw</u>	ROOTSAW, also known as EnvyScout, is a malicious dropper program used in the initial stage of attacks by the APT29 hacking group. Its main purpose is to install the actual malicious payload, such as WINELOADER, which allows attackers remote access.	Spear Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Dropper			PATCH LINK
ASSOCIATED ACTOR			-
APT 29			

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
<u>VaporRage</u>	VaporRage, a downloader malware by the APT29 group. VaporRage is designed to download, decode, and execute an arbitrary payload fully in memory. Its deployment patterns, including staging payloads on compromised websites, make it challenging for traditional forensic investigations.	Spear Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			
APT 29			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>XMRig</u>	XMRig is a widely-used form of malware designed to mine cryptocurrencies like Monero. It covertly harnesses the computing power of infected systems for unauthorized mining activities.	Exploiting vulnerabilities	CVE-2017-3506 CVE-2023-21839
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage, Resource Hijacking, Financial Loss	Oracle WebLogic Server
Cryptominer			PATCH LINKS
ASSOCIATED ACTOR			
8220 Gang			https://www.oracle.com/security-alerts/cpuapr2017.html https://www.oracle.com/security-alerts/cpujan2023.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PureCrypter</u> TYPE Downloader ASSOCIATED ACTOR 8220 Gang	PureCrypter is an advanced loader that has been marketed since at least March 2021. This malware is known for distributing various remote access trojans and information stealers. The loader, implemented as a .NET executable, uses SmartAssembly for obfuscation and other obfuscation techniques to evade antivirus detection.	Exploiting vulnerabilities	CVE-2017-3506 CVE-2023-21839
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage, Resource Hijacking,	Oracle WebLogic Server
			PATCH LINKS
			https://www.oracle.com/security-alerts/cpuapr2017.html https://www.oracle.com/security-alerts/cpujan2023.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nim Downloader</u> TYPE Downloader ASSOCIATED ACTOR -	The Nim downloader is a basic utility coded in Nim, designed to retrieve second-stage malware from a staging server under the attacker's control.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
			PATCH LINK
			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Donut</u> TYPE Framework	Donut, a position-independent shellcode generation framework, is engineered to bypass security measures by manipulating functions, facilitating the deployment and execution of embedded payloads.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Silver</u> TYPE Trojan	Sliver, a freely available Golang trojan designed as a substitute for CobaltStrike, provides attackers with complete control over the victim’s machine, allowing them to leverage all of Sliver’s functionalities to carry out any desired actions.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Mekotio</u> TYPE Banking Trojan	The Mekotio banking trojan, a sophisticated malware in operation since at least 2015, predominantly targets Latin American countries to illicitly obtain sensitive information, especially banking credentials. Mekotio is linked to other notable Latin American banking malware, including Grandoreiro.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Financial Gain, and Compromise infrastructure	-
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
<u>Eldorado ransomware</u>	Eldorado, a new Golang-based ransomware, targets Windows and VMware ESXi systems, significantly impacting sectors in the U.S., including real estate, education, healthcare, and manufacturing. This ransomware employs ChaCha20 and RSA encryption to lock files while deliberately avoiding critical system files to ensure continued usability of the affected systems. Post-encryption, Eldorado self-deletes to cover its tracks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Lumma</u>	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two-factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	Exploiting Vulnerabilities	CVE-2024-21412
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	Microsoft Windows Internet Shortcut Files
ASSOCIATED ACTOR			PATCH LINK
Stargazer Goblin			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

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
<u>Meduza Stealer</u>	The Meduza Stealer malware has an objective of comprehensive data theft. It pilfers users' browsing activities, extracting a wide array of browser-related data. From critical login credentials to browsing history and curated bookmarks, no digital artifact is safe. Even crypto wallet extensions, password managers, and 2FA extensions are vulnerable, making Meduza Stealer a significant threat to users' financial and personal data.	Exploiting Vulnerabilities	CVE-2024-21412
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	Microsoft Windows Internet Shortcut Files
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ViperSoftX</u>	ViperSoftX is an information-stealing malware primarily targeting cryptocurrencies, and known for its unique technique of hiding malicious code inside log files. This multi-stage stealer exhibits sophisticated evasion capabilities, concealing small PowerShell scripts on a single line within otherwise innocent-looking large log files. ViperSoftX focuses on stealing cryptocurrencies, clipboard swapping, fingerprinting the infected machine, downloading and executing arbitrary additional payloads, and executing commands.	Pirated software and torrents	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Kematian Stealer</u>	Kematian-Stealer is a newly emerging information stealer actively developed on GitHub and disseminated as open-source software. This malware extracts sensitive information from various applications, targeting and copying data, capturing images, processing cookie files, and compressing the collected data into a ZIP file for exfiltration. It also deletes temporary files and the executed PowerShell script to minimize evidence. The builder is hosted on GitHub, allowing users to customize and deploy the malware, configure features, and input C2 server details through a web interface.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>EstateRansomware</u>	EstateRansomware is a recently surfaced ransomware strain that gains access to victims' systems by brute-forcing dormant accounts on Fortinet FortiGate VPN. Moreover, the ransomware exploits vulnerabilities in Veeam Backup software to propagate within the compromised environments.	Abusing Fortinet VPN Service	CVE-2023-27532
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	Veeam Backup & Replication
ASSOCIATED ACTOR			PATCH LINK
-			<u>https://www.veeam.com/kb4424</u>

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BugSleep Backdoor</u>	BugSleep is a backdoor designed to execute threat actors' commands and transfer files between the compromised machine and the C&C server. BugSleep supports 11 different commands. Its core functionality includes sending file content to its C&C server, writing content into files, and running commands through a command pipe.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ShadowRoot Ransomware</u>	The ShadowRoot ransomware campaign uses a downloaded payload, a Delphi binary designed to include additional components that conceal its operations and evade known cybersecurity solutions. These components culminate in executing the primary ransomware payload, “RootDesign.exe,” which methodically encrypts files on the victim’s PC and appends the “.shadowroot” extension to each compromised file.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Atlantida Stealer</u>	Atlantida stealer is an info-stealer malware targeting sensitive information from various applications, including Telegram, Steam, FileZilla, cryptocurrency wallets, and web browsers. This malware extracts stored sensitive and potentially valuable data, such as passwords and cookies, and collects files with specific extensions from the infected system's desktop. Additionally, Atlantida stealer captures the victim's screen and gathers comprehensive system information, enhancing its ability to exploit compromised systems.	Exploiting Vulnerabilities	CVE-2024-38112
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	Windows MSHTML
ASSOCIATED ACTOR			PATCH LINK
Void Banshee, Stargazer Goblin			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>9002 RAT (aka McRAT, Hydraq, HOMEUNIX)</u>	The 9002 RAT is a Remote Access Tool (RAT) commonly used by Advanced Persistent Threat (APT) groups to take control of a victim's machine. It is typically spread through zero-day exploits, such as those targeting Internet Explorer, and via email attachments. The infection process begins when a .LNK file is opened, triggering the execution of a PowerShell command.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
APT17			-

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
Jellyfish Loader	Jellyfish Loader is a .NET-based shellcode loader engineered for malicious purposes. It distinguishes itself by using asynchronous task method builders to execute code, securely gather and transmit system information, and prepare for the execution of additional malicious code delivered by the C&C server.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Information Theft, Resource Hijacking	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Play Ransomware	A new Linux variant of the Play ransomware that targets VMware ESXi environments, marking a shift from its previous focus on Windows systems. This ransomware employs advanced evasion techniques and is linked to the Prolific Puma group, enhancing its operational capabilities. It encrypts critical files and disrupts business operations by leaving ransom notes.	Valid credentials or Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Information Theft, Compromise Infrastructure, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Coroxy Backdoor</u>	<p>The Coroxy backdoor, also called SystemBC or DroxiDat, employed by Play ransomware, has been identified as making a connection to the designated IP address. This IP address further resolves to various domains that correspond to the registered domains of Prolific Puma. The backdoor executes instructions from a remote adversary, thereby compromising the integrity of the affected system.</p>	Dropped via other malware	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Compromise Infrastructure	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Braodo Stealer</u>	<p>Braodo Stealer is a Python-based malware that has been targeting users since early 2024. It spreads through phishing and spear-phishing emails, using GitHub and a Singapore-based VPS server to host and distribute its malicious code. The malware exfiltrates internet browser data through Telegram bots.</p>	Spear Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Stealing Credentials, Espionage, Identity Theft, Financial Loss	-
Information Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			

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
<u>Demodex Rootkit</u>	The Demodex rootkit, a critical component of GhostEmperor's toolkit, operates at the kernel level, making it extremely difficult to detect and remove. This sophisticated rootkit uses advanced techniques to avoid detection, including EDR evasion and a reflective loader to execute the Core-Implant.	Exploiting zero-day vulnerabilities in Internet-facing applications or Spear-phishing campaigns	-
TYPE		IMPACT	AFFECTED PRODUCTS
Rootkit		Information Theft, Financial Loss, and Compromise Infrastructure	-
ASSOCIATED ACTOR			PATCH LINK
GhostEmperor			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Rhadamanthys</u>	Rhadamanthys is an information stealer with a diverse set of modules and a multilayered design. It is sold on the black market and frequently updated, making it a persistent threat. Its multi-layer architecture allows it to evade detection and perform a range of malicious activities, such as stealing sensitive information and exfiltrating data.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Info Stealer		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
Stargazer Goblin			-


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RisePro</u>	RisePro is a stealer written in C++ that spreads through downloaders like win.privateloader. It possesses similar functionality to the stealer malware “Vidar.” RisePro targets sensitive information on infected machines and attempts to exfiltrate it in the form of logs. It can steal credit card information, passwords, personal data, and other confidential information, posing a significant threat to affected systems.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal Data	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			
Stargazer Goblin			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RedLine</u>	RedLine Stealer is a versatile malware that can be purchased either as a standalone product or on a subscription basis. It is designed to collect a wide range of information from browsers, including saved credentials, autocomplete data, and credit card details. RedLine Stealer have expanded their capabilities to include the theft of cryptocurrency.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal Data	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			
Stargazer Goblin			-

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
<div> <u>Velvet Ant</u></div>	China	All	Worldwide
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-20399	-	Cisco NX-OS Software
TTPs			
TA0042: Resource Development; TA0011: Command and Control; TA0010: Exfiltration; TA0009: Collection; TA0008: Lateral Movement; TA0007: Discovery; TA0006: Credential Access; TA0005: Defense Evasion; TA0004: Privilege Escalation; TA0003: Persistence; TA0002: Execution; TA0001: Initial Access; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1572: Protocol Tunneling; T1570: Lateral Tool Transfer; T1569: System Services; T1569.002: Service Execution; T1562.004: Disable or Modify System Firewall; T1135: Network Share Discovery; T1133: External Remote Services; T1090.001: Internal Proxy; T1087.002: Domain Account; T1083: File and Directory Discovery; T1082: System Information Discovery; T1078.003: Local Accounts; T1078.002: Domain Accounts; T1070.006: Timestamp; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1059.008: Network Device CLI; T1055: Process Injection; T1048: Exfiltration Over Alternative Protocol; T1047: Windows Management Instrumentation; T1039: Data from Network Shared Drive; T1037.004: RC Scripts; T1021.004: SSH; T1021.001: Remote Desktop Protocol; T1018: Remote System Discovery; T1016: System Network Configuration Discovery; T1003.001: LSASS Memory			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>APT 29 (aka Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, ATK7, Blue Kitsune, G0016, Midnight Blizzard, SeaDuke, TA421, UAC-0029)</u></p>	Russia	Aerospace, Defense, Education, Embassies, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Technology	Australia, Azerbaijan, Belarus, Belgium, Brazil, Canada, Chechnya, Chile, China, Cyprus, Czech, Denmark, France, Georgia, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Luxembourg, Mexico, Netherlands, New Zealand, Portugal, Russia, Singapore, Spain, South Korea, Switzerland, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO
	MOTIVE		
	Espionage and Information theft		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	WINELOADER, RootSaw, VaporRage	-


TTPs
TA0007: Discovery; TA0011: Command and Control; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1204: User Execution; T1082: System Information Discovery; T1134: Access Token Manipulation; T1057: Process Discovery; T1007: System Service Discovery; T1027: Obfuscated Files or Information; T1070.004: File Deletion; T1070: Indicator Removal; T1055.003: Thread Execution Hijacking; T1055: Process Injection; T1083: File and Directory Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1566: Phishing; T1110: Brute Force; T1110.003: Password Spraying; T1078.004: Cloud Accounts; T1528: Steal Application Access Token; T1078: Valid Accounts; T1621: Multi-Factor Authentication Request Generation; T1543.003: Windows Service; T1543: Create or Modify System Process; T1012: Query Registry; T1098.005: Device Registration; T1098: Account Manipulation; T1651: Cloud Administration Command; T1059.009: Cloud API; T1059: Command and Scripting Interpreter


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 8220 Gang (aka 8220 Mining Group, Water Sigbin)	China	All	Worldwide
	MOTIVE		
	Financial Gain	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	TARGETED CVEs		
	CVE-2017-3506 CVE-2023-21839	XMRig Cryptominer, PureCrypter loader	Oracle WebLogic Server
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1047: Windows Management Instrumentation; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information; T1112: Modify Registry; T1562.001: Disable or Modify Tools; T1620: Reflective Code Loading; T1055: Process Injection; T1055.012: Process Hollowing; T1053.005: Scheduled Task; T1057: Process Discovery; T1012: Query Registry; T1518.001: Security Software Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1001: Data Obfuscation; T1571: Non-Standard Port; T1095: Non-Application Layer Protocol; T1496: Resource Hijacking			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>CloudSorcerer</u>	-	Government	Russia
	MOTIVE		
	Information theft and espionage	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	TARGETED CVEs		
	-	-	-
TTPs			
TA0007: Discovery; TA0011: Command and Control; TA0009: Collection; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0010: Exfiltration; T1059: Command and Scripting Interpreter T1059.009: Cloud API; T1559: Inter-Process Communication; T1053: Scheduled Task/Job; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1140: Deobfuscate/Decode Files or Information; T1112: Modify Registry; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1012: Query Registry; T1082: System Information Discovery; T1005: Data from Local System; T1102: Web Service; T1568: Dynamic Resolution; T1567: Exfiltration Over Web Service; T1537: Transfer Data to Cloud Account			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><u>CRYSTALRAY</u></div>	-	All	Australia, Bangladesh, Brazil, Canada, China, Colombia, Czechia, France, Germany, India, Indonesia, Iran, Ireland, Italy, Japan, Korea, Mexico, Netherlands, Northern Ireland, Poland, Russia, Singapore, Sweden, Taiwan, UK, USA, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2022-44877 CVE-2021-3129 CVE-2019-18394	-	CWP Control Web Panel, Laravel Ignition, Ignite Realtime Openfire
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; TA0043: Reconnaissance; TA0042: Resource Development; T1595: Active Scanning; T1595.002: Vulnerability Scanning; T1592: Gather Victim Host Information; T1590: Gather Victim Network Information; T1588: Obtain Capabilities; T1588.002: Tool; T1588.006: Vulnerabilities; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1555: Credentials from Password Stores; T1496: Resource Hijacking; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1071: Application Layer Protocol; T1070: Indicator Removal; T1010 Application Window Discovery; T1005: Data from Local System; T1053: Scheduled Task/Job; T1053.003: Cron;			


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)</u></p>	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Airlines, Journalists, Logistics	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Sudan, Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	BugSleep Backdoor	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1036: Masquerading; T1053: Scheduled Task/Job; T1204: User Execution; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1059: Command and Scripting Interpreter; T1133: External Remote Services; T1574: Hijack Execution Flow; T1497: Virtualization/Sandbox Evasion; T1070: Indicator Removal; T1033: System Owner/User Discovery; T1132: Data Encoding; T1132.002: Non-Standard Encoding; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Void Banshee</u>	-	Education	North America, Europe, and Southeast Asia
	MOTIVE		
	Information Theft & Financial Gainer		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2024-38112	Atlantida Stealer	Windows MSHTML
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1218: System Binary Proxy Execution; T1218.009: Regsvcs/Regasm; T1584: Compromise Infrastructure; T1584.004: Server; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1055: Process Injection; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1005: Data from Local System; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>APT17 (aka Tailgater Team, Elderwood, Elderwood Gang, Sneaky Panda, SIG22, Beijing Group, Bronze Keystone, TG-8153, TEMP.Avengers, Dogfish, Deputy Dog, ATK 2)</u></p>	China	Defense, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs, lawyers, Business	Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	9002 RAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel; T1083: File and Directory Discovery; T1007: System Service Discovery; T1005: Data from Local System; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1656: Impersonation; T1036: Masquerading; T1562: Impair Defenses; T1056: Input Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>GhostEmperor</u>	China	Telecommunications and Government	Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Demodex Rootkit	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1014: Rootkit; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Andariel (aka APT45, Onyx Sleet, formerly PLUTONIUM, DarkSeoul, Silent Chollima, and Stonefly)</u></p>	North Korea	Critical Infrastructure, Defense, Aerospace, Government, Financial, Healthcare, Pharmaceutical, Engineering, Telecommunications, Transportation, Technology, Biotech, Chemicals, Education, Energy, Insurance, Legal, Medical Equipment, Nuclear Power, Retail, Utilities, and Agricultural	United States, Brazil, India, Japan, South Korea, United Kingdom, Germany, France, Nigeria
	MOTIVE		
	Espionage and Information theft, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2021-44228	Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimos2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI ransomware	Apache Log4j2
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0042: Resource Development; TA0003: Persistence; TA0007: Discovery; TA0008: Lateral Movement; TA0043: Reconnaissance; TA0009: Collection; TA0011: Command and Control; TA0006: Credential Access; TA0010: Exfiltration; TA0005: Defense Evasion; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059.001: PowerShell; T1059.006: Python; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.003: Windows Command Shell; T1055.012: Process Hollowing; T1055: Process Injection; T1055.003: Thread Execution Hijacking; T1134: Access Token Manipulation; T1098: Account Manipulation; T1543.003: Windows Service; T1543: Create or Modify System Process; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1007: System Service Discovery; T1087: Account Discovery; T1591: Gather Victim Org Information; T1592: Gather Victim Host Information; T1595: Active Scanning; T1596: Search Open Technical Databases; T1003: OS Credential Dumping; T1048: Exfiltration Over Alternative Protocol; T1090: Proxy; T1560: Archive Collected Data; T1572: Protocol Tunneling; T1587.001: Malware; T1587.004: Exploits; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1039: Data from Network Shared Drive; T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Stargazer</u> <u>Goblin</u>	-	All	Worldwide
	MOTIVE		
	Information theft, Financial gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Atlantida Stealer, Rhadamanthys, RisePro, Lumma Stealer, and RedLine	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0042: Resource Development; T1204: User Execution; T1566: Phishing; T1189: Drive-by Compromise; T1059: Command and Scripting Interpreter; T1071: Application Layer Protocol; T1027: Obfuscated Files or Information; T1036: Masquerading; T1212: Exploitation for Credential Access; T1083: File and Directory Discovery; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1608: Stage Capabilities; T1608.001: Upload Malware			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1592: Gather Victim Host Information	
	T1590: Gather Victim Network Information	
	T1598: Phishing for Information	T1598.003: Spearphishing Link
	T1591: Gather Victim Org Information	
	T1596: Search Open Technical Databases	
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities T1588.005: Exploits T1588.002: Tool
	T1584: Compromise Infrastructure	T1584.004: Server
	T1583: Acquire Infrastructure	T1583.001: Domains
	T1608: Stage Capabilities	T1608.004: Drive-by Target T1608.001: Upload Malware
	T1587: Develop Capabilities	T1587.001: Malware T1587.004: Exploits
	T1585: Establish Accounts	T1585.001: Social Media Accounts
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain T1195.001: Compromise Software Dependencies and Development Tools
TA0001: Initial Access	T1566: Phishing	T1566.002: Spearphishing Link T1566.001: Spearphishing Attachment
	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1059: Command and Scripting Interpreter	T1059.008: Network Device CLI T1059.006: Python T1059.003: Windows Command Shell T1059.009: Cloud API T1059.001: PowerShell T1059.007: JavaScript T1059.005: Visual Basic T1059.010: AutoHotKey & AutoIT T1059.004: Unix Shell
	T1203: Exploitation for Client Execution	
TA0002: Execution	T1204: User Execution	T1204.002: Malicious File T1204.001: Malicious Link
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1651: Cloud Administration Command	
	T1047: Windows Management Instrumentation	
	T1129: Shared Modules	
	T1559: Inter-Process Communication	
	T1569: System Services	T1569.002: Service Execution

Tactic	Technique	Sub-technique
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading T1574.011: Services Registry Permissions Weakness
	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.005: Device Registration
	T1133: External Remote Services	
	T1505: Server Software Component	T1505.001: SQL Stored Procedures
	T1136: Create Account	T1136.001: Local Account
TA0004: Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task T1053.003: Cron
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1134: Access Token Manipulation	
	T1055: Process Injection	T1055.003: Thread Execution Hijacking T1055.012: Process Hollowing
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading T1574.011: Services Registry Permissions Weakness
		T1574.011: Hijack Execution Flow: Services Registry Permissions Weakness
	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.005: Device Registration
TA0005: Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location T1036.008: Masquerade File Type T1036.004: Masquerade Task or Service
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1134: Access Token Manipulation	
	T1070: Indicator Removal	T1070.004: File Deletion T1070.001: Clear Windows Event Logs
	T1055: Process Injection	T1055.003: Thread Execution Hijacking T1055.012: Process Hollowing
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1620: Reflective Code Loading	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1140: Deobfuscate/Decode Files or Information	
	T1112: Modify Registry	
	T1656: Impersonation	
	T1480: Execution Guardrails	
	T1222: File and Directory Permissions Modification	
	T1218: System Binary Proxy Execution	T1218.005: Mshta T1218.009: Regsvcs/Regasm
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1497: Virtualization/Sandbox Evasion	
	T1014: Rootkit	

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	T1110.003: Password Spraying
	T1528: Steal Application Access Token	
	T1621: Multi-Factor Authentication Request Generation	
	T1040: Network Sniffing	
	T1649: Steal or Forge Authentication Certificates	
	T1606: Forge Web Credentials	T1606.001: Web Cookies
	T1003: OS Credential Dumping	
	T1212: Exploitation for Credential Access	
TA0007: Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1083: File and Directory Discovery	
	T1012: Query Registry	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1046: Network Service Discovery	
	T1040: Network Sniffing	
	T1217: Browser Information Discovery	
	T1087: Account Discovery	T1087.001: Local Account
	T1033: System Owner/User Discovery	
	T1010: Application Window Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1115: Clipboard Data	
	T1056: Input Capture	T1056.001: Keylogging
	T1005: Data from Local System	
	T1213: Data from Information Repositories	
	T1113: Screen Capture	
	T1039: Data from Network Shared Drive	
TA0011: Command and Control	T1571: Non-Standard Port	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1095: Non-Application Layer Protocol	
	T1001: Data Obfuscation	
	T1573: Encrypted Channel	
	T1105: Ingress Tool Transfer	
	T1102: Web Service	
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1132: Data Encoding	T1132.001: Standard Encoding T1132.002: Non-Standard Encoding
	T1090: Proxy	
	T1572: Protocol Tunneling	

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1048: Exfiltration Over Alternative Protocol	
	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	
	T1537: Transfer Data to Cloud Account	
TA0040: Impact	T1496: Resource Hijacking	
	T1565: Data Manipulation	
	T1657: Financial Theft	
	T1498: Network Denial of Service	
	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1485: Data Destruction	
	T1491: Defacement	T1491.001: Internal Defacement
	T1489: Service Stop	

Top 5 Takeaways

#1

In July, there were **six zero-day** vulnerabilities, with the 'Three Celebrity Vulnerabilities' taking center stage. These featured flaws such as **regreSSHion**, **CosmicSting** and **Log4shell**.

#2

Over the course of the month, a variety of ransomware variants, including the well-known **Play ransomware**, have been actively targeting victims with its new Linux Variant. **Eldorado ransomware**, another malicious program, has focused its attacks on a more specific geographical range, primarily targeting victims in **United States, Italy, Croatia**. Furthermore, **Void Banshee**, an APT group, has exploited the **CVE-2024-38112** flaw in the Education sector in North America, Europe, and Southeast Asia for information theft and financial gain.

#3

A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **Atlantida Stealer**, **Play ransomware**, **Coroxy backdoor**, **Braodo Stealer** and **Demodex Rootkit**.

#4

Eleven active adversaries were identified across multiple campaigns, targeting the following key industries: **Government, Transportation, Education and Healthcare**.

#5

Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of 29 attacks. These attacks top impacted **United States, Germany and United Kingdom**.

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 **11 active threat actors**, **29 active malware**, and **170 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 (JUNE 2024)

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

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

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

Appendix

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

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

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

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

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

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities

CVE - Common Vulnerabilities and Exposures

CPE - Common Platform Enumeration

CWE - Common Weakness Enumeration

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>dllFake</u>	SHA256	1fa84b696b055f614ccd4640b724d90ccad4afc035358822224a02a9e2c12846, cdc1f2430681e9278b3f738ed74954c4366b8eff52c937f185d760c1bbba2f1d, fdc84cb0845f87a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91eb, a89953915eabe5c4897e414e73f28c300472298a6a8c055fcc956c61c875fd96, 70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093, 33e4d5eed3527c269467eec2ac57ae94ae34fd1d0a145505a29c51cf8e83f1b9, 03761d9fd24a2530b386c07bf886350ae497e693440a9319903072b93a30c82d, de4e03288071cdebe5c26913888b135fb2424132856cc892baea9792d6c66249
<u>MerkSpy</u>	SHA256	92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08, 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a, 0ffadb53f9624950dea0e07fcffcc31404299230735746ca43d4db05e4d708c6, dd369262074466ce937b52c0acd75abad112e395f353072ae11e3e888ac132a8, 569f6cd88806d9db9e92a579dea7a9241352d900f53ff7fe241b0006ba3f0e22, 6cdc2355cf07a240e78459dd4dd32e26210e22bf5e4a15ea08a984a5d9241067
<u>WINELOADER</u>	SHA256	d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b741750, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45

Attack Name	TYPE	VALUE
<u>RootSaw</u>	SHA256	a0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c
<u>VaporRage</u>	SHA256	c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4, 7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e, 773f0102720af2957859d6930cd09693824d87db705b3303cef9ee794375ce13
<u>XMRig</u>	SHA256	f4d1b970bc9e5d319c5432be9e3863b5a20bf26e557c8cea6f3949df0012cf01, 3961c31ed8411944c5401bb7a9c6738ec963910c205dba5e35292c7d4f7b912b, 74d22338e9b71cefb4f5d62497e987e396dc64ca86b04a623c84d5b66a2d7d3e, f34fc824a6c655bd6320b7818acdada9a5a570b88dd46507fdf73cd254af9b19f, 621a9f892436647a492e3877502454d1783dc0cf4e4ba9f3f459a8c2ac7e6d97, f63921129822475dd132a116b11312ebbb0cdc8b54f188aabeb7cf7a8c9065fd, 05e1988f56fe199f7e401c8f4d6ee50bb26ab34fb3f96c22de959c7e5f92de77, d0cf7388253342f43f9b04da27f3da9ee18614539efdc2d9c4a0239af51ddbe4, 09ec3bf64600d1fedbd11bb3ebb705a0f541d1310f5f8690de70d37648fcd4b4
<u>PureCrypter</u>	SHA256	397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3, 5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2cd80e99, 5d649c5aa230376f1a08074aee91129b8031606856e9b4b6c6d0387f35f6629d, 7a5b8b448e7d4fa5edc94dcb66b1493adad87b62291be4ddcbd61fb4f25346a8, a7c006a79a6ded6b1cb39a71183123dcaaaa21ea2684a8f199f27e16fcb30e8e, be18d4fc15b51daedc3165112dad779e17389793fe0515d62bbcf00def2c3c2d, c846e7bbbc1f65452bdca87523edf0fd1a58cbd9a45e622e29d480d8d80ac331, efc0b3bfcec19ef704697bf0c4fd4f1cfb091dbfee9c7bf456fac02bcffcfd,f, f950d207d33507345beeb3605c4e0adfa6b274e67f59db10bd08b91c96e8f5ad

Attack Name	TYPE	VALUE
<u>PureCrypter</u>	MD5	0d8b1ad53fddacf2221409c1c1f3fd70, 0ede257a56a6b1fbd2b1405568b44015, 14e4bfe2b41a8cf4b3ab724400629214, 17f512e1a9f5e35ce5761dba6ccb09cb, 18e9cd6b282d626e47c2074783a2fa78, 1d3c8ca9c0d2d70c656f41f0ac0fe818, 2499343e00b0855882284e37bf0fa327, 2964ce62d3c776ba7cb68a48d6afb06e, 2fa290d07b56bde282073b955eae573e, 3f92847d032f4986026992893acf271e, 5420dcbae4f1fba8afe85cb03dcd9bfc, 61259b55b8912888e90f516ca08dc514, 71b4db69df677a2acd60896e11237146, 754920678bc60dabeb7c96bfb88273de, 765f09987f0ea9a3797c82a1c3fced46, 785bfaa6322450f1c7fe7f0bf260772d, 8503b56d9585b8c9e6333bb22c610b54, 8ef7d7ec24fb7f6b994006e9f339d9af, a478540cda34b75688c4c6da4babf973, ae158d61bed131bcfd7d6cecdccde79b, b4fd2d06ac3ea18077848c9e96a25142, b5c60625612fe650be3dcbe558db1bbc, b6c849fcdca6c6d8367f159047d26c4, bbd003bc5c9d50211645b028833bbeb2 c3b90a10922eef6d635c6c786f29a5d0, c9ca95c2a07339edb13784c72f876a60, d70bb6e2f03e5f456103b9d6e2dc2ee7, dbcaa05d5ca47ff8c893f47ad9131b29, de94d596cac180d348a4acdeaaa9439, eaaf20fdc4a07418b0c8e85a2e3c9b27, f1c29ba01377c35e6f920f0aa626eaf5, f34d5f2d4577ed6d9ceec516c1f5a744, f4eebe921b734d563e539752be05931d, fa4ffa1f263f5fc67309569975611640, fdd4cd11d278dab26c2c8551e006c4ed
<u>Nim Downloader</u>	SHA256	d891f4339354d3f4c4b834e781fa4eaca2b59c6a8ee9340cc489ab00 23e034c8, d7a66f8529f1c32342c4ed06c4a4750a93bd44161f578e5b94d6d30f 7cc41581, c21ad804c22a67ddb62adf5f6153a99268f0b26e359b842ebeabcada 824c277f
	URL	hxxps://auth.economy-gov- il[.]com/SUPPOSED_GRASSHOPPER.bin?token=ghhdjsdgsd
<u>Donut</u>	SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223df090 bb26b3cd7
<u>Silver</u>	SHA256	2070dd30e87c492e6f44ebb0a37bcae7cb309de61e1c4e6223df090 bb26b3cd7
	Hostname	www.economy-gov-il[.]com

Attack Name	TYPE	VALUE
<u>Mekotio</u>	SHA1	5e92f0fcddc1478d46914835f012137d7ee3c217, f68d3a25433888aa606e18f0717d693443fe9f5a, 3fe5d098952796c0593881800975bcb09f1fe9ed, 1087b318449d7184131f0f21a2810013b166bf37, ef22c6b4323a4557ad235f5bd80d995a6a15024a
<u>Eldorado Ransomware</u>	SHA256	1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0a b9f27b, 7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122 ae66dd, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d967 36174a7, b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379 f12c70de, dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22 258c33, 8badf1274da7c2bd1416e2ff8c384348fc42e7d1600bf826c9ad695fb5 192c74, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d967 36174a7
	MD5	9d1fd92ea00c6eef88076dd55cad611e, 315a9d36ed86894269e0126b649fb3d6
	TOR Address	hxxp[:]//dataleakypypu7uwbIm5kttv726l3iripago6p336xjnbstkjwrlnli d[.]onion
	Email	russoschwartz@onionmail[.]org
	IPv4	173[.]44[.]141[.]152
<u>Lumma</u>	SHA256	B1B8EA15E6BBFC7C38EB394D7E81A99A93689464FAF991D77E2872 2E5B0E4681, D9F6408B67628D5618A4FBABA97404AC55988633CCB2A02A09C95 B0B134BAFC9, DD5B52A63E8A774C058E558AA7E983D6AA51F560BA3F01829287C 4B85081B884, D856A66EA554538D421ABCEB2D304200537F5A268CBFDE8F52F41A 0C048EDFDC, 148c456e83e746a63e54ec5abda801731c42f3778e8eb0bf5a5c731b9 a48c45d, 2f5624dcda1d58a45491028acc63ff3f1f89f564015813c52eebd80f51 220383, 98b7488b1a18cb0c5e360c06f0c94d19a5230b7b15d0616856354fb6 4929b388, a484fa09be45608e23d8e67cd28675fa3e3c4111af396501385256ce3 4ff1d95
	URLs	hxxps[:]//considerrycurrentyws[.]shop, hxxps[:]//deprivedrinkyfair[.]shop, hxxps[:]//detailbaconroollyws[.]shop, hxxps[:]//distincttangyflippan[.]shop, hxxps[:]//greentastellesqwm[.]shop, hxxps[:]//horsedwollfedrwos[.]shop, hxxps[:]//innerverdanytiresw[.]shop,

Attack Name	TYPE	VALUE
<u>Lumma</u>	URLs	hxxps[:]//lamentablegapinkwaq[.]shop, hxxps[:]//macabrecondfucews[.]shop, hxxps[:]//messtimetabledkolvk[.]shop, hxxps[:]//patternapplauderw[.]shop, hxxps[:]//relaxtionflouwerwi[.]shop, hxxps[:]//sideindexfollowragelrew[.]pw, hxxps[:]//slamcopynammeks[.]shop, hxxps[:]//standingcomperewhitwo[.]shop, hxxps[:]//stickyyummyskiwffe[.]shop, hxxps[:]//sturdyregulararmsnhw[.]shop, hxxps[:]//understanndtytonyguw[.]shop, hxxps[:]//vivaciousdqugilew[.]shop
<u>Meduza</u>	SHA256	2aa321a93bfa09139831e510e3cf9a869ece3d2e00889c846be1699 63cbb3b34, e29fa10b148be279c203e1f9079e7245b834f7912534c1bf4180af37 686f621e, 73171634ceb5c5007cf78a6f32d6633590830f39f4e5311a4f323a4d 44975ca7, cee2442ce10695e29830a77d38d4af1e24d6881203743664abc4ad 9a8c97c0f2, 2ad84bfff7d5257fdeb81b4b52b8e0115f26e8e0cdaa014f9e3084f5 18aa6149, 114b868f319162c5d6ff92796e41910f54de0e89f895a066fd4980c6 dba2e323, 478eb22a1f1be2ef6e70625cf42ca61c716389135acbb705c0e21f0c f330bf46, 811dbefc20a0a348038ef8f6adc70c38f9b778c20abfb85953a26dc6 037a0cde, 62460105edf1636fd9605894deba01a417fcd8558c9a43ceefbf9fdd a536a9c1, 4cfc33deeedcc336cc541b2a91eb666fdb2c8984c215daf8cee6ab79 3c9ef9d1, aa46a10b5392afadabb645417e88a32a95a82796b4b9517ea983ee 589ed78ab6, Bdcd3addc990fa93827a6cfbf9687076df89cead996396e443d4465 c4de43aba
<u>ViperSoftX</u>	SHA256	814297c47c67c82c4700ed0f099d558b8ac45e91cbb72d44a46c2e2 a0c6b11aa, fef939b4a90ee28e2cffe1d8f0dcfc0d5dd174b0321e2a2c6cd46c65b 7b79a2d, 779323771d4ebd97de44bdb9cb03e40156182b2012acfd444a4787 902b0f1f35, 4d1ef869c4bddeccc318939ea2651ce5a3fc2e369ba44a2e24cb9b1 02ef2be19, d55aaa430ea18f3b85ccbfe2f34ce14b9b88d348d83e6c41d3aaea4 56b69b869
<u>Kematian Stealer</u>	SHA256	1c7424d6cbd0e5104151b6317b914a24992a9de9855d7ec4e0cd49 3fac0a3b98

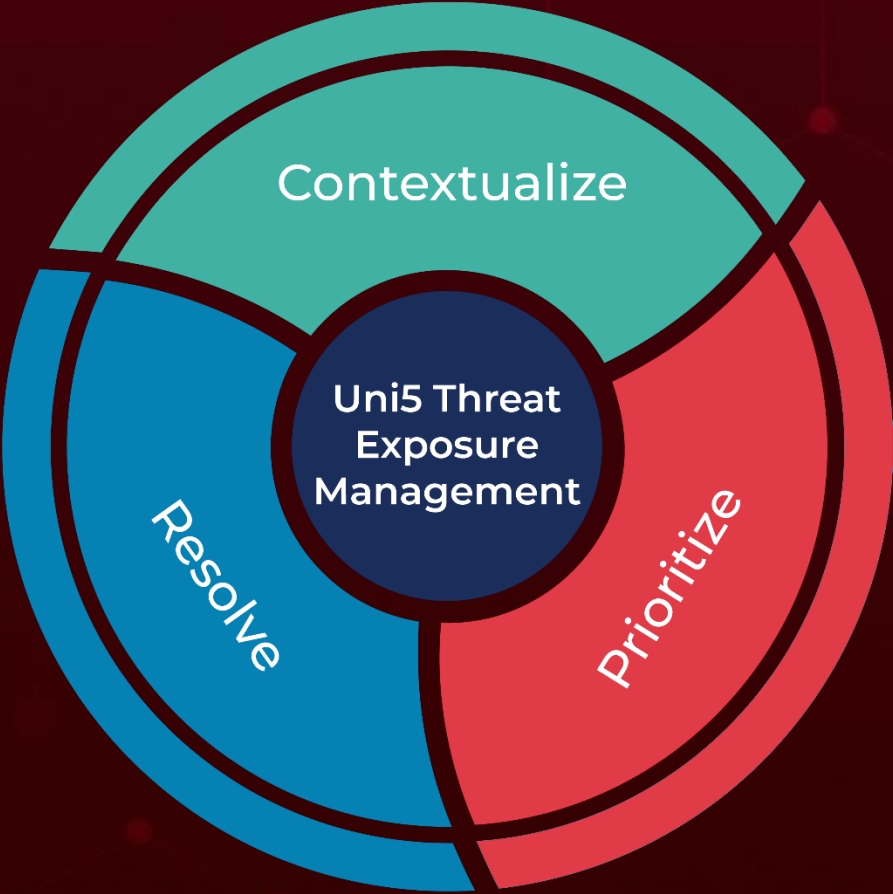
Attack Name	TYPE	VALUE
<u>EstateRansom</u> <u>ware</u>	SHA1	cb704d2e8df80fd3500a5b817966dc262d80ddb8, 2c56e9beea9f0801e0110a7dc5549b4fa0661362, 5e460a517f0579b831b09ec99ef158ac0dd3d4fa, 107ec3a7ed7ad908774ad18e3e03d4b999d4690c
<u>BugSleep</u> <u>Backdoor</u>	SHA256	73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52 b9c6b30e, 960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c9 6ba5809, b8703744744555ad841f922995cef5dbca11da22565195d05529f5f90 95fbfca, 94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7 130c472, 5df724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a7060 8f3a1c0
<u>ShadowRoot</u> <u>Ransomware</u>	SHA1	cd8fbf0dcdd429c06c80b124caf574334504e99a, 1c9629aeb0e6dbe48f9965d87c64a7b8750bbbf93
<u>Atlantida</u> <u>Stealer</u>	SHA256	6f1f3415c3e52dcdabb012f412aef7b9744786b2d4a1b850f1f45610487 16c750, 2b6c8aa2ac917d978dfec53cef70eaca36764a93d01d93786cc0d84da 47ce8e6, 385ebe3d5bd22b6a5ae6314f33a7fa6aa24814005284c79edaa5bdcf9 8e28492, 2ebf051f6a61fa825c684f1d640bfb3bd79add0afcff698660f83f22e65 44cba, ab59a8412e4f8bf3a7e20cd656edacf72e484246dfb6b7766d467c2a1 e4cdab0
	IPv4	185[.]172[.]128[.]95
<u>9002 RAT</u>	SHA256	28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd 7a41e e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f2 29513c, d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d00 27172436, c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3 d72b50c, caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec 973af5, de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d 00edd0
<u>Jellyfish Loader</u>	MD5	e577fa8e0491fe027bc4da86a01f64ea
	SHA1	9ff473df01487ca59d6426c8fddf77a1c27b2437
	SHA256	e654e97efb6214bea46874a49e173a3f8b40ef30fd0179b1797d14b cc2c2aa6c

Attack Name	TYPE	VALUE
<u>Play Ransomware</u>	SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30
	IPv4	108[.]61[.]142[.]190 , 45[.]76[.]165[.]129, 149[.]248[.]2[.]142
	URL	hxxp[:]//108[.]61[.]142[.]190/FX300[.]rar, hxxp[:]//108[.]61[.]142[.]190/1[.]dll[.]sa, hxxp[:]//108[.]61[.]142[.]190/64[.]zip, hxxp[:]//108[.]61[.]142[.]190/winrar-x64-611[.]exe, hxxp[:]//108[.]61[.]142[.]190/PsExec[.]exe, hxxp[:]//108[.]61[.]142[.]190/host1[.]sa
<u>Coroxy Backdoor</u>	SHA256	872b07b4a322a8fd471d076c55c2231c26c011891f90821e839ae3604cc52de5
	URL	hxxp[:]//108[.]61[.]142[.]190/host1[.]sa, hxxp[:]//108[.]61[.]142[.]190/1[.]dll[.]sa
	IPv4	45[.]76[.]165[.]129, 108[.]61[.]142[.]190
<u>Braodo Stealer</u>	SHA256	8dccc38514c8167c849c1bba9c3c6ef20f219a7439d2fc1f889410e34d8f6c9, 204a8346a401f3101361c4571fe1c4bbedc9e54e4f5c181bb7c81cf843286730
<u>Demodex Rootkit</u>	MD5	4bb191c6d3a234743ace703d7d518f8f, 95e3312de43c1da4cc3be8fa47ab9fa4, d8ebfd26bed0155e7c4ec2ca429c871d
	SHA1	43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de, a59cca28205eeb94c331010060f86ad2f3d41882, bab2ae2788dee2c41065850b2877202e57369f37
<u>Rhadamanthys</u>	SHA256	060de3b4cf3056f24de882b4408020cee0510cb1ff0e5007c621bc98e5b4bdf3, 64a49ff6862b2c924280d5e906bc36168112c85d9acc2eb778b72ea1d4c17895
	IPv4:Port	147[.]45[.]44[.]73[:]:1488, 89[.]23[.]98[.]116[:]:1444, 147[.]78[.]103[.]199[:]:2529
<u>RisePro</u>	SHA256	52c071349a51f000c446acb9ba38194449a455ba3cff5be290ba336da b1176fd 115aaa4fe6c3f309b03db57b4ce7e76ba8952cb240a22b6c35697cfe6352488f b8d237fe35a52972a376a80721d5a97f9edc5da447502d3564185eaa6df07706
<u>RedLine</u>	SHA256	8d8d7eb1180c13ed629dceac6c399c656692a6476c49047e0822bec6156a253a
	IPv4:Port	147[.]45[.]47[.]64[:]:11837

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
August 1, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com