Date of Publication
July 15, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

08 to 14 JULY 2024

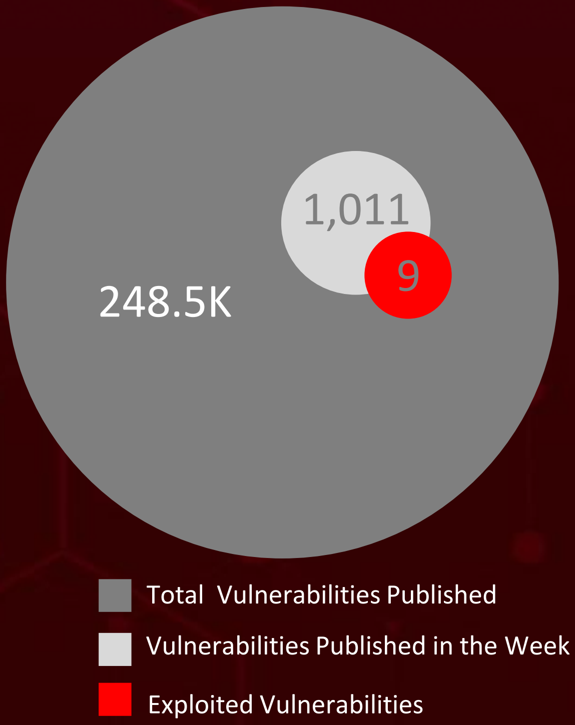
Table Of Contents

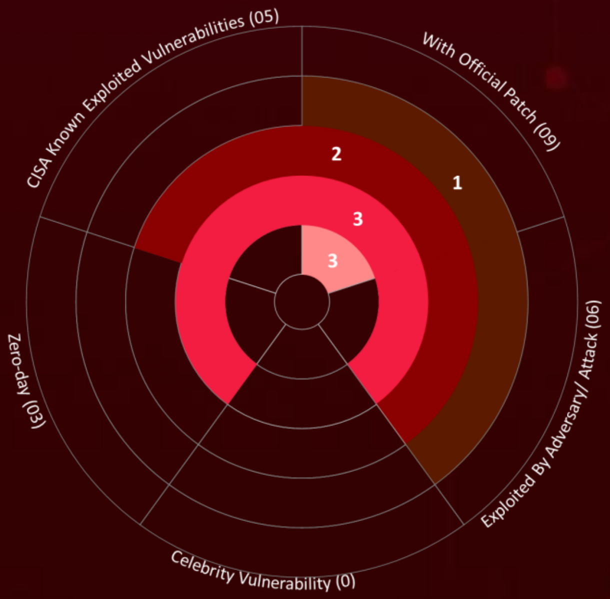
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **five** attacks were executed, **nine** vulnerabilities were uncovered, and **two** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a newly emerged cyber threat actor, **CRYSTALRAY** employing advanced tactics and tools to steal credentials and deploy cryptocurrency miners. CRYSTALRAY is motivated by collecting and selling credentials, deploying cryptominers, and maintaining persistence in victim environments. The threat actor leverages several open-source tools (OSS), including zmap, asn, httpx, nuclei, platypus, and SSH-Snake, to facilitate their malicious activities.

Furthermore, **Eldorado**, a new Golang-based ransomware, targets both Windows and VMware ESXi virtual machines. It has already claimed 16 victims in the U.S., affecting sectors such as real estate, education, healthcare, and manufacturing. Eldorado avoids critical system files to maintain usability, and self-deletes post-encryption to cover its tracks. These rising attacks present a significant and immediate threat to users globally.





High Level Statistics

5

Attacks Executed

- Eldorado ransomware
- Lumma
- Meduza Stealer
- ViperSoftX
- Kematian Stealer

9

Vulnerabilities Exploited

- CVE-2023-2071
- CVE-2023-29464
- CVE-2024-21412
- CVE-2024-5441
- CVE-2024-38080
- CVE-2024-38112
- CVE-2022-44877
- CVE-2021-3129
- CVE-2019-18394

2

Adversaries in Action

- CloudSorcerer
- CRYSTALRAY

Insights

CRYSTALRAY

a newly emerged cyber threat actor, employing advanced tactics and tools to steal credentials and deploy cryptocurrency miners

Eldorado Ransomware

a new Golang based ransomware, targets Windows and VMware ESXi, affecting U.S. sectors like real estate, education, healthcare, and manufacturing

Kematian

an open-source, PowerShell-based malware, used for stealthy access and data transfer from Windows systems

CloudSorcerer

a newly discovered APT group has been targeting Russian government entities since May 2024. This group has shown a high level of sophistication and persistence in their attacks, posing a significant threat to the security and stability of the targeted organizations

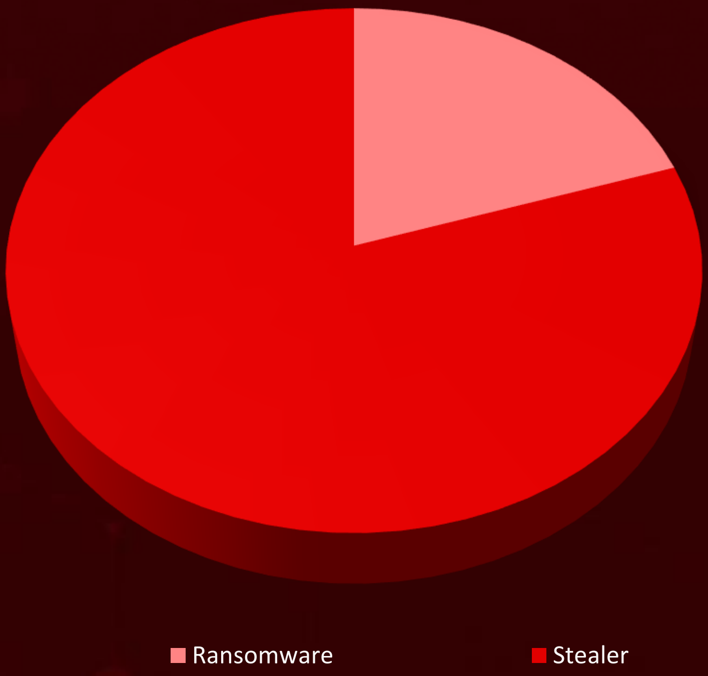
CVE-2024-21412

An active campaign is exploiting a vulnerability in Microsoft SmartScreen, leading to the deployment of malicious payloads such as Lumma and Meduza Stealer

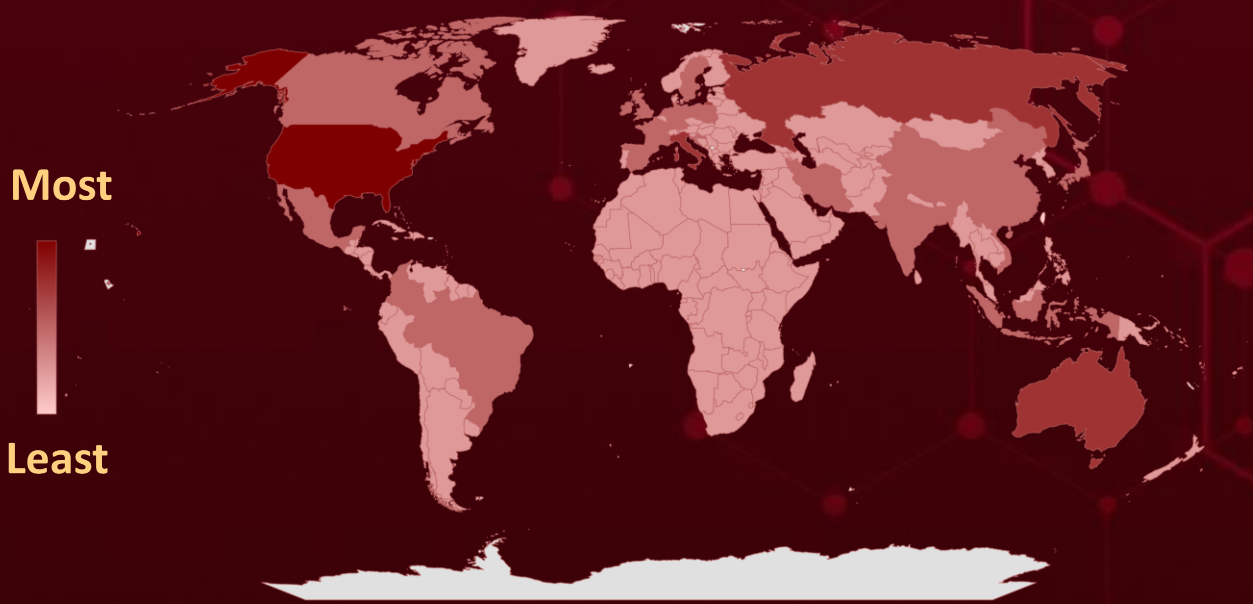
ViperSoftX

sophisticated malware, distributed as eBooks over torrent networks, employ the CLR to load and execute PowerShell commands

Threat Distribution



Targeted Countries



Powered by Bing

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

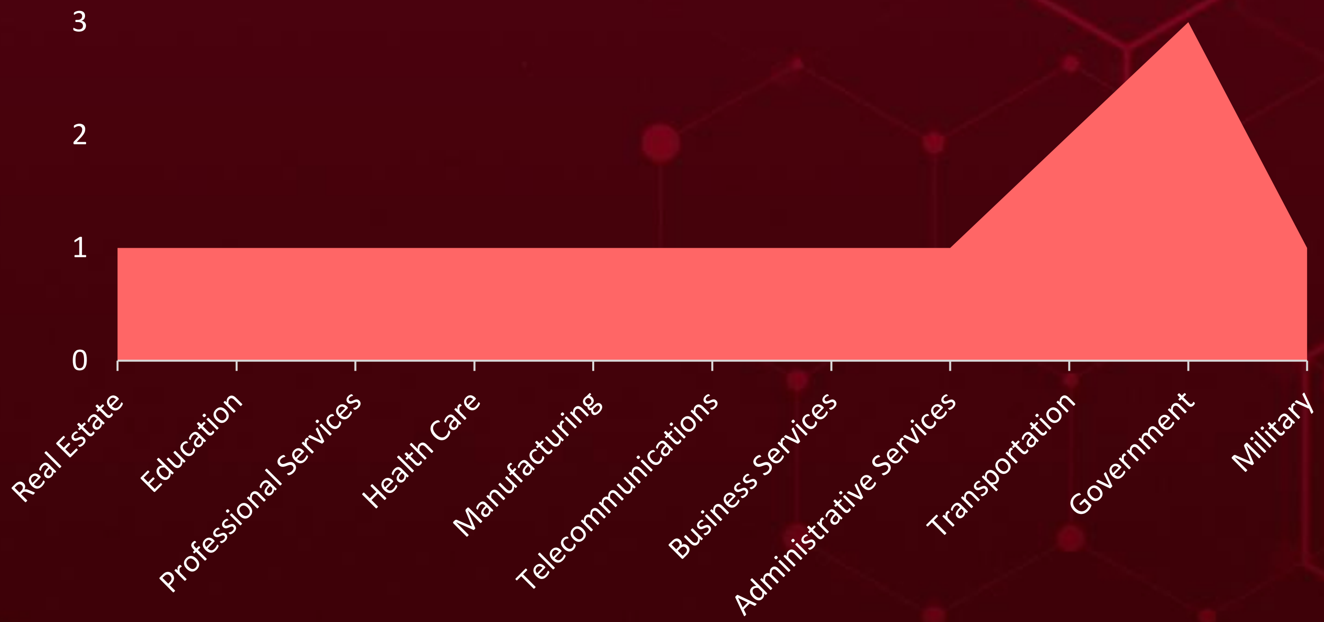
	Countries
	United States
	Australia
	Italy
	Russia
	Netherlands
	Bangladesh
	Iran
	Canada
	Vietnam
	China
	Sweden
	Colombia
	Ireland
	Croatia
	Japan
	France
	Mexico
	Poland
	Brazil
	Singapore
	Germany
	Spain
	India

	Countries
	Indonesia
	United Kingdom
	Seychelles
	Nauru
	United Arab Emirates
	Burkina Faso
	Peru
	Burundi
	Brunei
	Cabo Verde
	Moldova
	Cambodia
	North Macedonia
	Cameroon
	Saint Kitts & Nevis
	Antigua and Barbuda
	South Korea
	Central African Republic
	Tonga
	Chad
	Mauritania
	Chile
	Morocco

	Countries
	Argentina
	Nicaragua
	Armenia
	Palau
	Comoros
	Qatar
	Congo
	Sao Tome & Principe
	Costa Rica
	Slovenia
	Côte d'Ivoire
	St. Vincent & Grenadines
	Algeria
	Tanzania
	Cuba
	Turkmenistan
	Cyprus
	Malta
	Czech Republic (Czechia)
	Benin
	Denmark
	Mongolia
	Argentina

	Countries
	Djibouti
	Myanmar
	Dominica
	Bhutan
	Dominican Republic
	Nigeria
	DR Congo
	Oman
	Ecuador
	Papua New Guinea
	Egypt
	Bolivia
	El Salvador
	Bosnia and Herzegovina
	Equatorial Guinea
	Samoa
	Eritrea
	Senegal
	Estonia
	Botswana
	Eswatini
	Somalia
	Djibouti

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1588.006 Vulnerabilities

T1588 Obtain Capabilities

T1204 User Execution

T1190 Exploit Public-Facing Application

T1053 Scheduled Task/Job

T1005 Data from Local System

T1027 Obfuscated Files or Information

T1082 System Information Discovery

T1083 File and Directory Discovery

T1070 Indicator Removal

T1059.001 PowerShell

T1071 Application Layer Protocol

T1498 Network Denial of Service

T1566 Phishing

T1564 Hide Artifacts

T1070.004 File Deletion

T1041 Exfiltration Over C2 Channel

T1068 Exploitation for Privilege Escalation

T1047 Windows Management Instrumentation

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Eldorado ransomware	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**
-			-

IOC TYPE	VALUE
SHA256	1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b, 7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lumma	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**
-			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412

IOC TYPE	VALUE
SHA256	B1B8EA15E6BBFC7C38EB394D7E81A99A93689464FAF991D77E28722E5B0E4681, D9F6408B67628D5618A4FBABA97404AC55988633CCB2A02A09C95B0B134BAFC9

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
Meduza Stealer	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
IOC TYPE	VALUE		
SHA256	643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2, d278aa079205cf4bb605de28bc6d6eca5a63b4cdd9d0c7488c40945d2b90b0a0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ViperSoftX	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
-			-
IOC TYPE	VALUE		
SHA256	814297c47c67c82c4700ed0f099d558b8ac45e91cbb72d44a46c2e2a0c6b11aa, fef939b4a90ee28e2cffe1d8f0dcfc0d5dd174b0321e2a2c6cd46c65b7b79a2d		

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
Kematian Stealer	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**
-			-

IOC TYPE	VALUE
MD5	80cf2d7ae1f3acc750f2cf454b4832c6

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2071	✗	FactoryTalk View Machine Edition: 12.0 - 13.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	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
CVE-2023-29464	✗	FactoryTalk Linx: 6.20	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rockwellautomation:factorytalk_linx:6.20:*:*:*:*:*:*:* cpe:2.3:a:rockwellautomation:factorytalk_linx:6.30:*:*:*:*:*:*:*	-
FactoryTalk Linx Denial-of-Service and Information Disclosure Vulnerability	✗		
	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
CVE-2024-21412	✗	Microsoft Windows Internet Shortcut Files	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	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
CVE-2024-5441	✗	Modern Events Calendar, Modern Events Calendar Lite	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	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
CVE-2024-38080	✗	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 KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V Elevation of Privilege Vulnerability	✓		
	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
[CVE-2024-38112](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112)	✗	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 KEV	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows MSHTML Platform Spoofing Vulnerability	✓		
	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
CVE-2022-44877	✗	CWP Control Web Panel	CRYSTALRAY
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	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
CVE-2021-3129	✗	Laravel Ignition	CRYSTALRAY
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:facade:ignition:*:*:*:*:*:laravel:*:*	-
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
CVE-2019-18394	✗	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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
CloudSorcerer	-	Government	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
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
CRYSTALRAY	-	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/RANSOMWARE	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;

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **CloudSorcerer, CRYSTALRAY** and malware **Eldorado ransomware, Lumma, Meduza Stealer, ViperSoftX, Kematian Stealer.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **CloudSorcerer, CRYSTALRAY** and malware **Eldorado ransomware, Lumma, ViperSoftX, Kematian Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

Cracking Open the Dual Weaknesses of Rockwell Automation's PanelView Plus

Eldorado: A New Ransomware Threat Targeting Windows and Vmware

CloudSorcerer APT: A Stealthy Cloud Threat Targeting Russia

Microsoft SmartScreen Flaw Used for Covert Stealer Deliveries

RCE Flaw in WordPress Calendar Plugin Puts 150,000 Sites at Risk

Microsoft’s July Patch Tuesday Addresses Active Zero-Day Exploits

Inside ViperSoftX: Exploiting AutoIt and CLR for Stealthy PowerShell Execution

Kematian: The Versatile Information-Stealing Malware

Critical GitLab Flaw Lets Attackers Hijack User Pipelines

CRYSTALRAY Threat Actor Employs OSS to Strike 1,500 Targets

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 threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Eldorado Ransomware	SHA256	1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b, 7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7, b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de, dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33, 8badf1274da7c2bd1416e2ff8c384348fc42e7d1600bf826c9ad695fb5192c74, cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7
	MD5	9d1fd92ea00c6eef88076dd55cad611e, 315a9d36ed86894269e0126b649fb3d6
	TOR Address	hxxp[:]//dataleakypypu7uwblm5kttv726l3iripago6p336xjnbstkjwrlnlid[.]onion
	Email	russoschwartz@onionmail[.]org
	IPv4	173[.]44[.]141[.]152
Lumma	SHA256	B1B8EA15E6BBFC7C38EB394D7E81A99A93689464FAF991D77E28722E5B0E4681, D9F6408B67628D5618A4FBABA97404AC55988633CCB2A02A09C95B0B134BAFC9, DD5B52A63E8A774C058E558AA7E983D6AA51F560BA3F01829287C4B85081B884, D856A66EA554538D421ABCEB2D304200537F5A268CBFDE8F52F41A0C048EDFDC,

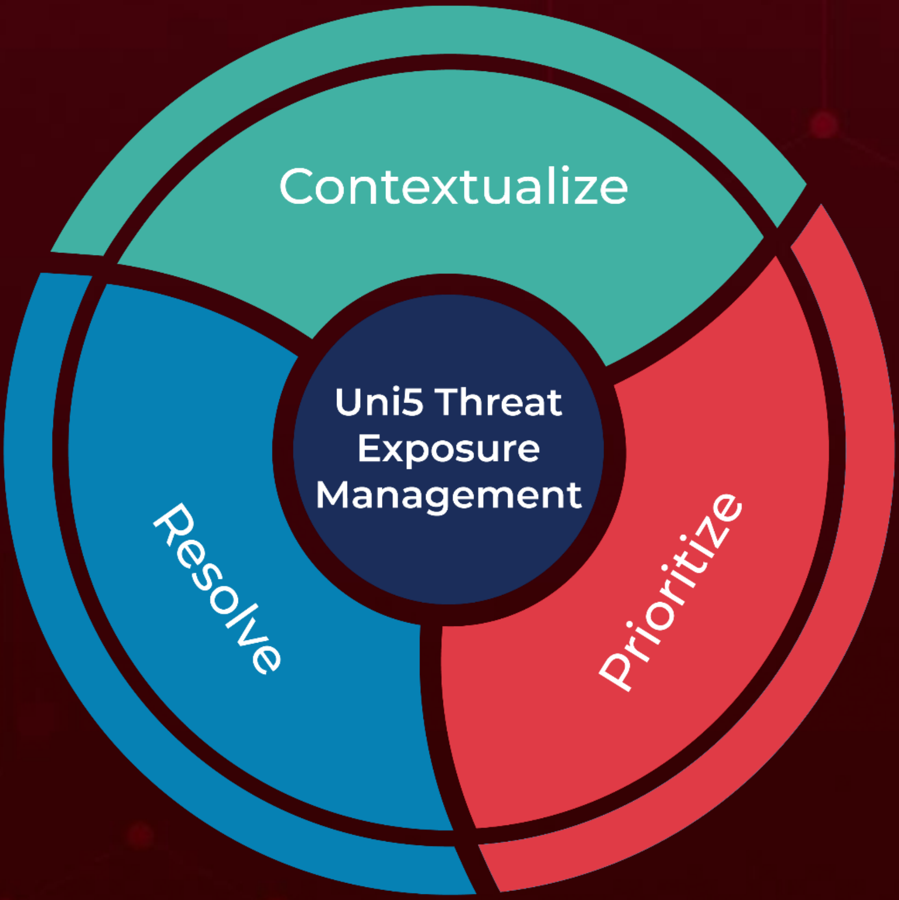
Attack Name	TYPE	VALUE
Lumma	SHA256	81B2DCBB79C2896141772043E55E5A6C667C16F4FA3E387AC308268C192F9C8A, D7A6D08355FD87431C3C0C6D68A41E925E707E06A33A2C51B3CBC8CF463B6C98, D17C03B595FD35D296CCB56BE6DED2C9D458695577EAA4B66BC42A99F08061E0, 0E922D6C34D784BE5BC4967AAD1D28A6A6651C6ACE414A7A25A508B15B163DCA, FB709C35CAB1CC48E1E723081CA5022510BFC413926E79E1D5A246CA243F97BA, E45BA4F91807634B98684857852FF1CCCB45A727286D22F9A29732804B1AC88C, D301CCB186D95CC6B08E1C6287C9884EDBE2C06625E119CD6305604F03FE9871, 266B3E9972AC9C25BD7312CCD28A598483F26261E882736A9518301AFF7559E5, DA1FF37345C1C448AF68615047659932A92BD6CC565F8DCEDB6C5C3FF89F091F, 4420D56E7D9699DC1962CB5504CD177D428AA1E2BFB96A77DFA455947D712CFE, 2E449F3F958BC7E68B7A18F6D9A62703D48646D315B3BC3751A979285468E30E, E843A9BD79891B33BC91AAA110B4F7A648FF73EE6CB8BAC04BBF5F2A685DECA3, 9F020143A87F223DE82B1204F9D7A154CD5974A68FDDD5CCFD2FEC93A18C93FB, 4DC5588AC49FA183824AB585B69A491FD45D1D3B2B01F052ADC5062B356E7434, A38B97CBCD242F41D9F05DA195E27F1AEC88689177E780E0BF7715CA62DA1DEC, 43C0C02903BFCE6E1B8FD95E53228823472F85E1A1F9C1312BF980E052A03AEA
Meduza	SHA256	643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2, d278aa079205cf4bb605de28bc6d6eca5a63b4cdd9d0c7488c40945d2b90b0a0, 44e715e3d9b5434c099452cc2cd991b1f02d4aba25114341a37dc142efd089ff, 9f2c70239fe518552ee44423564b075a85e0fc1e7bd80dc233bcc1f882ffceb9, b14af38c4230de20c7c4fefc1e3c5fffb1562bacedfebc56a508f55182a6fe88, 85b317bb4463a93ecc4d25af872401984d61e9ddcee4c275ea1f1d9875b5fa61,

Attack Name	TYPE	VALUE
Meduza	SHA256	2aa321a93bfa09139831e510e3cf9a869ece3d2e00889c846be169963cbb3b34, e29fa10b148be279c203e1f9079e7245b834f7912534c1bf4180af37686f621e, 73171634ceb5c5007cf78a6f32d6633590830f39f4e5311a4f323a4d44975ca7, cee2442ce10695e29830a77d38d4af1e24d6881203743664abc4ad9a8c97c0f2, 2ad84bfff7d5257fdeb81b4b52b8e0115f26e8e0cdaa014f9e3084f518aa6149, 114b868f319162c5d6ff92796e41910f54de0e89f895a066fd4980c6dba2e323, 478eb22a1f1be2ef6e70625cf42ca61c716389135acbb705c0e21f0cf330bf46, 811dbefc20a0a348038ef8f6adc70c38f9b778c20abfb85953a26dc6037a0cde, 62460105edf1636fd9605894deba01a417fcd8558c9a43ceefbf9fdda536a9c1, 4cfc33deeedcc336cc541b2a91eb666fdb2c8984c215daf8cee6ab793c9ef9d1, aa46a10b5392afadabb645417e88a32a95a82796b4b9517ea983ee589ed78ab6, Bded3addc990fa93827a6cfbf9687076df89cead996396e443d4465c4de43aba
ViperSoftX	SHA256	814297c47c67c82c4700ed0f099d558b8ac45e91cbb72d44a46c2e2a0c6b11aa, fef939b4a90ee28e2cffe1d8f0dcfc0d5dd174b0321e2a2c6cd46c65b7b79a2d, 779323771d4ebd97de44bdb9cb03e40156182b2012acfd444a4787902b0f1f35, 4d1ef869c4bddeccc318939ea2651ce5a3fc2e369ba44a2e24cb9b102ef2be19, d55aaa430ea18f3b85ccbfe2f34ce14b9b88d348d83e6c41d3aaea456b69b869
Kematian Stealer	SHA256	1c7424d6cbd0e5104151b6317b914a24992a9de9855d7ec4e0cd493fac0a3b98

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

July 15, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com