

Date of Publication
April 29, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

22 to 28 APRIL 2024

Table Of Contents

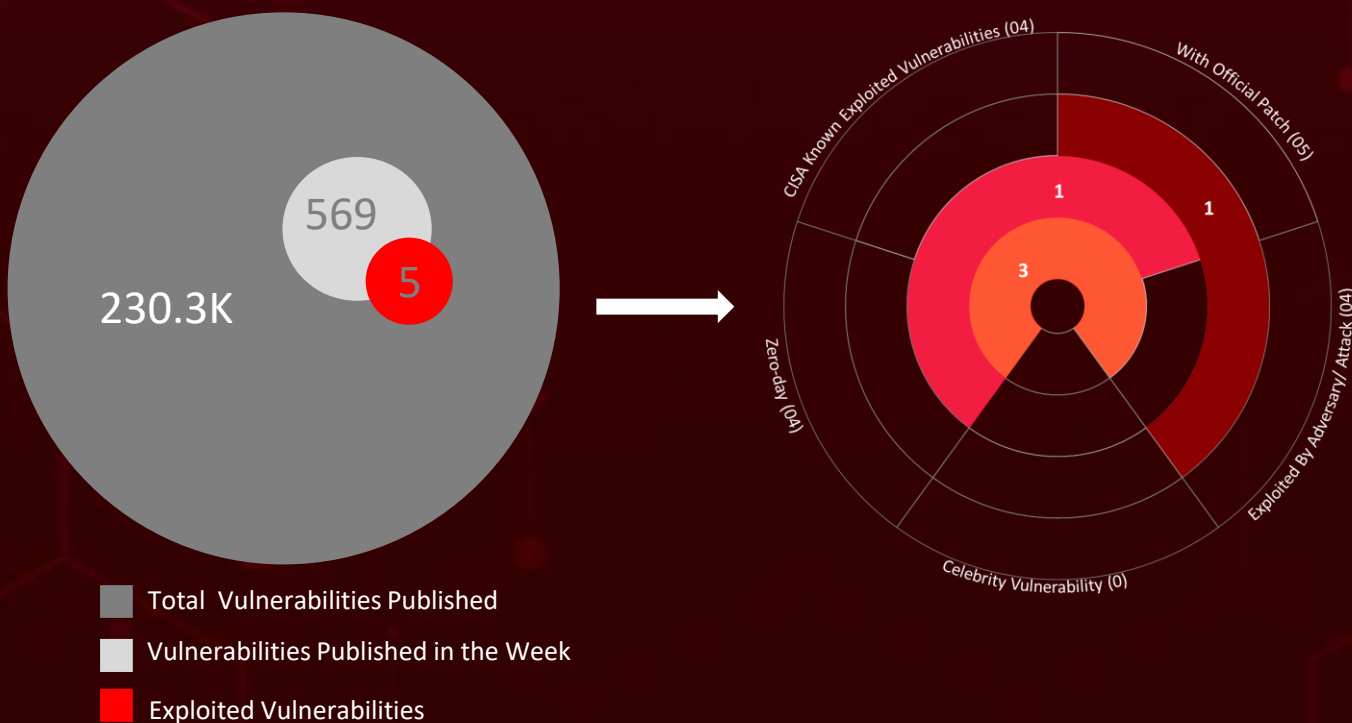
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	26

Summary

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

Furthermore, HiveForce Labs discovered that **APT28** threat actors are exploiting **CVE-2022-38028** a critical vulnerability in Microsoft Windows Print Spooler, allowing unauthenticated attackers to deploy GooseEgg Malware and move laterally within the network.

STORM-1849 has been orchestrating a campaign named ArcaneDoor targeting the Government, Critical Infrastructure, Telecommunication, Energy sectors worldwide. Their method involved targeting perimeter devices leveraging two zero-days **CVE-2024-20353** and **CVE-2024-20359** found within Cisco ASA and FTD firewalls. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

8

Attacks
Executed

5

Vulnerabilities
Exploited

5

Adversaries in
Action

- [Waterbear](#)
- [CR4T](#)
- [Cryptbot](#)
- [LummaC2](#)
- [Rhadamanthys](#)
- [GooseEgg](#)
- [KageNoHitobito](#)
- [DoNex](#)

- [CVE-2022-38028](#)
- [CVE-2024-20353](#)
- [CVE-2024-20359](#)
- [CVE-2024-4040](#)
- [CVE-2024-27956](#)

- [Earth Hundun](#)
- [ToddyCat](#)
- [CoralRaider](#)
- [APT28](#)
- [STORM-1849](#)



Insights

ArcaneDoor

Campaign orchestrated by STORM-1849, exploiting Cisco ASA and FTD flaws

WordPress Automatic Plugin Flaw

A critical SQL Injection vulnerability CVE-2024-27956 in WordPress allows attackers to create admin accounts, upload malicious files and take complete control

CVE-2024-4040

zero-day flaw in CrushFTP allows unauthenticated attackers to bypass the user's VFS

CVE-2022-38028

Flaw in Windows Print Spooler exploited by APT28 to deliver GooseEgg malware

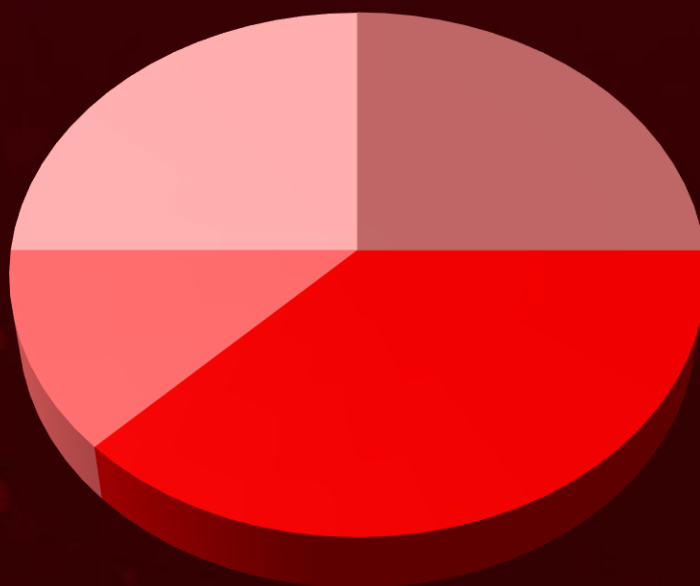
CoralRaider group

distributing three distinct stealers— CryptBot, LummaC2, and Rhadamanthys, in a persistent malware campaign

DuneQuixote Campaign

targeting Middle Eastern governments, deploying new backdoor named CR4T

Threat Distribution



■ Backdoor

■ Stealer

■ Loader

■ Ransomware

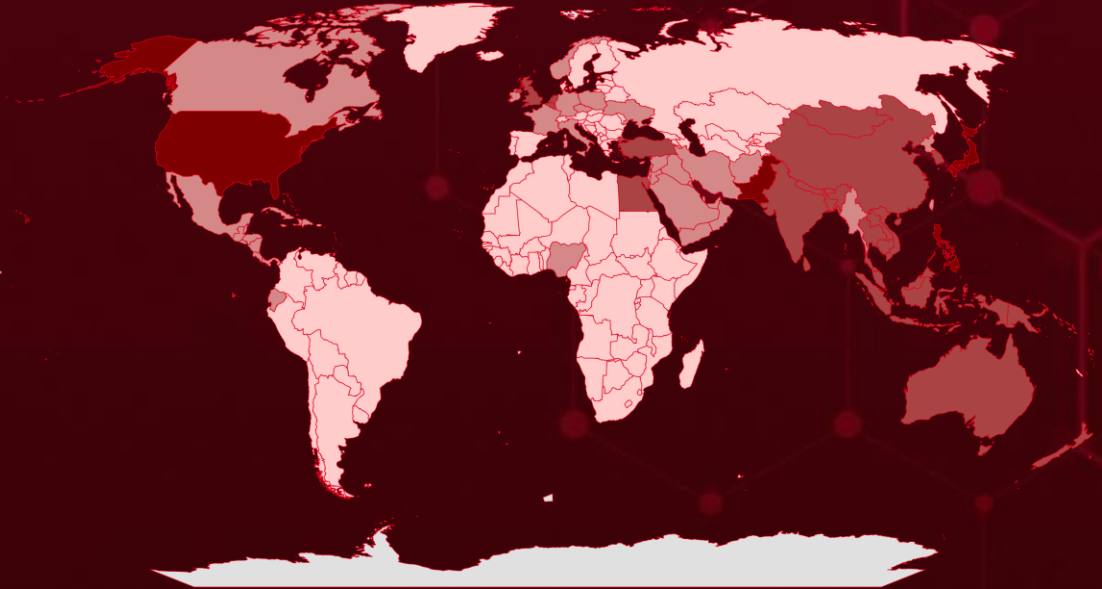


Targeted Countries

Most



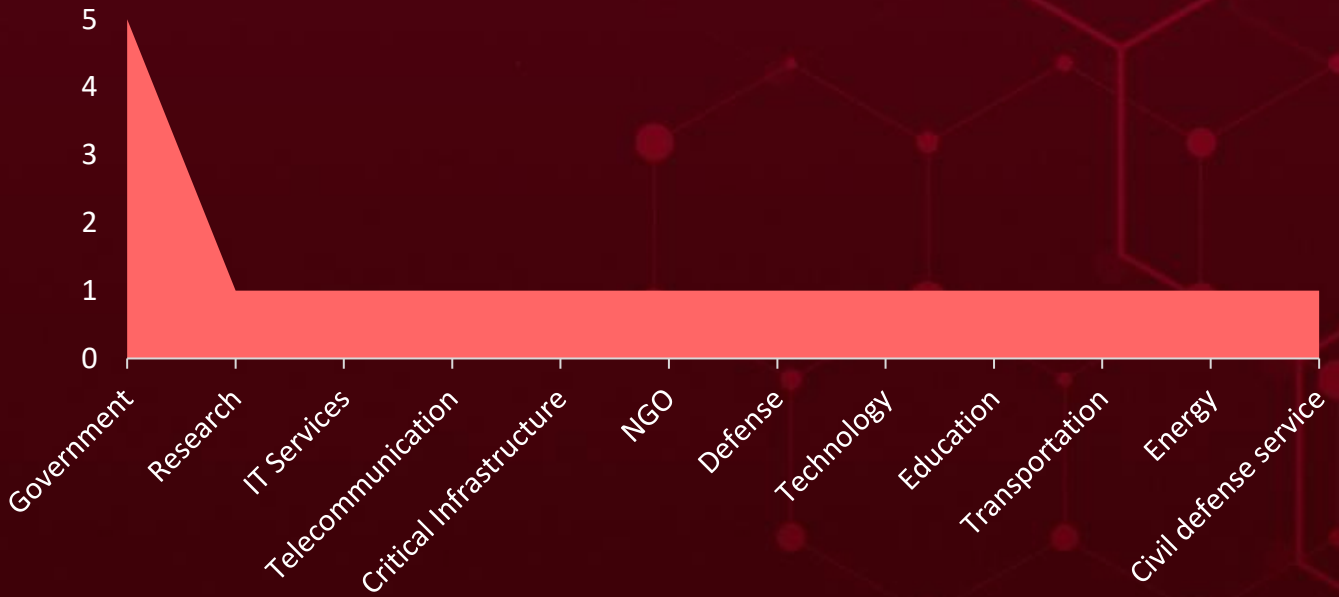
Least



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

Countries	Countries	Countries	Countries
Philippines	Laos	Cuba	Netherlands
Pakistan	Solomon Islands	Samoa	Taiwan
Japan	Timor-Leste	Cyprus	El Salvador
United States	Sri Lanka	Honduras	Iran
Marshall Islands	Tonga	Czech Republic	Nicaragua
Singapore	Bhutan	Barbados	Trinidad and Tobago
Bangladesh	Tuvalu	Dominica	Nigeria
Brunei	Turkey	Ireland	Israel
Thailand	Vietnam	Dominican Republic	North Korea
Cambodia	United Kingdom	Italy	United Arab Emirates
Nepal	Malaysia	Mexico	Norway
China	Vanuatu	France	Jamaica
Papua New Guinea	Qatar	Micronesia	Oman
Egypt	Ukraine	Germany	Lebanon
South Korea	Syria	Monaco	Yemen
Fiji	Canada	Poland	Afghanistan
Maldives	Panama	Ecuador	Luxembourg
India	Jordan	Saint Lucia	US Virgin Islands
Mongolia	Guatemala	Myanmar	Botswana
Indonesia	Bahamas	Saudi Arabia	Saint Vincent and the Grenadines
New Zealand	Iraq	Nauru	Burundi
Australia	Kuwait	Haiti	Cabo Verde
Palau	Bahrain	Belize	Russia
Kiribati	Costa Rica	Antigua and Barbuda	Austria
Belgium	Grenada		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1068

Exploitation for Privilege Escalation

T1041

Exfiltration Over C2 Channel

T1083

File and Directory Discovery

T1588.006

Vulnerabilities

T1082

System Information Discovery

T1055

Process Injection

T1140

Deobfuscate/Decode Files or Information

T1027

Obfuscated Files or Information

T1588

Obtain Capabilities

T1057

Process Discovery

T1053

Scheduled Task/Job

T1555

Credentials from Password Stores

T1036

Masquerading

T1105

Ingress Tool Transfer

T1071.001

Web Protocols

T1112

Modify Registry

T1584

Compromise Infrastructure

T1053.005

Scheduled Task

T1059.001

PowerShell

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Waterbear</u>	Waterbear has undergone more than 10 iterations since 2009, featuring a diverse range of measures to counter debugging, sandboxing, and conventional antivirus efforts. Waterbear employs a genuine executable to facilitate the loading of its proprietary DLL file.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Encrypt Data	PATCH LINK
Earth Hundun			
IOC TYPE	VALUE		
SHA256	e669aaf63552430c6b7c6bd158bcd1e7a11091c164eb034319e1188d43b5490c, 0da9661ed1e73a58bd1005187ad9251bcdea317ca59565753d86ccf1e56927b8, ca0423851ee2aa3013fe74666a965c2312e42d040dbfff86595eb530be3e963f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>CR4T</u>	The CR4T Backdoor is crafted with the main objective of providing attackers with access to a command-line console on the victim's system. Moreover, it enables the downloading, uploading, and alteration of files. This backdoor empowers attackers to run command lines on victims' machines, facilitating malicious actions such as file manipulation and data extraction.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Upload Files, data manipulation	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>Cryptbot</u>	CryptBot represents a common type of infostealer that specifically targets Windows systems. Its primary function is to pilfer sensitive data from compromised computers, including credentials from web browsers, cryptocurrency wallets, browser cookies, and credit cards. Additionally, it captures screenshots of the infected system.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			PATCH LINK
ASSOCIATED ACTOR			
CoralRaider	Data Theft	-	
IOC TYPE	VALUE		
SHA256	FF11E869A01559BF8B75131241B6CF5D670612D09F6EE89038486835F4B0FEAB, BACA9D0FDDDE0E897A98070E87D0529FB4FCD5BCD1F3584BB43281E61EE68352, 245C2379816C8AB8C0C83050DC7DA5375FC724788E6844540CF2BA537F6B727B		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>LummaC2</u>	LummaC2 is a widely known information stealer notorious for its efforts to gather data from victims' devices. Its initial exfiltration stage involves establishing a connection to the C2 server. If it fails to receive an "OK" response from any of the designated C2 servers, the malware will terminate the process. The subsequent step involves extracting information from compromised machines.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer			PATCH LINK
ASSOCIATED ACTOR			
CoralRaider	Steal data	-	
IOC TYPE	VALUE		
SHA256	65E1A8E550DF1000EB91A7B679CF586EFAB0F24385B810F50349D50EB80AE806, 5ECAFA1ECBC54D9A7B0E2E5C646578057215A246AECC2132FE7605A078AA43EC, D0E7A341FE199DBABB5F0798DBA0564E9B60E4736A405C46EAF7232CC10DC40		

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>Rhadamanthys</u>	Rhadamanthys is an information stealer coded in C++ that surfaced in August 2022. It focuses on acquiring credentials for email accounts, FTP servers, and online banking services.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
CoralRaider			-
IOC TYPE	VALUE		
SHA256	B9AD234ABEB1490F2C2D28DD2387F0575BA5128EBB799741B1F3179622204175, 7FAEB3F847830A2C52322565D8E73E07000003CCB54310790E10756CD3B2FF6B, C7CA2F9065557A6D8FB0C02C75804D386B77FFCA4466678B201C09E916AFA096		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>GooseEgg</u>	GooseEgg is a launcher application with the ability to carry out multiple malicious actions, operating with SYSTEM-level permissions. These actions include remote code execution and lateral movement within compromised networks.	Exploiting Vulnerabilities	CVE-2022-38028
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Code Execution	Windows
ASSOCIATED ACTOR			PATCH LINK
APT28			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-38028
IOC TYPE	VALUE		
SHA256	c60ead92cd376b689d1b4450f2578b36ea0bf64f3963cfa5546279fa4424c2a5, 6b311c0a977d21e772ac4e99762234da852bbf84293386fbe78622a96c0b052f		




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>KageNoHitobito</u>	KageNoHitobito ransomware is specifically engineered to encrypt files solely on the local drive, excluding networked drives from its encryption process. Encrypted files are marked with a ".hitobito" extension.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt data	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	8939bfe20bc6476806d22c8edfcaba5c36f936b893b3de1c847558502654c82f, 1940fdb2561c2f7b82f6c44d22a9906e5ffec2438d5dadfe88d1608f5f03c33, 506e8753dd5ca1c8387be32f26367e26f242b7c65e61203f7f926506c04163aa,		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>DoNex</u>	DoNex ransomware employs encryption mechanisms on both local drives and network shares, as indicated by the settings of <local_disks> and <network_shares> being set to true. Affected files have a victim ID appended as a file extension, and their file icons are altered by the ransomware.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca, 6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40, b32ae94b32bcc5724d706421f915b7f7730c4fb20b04f5ab0ca830dc88dcce4e		




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


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


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


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

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p>Earth Hundun (aka BlackTech, Circuit Panda, Radio Panda, Palmerworm, TEMP.Overboard, T-APT-03, Red Djinn, Manga Taurus)</p>	China	Technology, Research, Government, Construction, Financial, Healthcare, Media	China, Hong Kong, Japan, Taiwan, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	Waterbear backdoor	-	
TTPs			
TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1129: Shared Modules; T1106: Native API; T1574.002: DLL Side-Loading; T1547.012: Print Processors; T1027.001: Binary Padding; T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1497.003: Time Based Evasion; T1622: Debugger Evasion; T1083: File and Directory Discovery; T1016.001: Internet Connection Discovery; T1049: System Network Connections Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1012: Query Registry; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1071.001: Web Protocols; T1573: Encrypted Channel; T1132.002: Non-Standard Encoding			

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

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


TTPs

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

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>APT28 (aka Sofacy , Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)</u></p>	Russia	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Energy, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Saudi Arabia, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO and APEC and OSCE.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs		
	CVE-2022-38028	GooseEgg	Microsoft Windows Print Spooler

TTPs

TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0002: Execution; TA0007: Discovery; TA0042: Resource Development; TA0008: Lateral Movement; TA0005: Defense Evasion; T1112: Modify Registry; T1559.001: Component Object Model; T1559: Inter-Process Communication; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1588: Obtain Capabilities; T1083: File and Directory Discovery; T1588.006: Vulnerabilities; T1588.005: Exploits; T1584: Compromise Infrastructure; T1555: Credentials from Password Stores; T1068: Exploitation for Privilege Escalation; T1574.006: Dynamic Linker Hijacking; T1574: Hijack Execution Flow

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

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **Earth Hundun, ToddyCat, CoralRaider, APT28, STORM-1849** and malware **Waterbear backdoor, CR4T, Cryptbot, LummaC2, Rhadamanthys, GooseEgg, KageNoHitobito ransomware, DoNex Ransomware**.

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 **five exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Earth Hundun, ToddyCat, CoralRaider, APT28, STORM-1849** and malware **CR4T, Cryptbot, LummaC2, Rhadamanthys, GooseEgg, KageNoHitobito, DoNex Ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

[Earth Hundun's Deuterbear Sets Sights on High-Value Sectors](#)

[Middle East Targeted with CR4T Malware in DuneQuixote Campaign](#)

[Over 300k WordPress Sites Affected by Forminator Plugin Flaws](#)

[ToddyCat's Toolkit and Tactics Fueling Data Theft](#)

[CoralRaider's Malware Campaign Distributing Stealers Via CDN Cache](#)

[APT28 Exploits Windows Print Spooler Flaw with GooseEgg](#)

[ArcaneDoor a Novel Espionage Campaign Exploits Cisco Zero-Days](#)

[A Zero-Day Vulnerability in CrushFTP Results in Server Compromise](#)

[KageNoHitobito and DoNex Ransomware Plaguing Global Entities](#)

[Active Targeting of WP-Automatic Plugin Flaw Raises Concerns for Site Takeover](#)

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	TYP E	VALUE
Waterbear	SHA256	e669aaf63552430c6b7c6bd158bcd1e7a11091c164eb034319e1188d43b5490c, 0da9661ed1e73a58bd1005187ad9251bcdea317ca59565753d86ccf1e56927b8, ca0423851ee2aa3013fe74666a965c2312e42d040dbfff86595eb530be3e963f, 6dcc3af7c67403eaae3d5af2f057f0bb553d56ec746ff4cb7c03311e34343ebd, ab8d60e121d6f121c250208987beb6b53d4000bc861e60b093cf5c389e8e7162, a569df3c46f3816d006a40046dae0eb1bc3f9f1d4d3799703070390e195f6dd4, e483cae34eb1e246c3dd4552b2e71614d4df53dc0bac06076442ffc7ac2e06b2, c97e8075466cf91623b1caa1747a6c5ee38c2d0341e0a3a2fa8fcf5a2e6ad3a6, 6b9a14d4d9230e038ffd9e1f5fd0d3065ff0a78b52ab338644462864740c2241
Cryptobot	SHA256	FF11E869A01559BF8B75131241B6CF5D670612D09F6EE89038486835F4B0FEAB, BACA9D0FDDDE0E897A98070E87D0529FB4FCD5BCD1F3584BB43281E61EE68352, 245C2379816C8AB8C0C83050DC7DA5375FC724788E6844540CF2BA537F6B727B, D80B49455C86BB748C2B4D006443E73FB107F4CDFEE298991BB526BF9A6FA464, D4036C235FCA73A67732D884564991184B7A8EA148784F0CD70FA07ADBD8E160, B840500C7985E9A0DB4FAF55F633A1F0FC4A1F52344791B13E14B8FAFC8FFAB, 1DDBD0850493C851AB3503B8AF24118E2F4C0441A997436D13FB5596F96178EB, E8221B90D1CCC9761383DE1DAF68F7025FE9D38A4C5BFB6EF8DE71C525D53FE9, E41202C14467AC53D72BE5754802CE73A07C605C7159D4F65E0B9CDA1E36A836, 183F842CE161E8F0CCE88D6451B59FB681AC86BD3221AB35BFD675CB42F056AC, 91A270A7E220EAD2D197732A5C0F08F1186AD7EF53BDB11749FF014AFC5FFE48, EBCD03FB51CF4AB8CD5636F1894276886E64014F3AB8C0468A9E528073931F08, 24336A3C69F863981DF13CC9C2CC8FE002D642962FC1D12C87062A8E5D273889, F4D74FDB147B02ED456DA86058C56F78708FD386EF6B893795BC44A8AFA42E9C, F667AB33B49D8B8389E116A05849032CC2E78A7578B12CDD07ED89A931C3C464, B4CAEA526BAC33E9A0F02A6CD303A5EFC557C21CB44814C096C755E4C1AF0C98, F971BC6B48B1B12ABE708F9CFA090E8A22111B689549F46B6010E30153B1467E, BDCE60E92616F204631EBAC6D57C74FD2214C9591C6FAA2A76150C6AC15C6AC0, F5525DA97ACAB586AD247CCC199D0D6FA6487F9B7F4BB66E36FAF52BE1A8D9F1, CB3B9C473954B995C70BE161F1332AAE47E1E0BDD5BE80DDFE7AF9B76CECB7A2

Attack Name	TYPE	VALUE
<u>LummaC2</u>	SHA256	<p>65E1A8E550DF1000EB91A7B679CF586EFAB0F24385B810F50349D50 EB80AE806, 5ECAFA1ECBC54D9A7B0E2E5C646578057215A246AEEC2132FE7605A 078AA43EC, D0E7A341FE199DBABB5F0798DBA0564E9B60E4736A405C46EAF723 2CC10DC40, 8A80210B1F6382CDBFF2AFC0C9A30092FC13687A33F293E36A9DBC0 263A45101, A90294B602B51FFF7B04E72DEEB3E88FB200272321C939F00E13BDE1 D49FF1A3, 257BCB2BAC99FE5E876857EC4511CADA759E7F515DE629E43CBB0F8 39575E7FC, 8BFDD127054E1EE93F58148677961929BB9265BB6BA9648F517118C 1DFCA6504, 78785AB759DD61F4A9FB561FAEF90234FB0A78696523D1DF53312C7 A3EFF99FE, A4EA760306249B07D5AF054B5FC82D5FD9DCAB5E5CB6EAB3C8E8EB 9132EBF882, 3D1D2E2B702D493DDAAD5D7DEB780EE227EB24438E68B499839A47 22E212F8FB, 1BE53A1BC4D191E139AFB7C053B8F54AF43C0338FF1EEE40CD1486D FE5B787B1, D0130399FD404226AE5B90897E8E3AFFE29B7D34081EE1BF11ECB37 50CA342C5, D932EE10F02EA5BB60ED867D9687A906F1B8472F01FC5543B06F9AB 22059B264, E4D5B043F5C9E0894A5F4A21C93CD7347A609A900DA8F56F55A0DD 84269E81F1, CE00C5433FB2481534577E90B23E61B164654AD41C5A0F14BA59735 ED637E326, 4DC5588AC49FA183824AB585B69A491FD45D1D3B2B01F052ADC506 2B356E7434, 984A58B77A8657D009B7867D392F320F65BB8CB72B63D9960A90F5 A94721F8FB, 43D0CFCE7AB2B0C2F6F89F0FA93083F46F290047CEF0F75A0AE3A0B8 742D84D8, DE6C4C3DDB3A3DDBCBEA9124F93429BF987DCD8192E0F1B4A82650 5429B74560, 77460056386F07D96908455241B15091C3EDEC9FD55FBF6CE7F3A0 61C7AC5CD</p>
<u>Rhadamanth</u> <u>vs</u>	SHA256	<p>B9AD234ABEB1490F2C2D28DD2387F0575BA5128EBB799741B1F317 9622204175, 7FAEB3F847830A2C52322565D8E73E07000003CCB54310790E10756 CD3B2FF6B,</p>

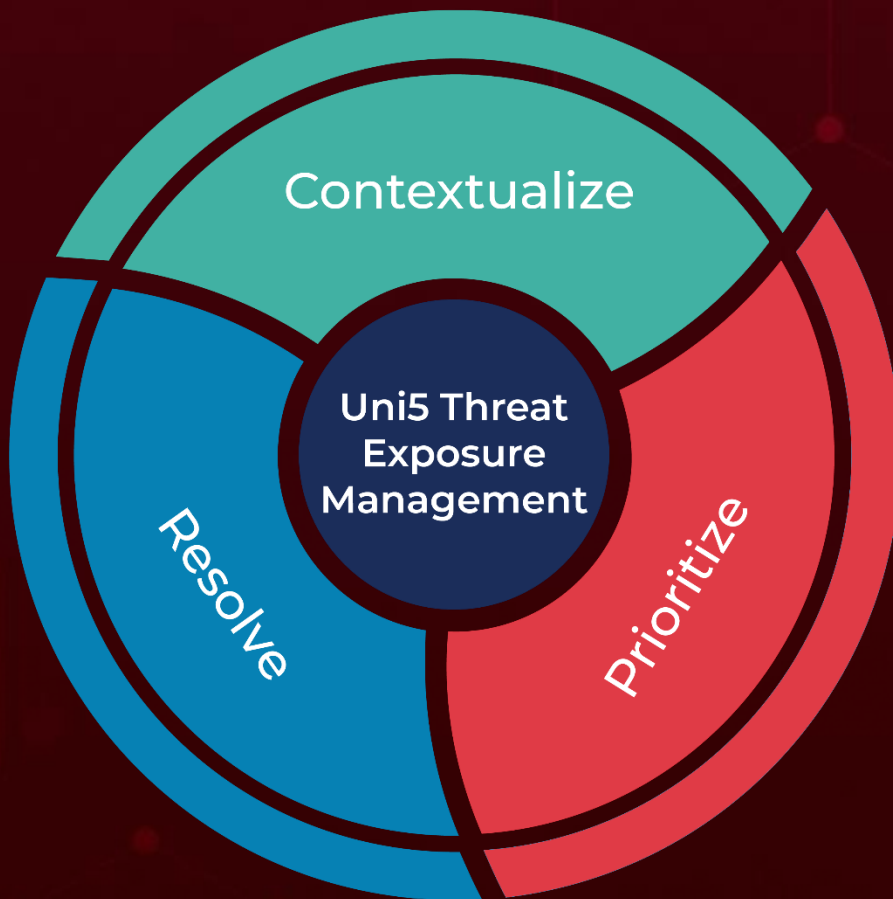
Attack Name	TYPE	VALUE
<u>Rhadamanth</u> <u>ys</u>	SHA256	C7CA2F9065557A6D8FB0C02C75804D386B77FFCA4466678B201C09E916AFA096, A432BF6943599E53A12D5615F91FE3D636A6820073B60A7068FA9508849806B4, 30B5B1D6877DF251F4007725DF4E043F704D80A55B4EBD7C952B4F24B7806712, 8404CB4A740D169256E49E3A22B2AF1A61B2606E71CDCA4F39DEECCD5D461C91,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

Attack Name	TYPE	VALUE
<u>KageNoHitobito</u>	SHA256	8939bfe20bc6476806d22c8edfcaba5c36f936b893b3de1c847558502654c82f, 1940fcdb2561c2f7b82f6c44d22a9906e5ffec2438d5dadfe88d1608f5f03c33, 506e8753dd5ca1c8387be32f26367e26f242b7c65e61203f7f926506c04163aa, 8a10e0dc4994268ea33baecd5e89d1e2ddabef30afa09961257a4329669e857a, bec9d2dcd9565bb245f5c8beca4db627390bcb4699dd5da192cc8aba895e0e6a

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

April 29, 2024 • 7:20 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com