Date of Publication
September 18, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

11 to 17 SEPTEMBER 2023

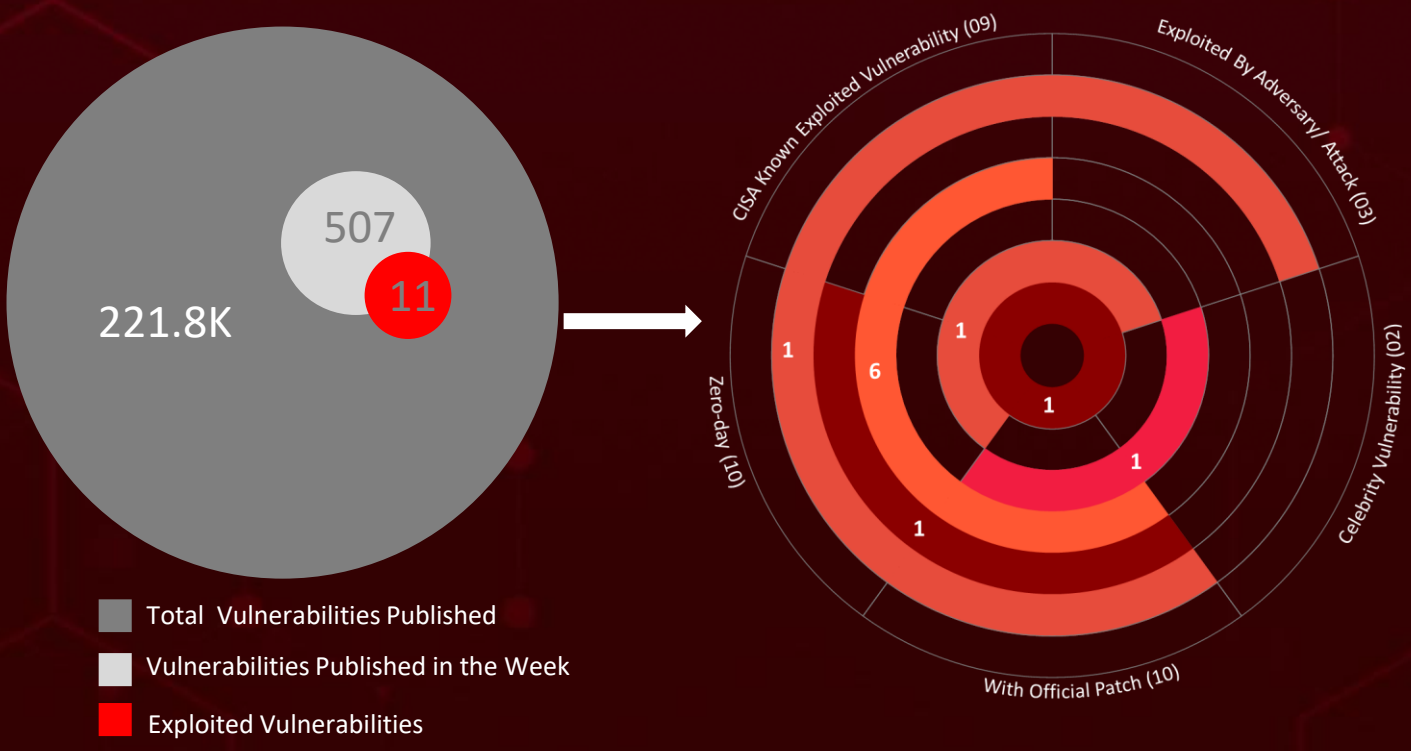
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, a total of **eight** attacks were executed, along with **eleven** vulnerabilities discovered, and **two** different adversaries were identified, all of which underscore the ever-present danger of cyberattacks.

Moreover, HiveForce Labs discovered that the **Cisco zero-day** vulnerability was exploited by the **Akira Ransomware** threat actors, playing a pivotal role in breaching corporate networks and leveraging tools like RustDesk for stealthy access. Additionally, identified **zero-days** in **Google**, **Adobe Acrobat**, **Apple**, and **Microsoft**.

In the meantime, **Charming Kitten** orchestrated a sophisticated campaign employing the **Sponsor** backdoor, targeting **34** diverse entities across Brazil, Israel, and the United Arab Emirates. **Storm-0324** exploited a **Microsoft Teams zero-day** to deploy **JSSLoader**. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

8
Attacks Executed

11
Vulnerabilities Exploited

2
Adversaries in Action

- Akira Ransomware
- HijackLoader
- PhoenixMiner
- lolMiner
- M3_Mini_Rat
- Sponsor Backdoor
- 3AM Ransomware
- JSSLoader

- CVE-2023-20269
- CVE-2023-4863
- CVE-2021-26855
- CVE-2023-26369
- CVE-2023-36761
- CVE-2023-36802
- CVE-2023-41064
- CVE-2023-41061
- CVE-2023-3676
- CVE-2023-21715
- CVE-2023-38146

- Charming Kitten
- Storm-0324

Insights

The Malware Kingpin: HijackLoader's Meteoric Ascent in Cybercriminal Circles

LockBit's Miss and 3AM's Bliss: The Unpredictable Journey of 3AM Ransomware Arising from a Rogue Attack by an Affiliate.

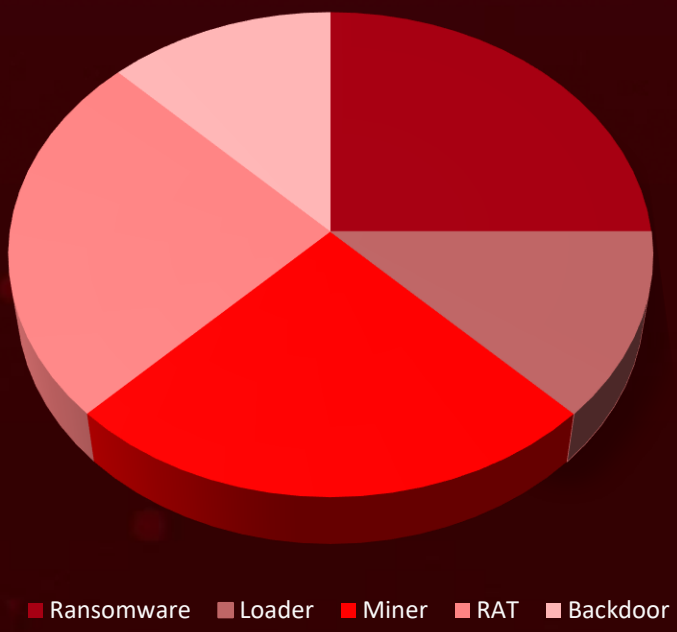
CVE-2023-20269: Akira Ransomware Strikes Gold with Cisco VPN Vulnerability

34 Firms on Alert: Charming Kitten's 'Sponsor' Revelation Shakes Brazil, Israel, and the United Arab Emirates.

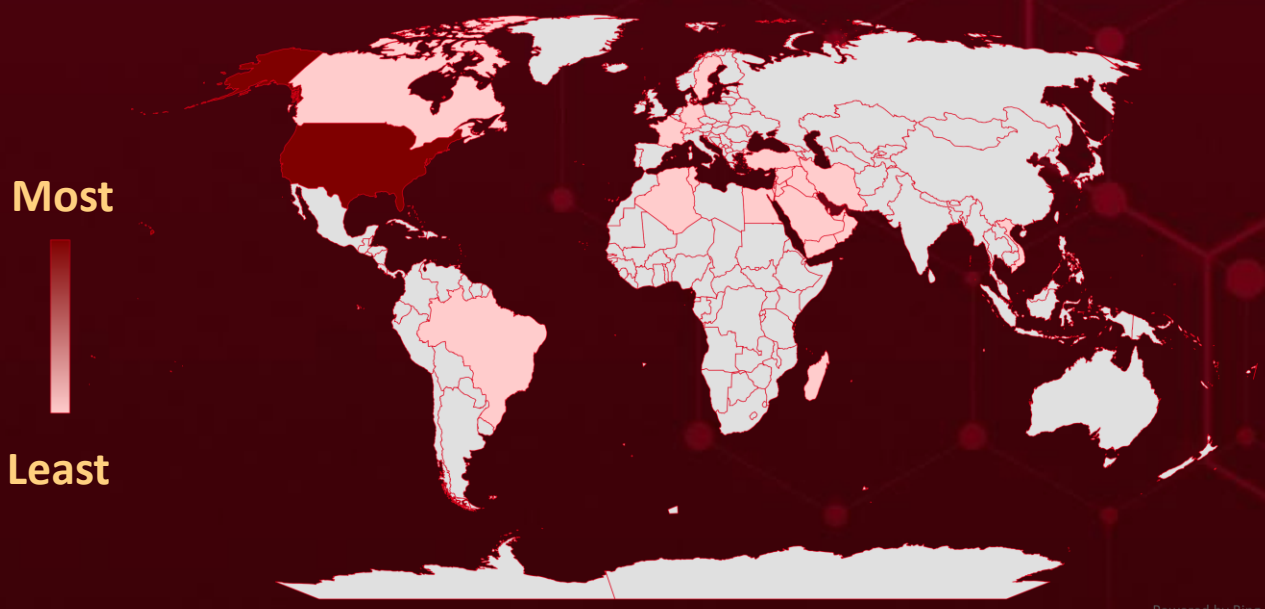
Unveiling the Storm-0324 Collaboration: The Mastermind Behind Ransomware, Its Connection with FIN7, and Network Breaches

ThemeBleed Strikes Windows 11: Code Execution Threat Unleashed

Threat Distribution



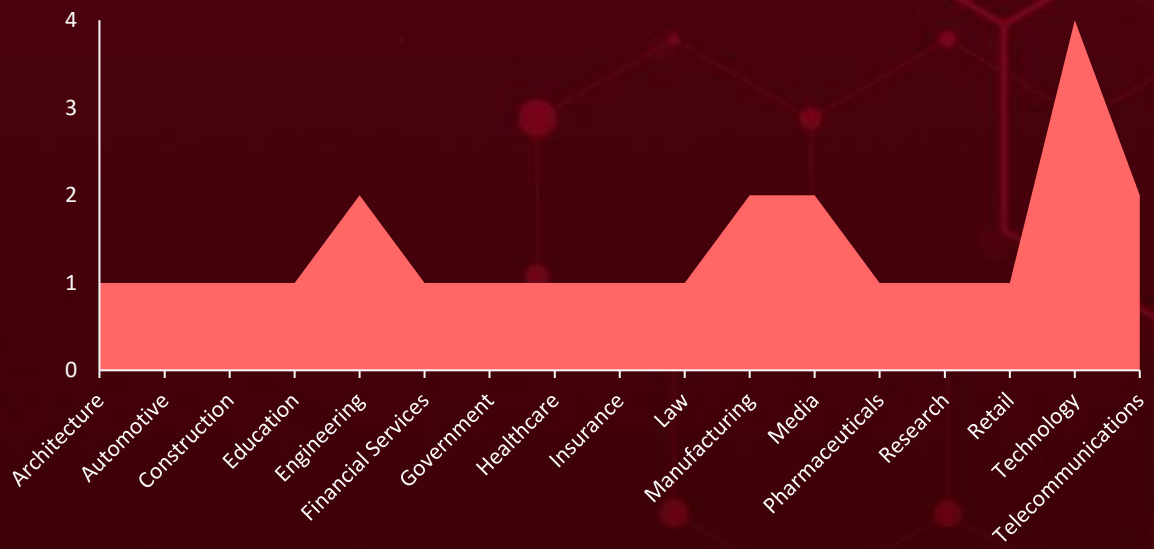
Targeted Countries



	Countries
	US
	Saudi Arabia
	Akrotiri and Dhekelia
	Algeria
	Syria
	Bahrain
	Palestine
	Brazil
	Sweden
	Canada
	Turkey
	Cyprus
	Yemen
	Egypt
	Oman

	Countries
	France
	Qatar
	Germany
	Singapore
	Iran
	Switzerland
	Iraq
	Tunisia
	Israel
	United Arab Emirates
	Jordan
	Vietnam
	Kuwait
	Lebanon
	Madagascar

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1203** Exploitation for Client Execution	**T1588.005** Exploits	**T1068** Exploitation for Privilege Escalation
T1204 User Execution	**T1027** Obfuscated Files or Information	**T1566** Phishing	**T1543.003** Windows Service	**T1588.006** Vulnerabilities
T1036 Masquerading	**T1055** Process Injection	**T1569.002** Service Execution	**T1083** File and Directory Discovery	**T1548** Abuse Elevation Control Mechanism
T1018 Remote System Discovery	**T1566.002** Spearphishing Link	**T1059.001** PowerShell	**T1078.003** Local Accounts	**T1204.002** Malicious File

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira Ransomware	Akira, a relatively new ransomware operation, emerged in March 2023 and is written in C++. It has expanded its tactics by adding a Linux encryptor to target VMware virtual machines. The Akira ransomware group targets Cisco VPN products to breach corporate networks and leverages tools like RustDesk for stealthy access.	Cisco VPN products	CVE-2023-20269
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Extortion of data and Financial Loss	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)
ASSOCIATED ACTOR			**Workaround**
-			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc
IOC TYPE	**VALUE**		
IPv4	161.35.92[.]242, 173.208.205[.]10, 185.157.162[.]21		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HijackLoader	A new malware loader, HijackLoader, is swiftly gaining prominence within the cybercriminal sphere, being leveraged to disseminate an array of malicious malware strains, including DanaBot, SystemBC, and RedLine Stealer.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft and compromised systems	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	7bd39678ac3452bf55359b44c5192b79412ce61a82cd72eef88f91aba5792ee6, 6b1621bded06b082f83c731319c9deb2fdf751a4cec1d1b2b00ab9e75f4c29ca, e67790b394f5238908fcc326a9db940b200d9b50cbb45f0bfa94038db50beeae		

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
PhoenixMiner	PhoenixMiner Ethereum cryptocurrency mining malware with the filename "svhost.exe". PhoenixMiner is a publicly available miner that relies on the GPU capabilities of computers. The PowerShell launcher executes PhoenixMiner with the Ethereum Classic mining parameters from the victim machine's Windows systems folder.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3, c7e1aa53dc667581f37bcbd0793c2ef909e8a4461c59641cb2c672ebe192609c, 201a1979e02bcaa2808e31613a0bef99ad55d514fcaed973840a1bf1efdb4cbe, f4b1dc6456aed765e11878c6a5b9555ee2aec1737219137d187e480599e254c9, d241ef2a157f44dcc323279bd89168c0f6b142de964815ceb0429181eae9a789		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
lolMiner	lolMiner mines cryptocurrency by stealing the computational power of AMD, Nvidia, and Intel graphics cards. lolMiner is compatible with a variety of protocols, including Etchash, Autolykos2, Beam, Grin, Ae, ALPH, Flux, Equihash, Kaspa, Nexa, Ironfish, and others. This campaign's lolMiner version is 1.76, which allows for the simultaneous mining of two different cryptocurrencies.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73, aafe94fe2ca6210fde8f5691c066dc128090b097a7d45a69d7ccc977891e08b4, 8ebe85fd149f9b1e93668a733182ad6e0cafd1a0b285800e4e6b226b8673cbaa, ac1af3a386b2dcf0e2a2955101dc91de7f5e62c900ba4476b0b842d1aa951bbe, 2c049deedbc83923abdd41580faa07c98037f09b5fabe98f97a9239a0b6e3542		

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
M3_Mini_Rat	The M3_Mini_Rat client stub is a PowerShell script that allows the attacker to create a backdoor as well as download and execute other threats. The M3_Mini_Rat payload grants the attackers remote access, allowing them to conduct system reconnaissance.	Malicious Installer	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sponsor	The Sponsor backdoor, written in C++, collects host information and executes commands from a remote server. It uses Windows APIs to retrieve current usernames and collect system data such as operating system build and power source status, which is then sent to the command-and-control server through port 80.	Exploiting well-documented vulnerabilities	CVE-2021-26855
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, compromised systems and Espionage	Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINKS**
Charming Kitten			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855
IOC TYPE	**VALUE**		
SHA1	098b9a6ce722311553e1d8ac5849ba1dc5834c52, 5aee3c957056a8640041abc108d0b8a3d7a02ebd, 764eb6ca3752576c182fc19cff3e86c38dd51475, 2f3eda9d788a35f4c467b63860e73c3b010529cc, e443dc53284537513c00818392e569c79328f56f		

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
3AM Ransomware	'3AM,' a new ransomware outbreak, is a 64-bit executable written in the Rust computer language. It was recently discovered in a cyberattack carried out by a ransomware affiliate. When the encryption process begins, the 3AM ransomware disables numerous services on the infected system. It then appends the '.threeamtime' extension to the encrypted files.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JSSLoader (aka Anunak)	JSSLoader is a remote access Trojan (RAT) with .NET and C++ variations that the threat actors have used since at least 2020. The JSSLoader malware provides access to ransomware-as-a-service (RaaS). When JavaScript is launched, a JSSLoader variation DLL is dropped.	Spearphishing Link	CVE-2023-21715
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	Microsoft Teams
ASSOCIATED ACTOR			**PATCH LINKS**
Storm-0324			https://msrc.microsoft.com/update-guide/en-us/advisory/CVE-2023-21715
IOC TYPE	**VALUE**		
SHA256	48053356188dd419c6212e8adb1d5156460339f07838f2c00357cfd1b4a05278, da480b19c68c2dee819f7b06dbfdba0637fea2c165f3190c2a4994570c3dae2a, 910b6f3087b1d5342a2681376c367b53e30cf21dd9409fb1000ffb60893a7051, de099bf0297de8e2fad37acc55c6b0456d1fd98a6fc1fbc381759e82a4e207c3		

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-2023-20269	✗	Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:h:cisco_systems:asa:6.2.3:*:*:*:*:*:*:* cpe:2.3:h:cisco_systems:firepower:6.2.3:*:*:*:*:*:*:*	Akira Ransomware
Cisco Brute Access Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**WORKAROUND**
	CWE-288	T1110: Brute Force,T1059: Command and Scripting Interpreter,T1059.008: Network Device CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC#workarounds

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38146	ThemeBleed	Windows 11 version 21H2, Windows 11 version 22H2	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows_11_21h2:*:*:*:*:*:*:*:*	-
Microsoft Windows Themes Remote Code Execution Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-20	T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1027: Obfuscated Files or Information	https://msrc.microsoft.com/CVE-2023-38146

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4863		Google Chrome version 116.0.5845.186 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Heap Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-122	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	Charming Kitten
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	Sponsor Backdoor
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1090: Proxy,T1135: Network Share Discovery,T1005: Data from Local System,T1133: External Remote Service	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-26369</td><td>  </td><td rowspan="2">Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions,Acrobat Reader 2020, 20.005.30516 (Mac), 20.005.30514 (Win) and earlier versions</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:adobe:adobe_reader:23.003.20284:*:*:*:*:*:*:* cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Adobe Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-787</td><td>T1203: Exploitation for Client Execution,T1588: Obtain Capabilities,T1588.005: Exploits,T1204: User Execution, T1204.002: Malicious File</td><td>https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#classic-track</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36761	✗	Microsoft Office: 365 - 2019, Microsoft Word: before 16.0.5413.1000, Microsoft 365 Apps for Enterprise: before 16.0.5413.1000	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_word:-:*:*:*:*:*:*:*	-
Microsoft Word Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1588.006: Vulnerabilities,T1068: Exploitation for Privilege Escalation,T1203: Exploitation for Client Execution, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36761

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36802	✗	Windows: 10 - 11 22H2, Windows Server: 2019 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_streaming_service:-:*:*:*:*:*:*:*	-
Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1588: Obtain Capabilities,T1588.005: Exploits,T1059: Command and Scripting Interpreter,T1588.006: Vulnerabilities,T1068: Exploitation for Privilege Escalation,T1203: Exploitation for Client Execution, T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41064	✗ ZERO-DAY	Apple iOS, iPadOS, and macOS	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-120	T1204: User Execution,T1204.002: Malicious File,T1588: Obtain Capabilities,T1588.005: Exploits,T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1204.003: Malicious Image	https://support.apple.com/en-us/HT213905 https://support.apple.com/en-us/HT213906

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41061	✗ ZERO-DAY	Apple iOS, iPadOS, and watchOS	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1204: User Execution,T1204.002: Malicious File,T1588: Obtain Capabilities,T1588.005: Exploits,T1203: Exploitation for Client Execution,T1588.006:Vulnerabilities,T1204.003: Malicious Image	https://support.apple.com/en-gb/HT213907 https://support.apple.com/en-us/HT213905

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3676	✗	kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:kubernetes:-:*:*:*:*:*:*:*	-
Kubernetes Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1609: Container Administration Command,T1610: Deploy Container,T1059: Command and Scripting Interpreter,T1059.001: PowerShell,T1548: Abuse Elevation Control Mechanism,T1068: Exploitation for Privilege Escalation	https://kubernetes.io/releases/patch-releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21715	✗	Microsoft Teams	Storm-0324
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:*:*	JSSLoader
Microsoft Office Publisher Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-863	T1059: Command and Scripting Interpreter,T1040: Network Sniffing,T1203:Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Charming Kitten (aka Ballistic Bobcat, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, Charming Kitten, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, MintSandstorm)	Iran	Automotive, Communications, Engineering, Financial Services, Healthcare, Insurance, Law, Manufacturing, Retail, Technology, Telecommunications, Research, Education, Government, Media, and Pharmaceuticals	Brazil, the Middle East, and the United States.
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2021-26855	Sponsor Backdoor	Microsoft Exchange Server

TTPs
T1595: Active Scanning; T1587.001: Malware; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1059.003: Windows Command Shell; T1569.002: Service Execution; T1543.003: Windows Service; T1078.003: Local Accounts; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1555.003: Credentials from Web Browsers; T1018: Remote System Discovery; T1001: Data Obfuscation

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0324 (aka DEV-0324)	Unknown	IT, Technology, High-Tech	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-21715	JSSLoader	Microsoft Teams

TTPs
T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1204: User Execution; T1204.001: Malicious Link; T1203: Exploitation for Client Execution

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eleven exploited vulnerabilities** and block the indicators related to the threat actors **Charming Kitten, Storm-0324,** and malware **Akira Ransomware, HijackLoader, PhoenixMiner, lolMiner, M3_Mini_Rat, Sponsor Backdoor, 3AM Ransomware, JSSLoader**.

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 **eleven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Charming Kitten, Storm-0324,** and malware **Akira Ransomware, HijackLoader, PhoenixMiner, lolMiner, M3_Mini_Rat, Sponsor Backdoor, 3AM Ransomware, JSSLoader** in Breach and Attack Simulation(BAS).

Threat Advisories

Akira Ransomware Exploits Cisco Zero-Day Vulnerability

HijackLoader a Deceptive Modular Malware Loader

Google Addresses Fourth Zero-Day Flaw Exploited by Attackers Wildly

Cybercriminals Target Graphic Designers with Cryptojacking Malware

Charming Kitten's 'Sponsor' Strikes 34 Organizations in Brazil, Israel, and U.A.E

Adobe Acrobat Zero-Day Exploited in Wild

Microsoft’s September 2023 Patch Tuesday Addresses Two Zero-day Vulnerabilities

3AM Ransomware: LockBit's Failed Standoff Revealed

Apple Addresses Two Zero-Day Flaws Exploited by Attackers

Proof-of-Concept Released for Kubernetes Vulnerabilities Exposing Windows Nodes

Storm-0324 Exploits Microsoft Teams Chats Deploying JSSLoader

‘ThemeBleed’ flaw in Windows 11 Enables Code Execution

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Akira Ransomware	IPv4	161.35.92[.]242, 173.208.205[.]10, 185.157.162[.]21, 185.193.64[.]226, 149.93.239[.]176, 158.255.215[.]236, 95.181.150[.]173, 94.232.44[.]118, 194.28.112[.]157, 5.61.43[.]231, 5.183.253[.]129 45.80.107[.]220, 193.233.230[.]161, 149.57.12[.]131, 149.57.15[.]181, 193.233.228[.]183, 45.66.209[.]122, 95.181.148[.]101, 193.233.228[.]86, 176.124.201[.]200, 162.35.92[.]242, 144.217.86[.]109, 31.184.236[.]63, 31.184.236[.]71
	SHA256	1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296,

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488, 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50, 1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc, 9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163, d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959, 6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
HijackLoader	SHA256	7bd39678ac3452bf55359b44c5192b79412ce61a82cd72eef88f91aba5792ee6, 6b1621bded06b082f83c731319c9deb2fdf751a4cec1d1b2b00ab9e75f4c29ca, e67790b394f5238908fcc326a9db940b200d9b50cbb45f0bfa94038db50beeae, 693cace37b4b6fed2ca67906c7a4b1c11273110561a207a222aa4e62fb4a184a, 04c0a4f3b5f787a0c9fa8f6d8ef19e01097185dd1f2ba40ae4bbbeca9c3a1c72
	URLs	hxxps://www.4sync[.]com/web/directDownload/KFtZysVO/4jBKM7R0. baa89a7b43a7b73227f22ae561718f7f, hxxps://geupdate-service[.]bond/img/3344379399.png
PhoenixMiner	SHA256	3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3, c7e1aa53dc667581f37bcbd0793c2ef909e8a4461c59641cb2c672ebe192609c, 201a1979e02bcaa2808e31613a0bef99ad55d514fcaed973840a1bf1efdb4cbe, f4b1dc6456aed765e11878c6a5b9555ee2aec1737219137d187e480599e254c9, d241ef2a157f44dcc323279bd89168c0f6b142de964815ceb0429181eae9a789
lolMiner	SHA256	2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73, aafe94fe2ca6210fde8f5691c066dc128090b097a7d45a69d7ccc977891e08b4, 8ebe85fd149f9b1e93668a733182ad6e0cafd1a0b285800e4e6b226b8673cbaa,

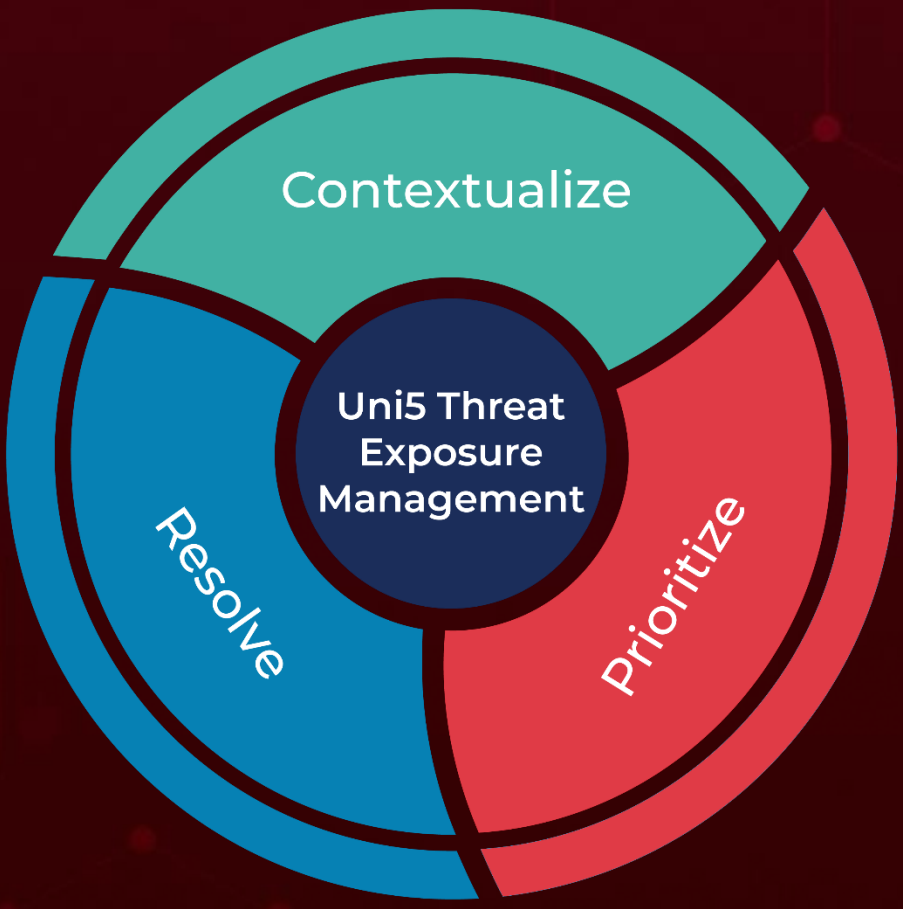
Attack Name	TYPE	VALUE
lolMiner	SHA256	ac1af3a386b2dcf0e2a2955101dc91de7f5e62c900ba4476b0b842d1aa951bbe, 2c049deedbc83923abdd41580faa07c98037f09b5fabe98f97a9239a0b6e3542
M3_Mini_Rat	SHA256	7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08
Sponsor Backdoor	SHA1	098b9a6ce722311553e1d8ac5849ba1dc5834c52, 5aee3c957056a8640041abc108d0b8a3d7a02ebd, 764eb6ca3752576c182fc19cff3e86c38dd51475, 2f3eda9d788a35f4c467b63860e73c3b010529cc, e443dc53284537513c00818392e569c79328f56f, c4bc1a5a02f8ac3cf642880dc1fc3b1e46e4da61, 39ae8ba8c5280a09ba638df4c9d64ac0f3f706b6, a200be662cdc0ece2a2c8fc4dbbc8c574d31848a, 5d60c8507ac9b840a13ffdf19e3315a3e14de66a, 50cfb3cf1a0fe5ec2264ace53f96fadfe99cc617, 1aae62acee3c04a6728f9edc3756fabd6e342252, 519ca93366f1b1d71052c6ce140f5c80ce885181, 4709827c7a95012ab970bf651ed5183083366c79, 99c7b5827df89b4fafc2b565abed97c58a3c65b8, e52aa118a59502790a4dd6625854bd93c0deaf27
	File Path	%SYSTEMDRIVE%\inetpub\wwwroot\aspnet_client\, %USERPROFILE%\AppData\Local\Temp\file\, %USERPROFILE%\AppData\Local\Temp\2\low\, %USERPROFILE%\Desktop\, %USERPROFILE%\Downloads\a\, %WINDIR%\, %WINDIR%\INF\MSExchange Delivery DSN\, %WINDIR%\Tasks\, %WINDIR%\Temp\%WINDIR%\Temp\crashpad\1\Files
	IPv4	162.55.137[.]20, 37.120.222[.]168, 198.144.189[.]74, 5.255.97[.]172
3AM Ransomware	IPv4	185.202.0[.]111, 212.18.104[.]6, 85.159.229[.]62
	SHA256	079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22, 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e, 680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4, 991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af, ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

Attack Name	TYPE	VALUE
JSSLoader	SHA256	67a1328242c89b2f54018d31eca071ab7edef6df30fea2633ad1a013aa5feb8a, 2373a6a7223154a2e4e3e84e4bdda0d5a9bc22580caf4f418dae5637efec65e5, 1f2ab2226f13be64feeece1884eaa46e46c097bb79b703f7d622d8ff1a91b938, 33b3a1da684efc2891668eecf883ba7b9768a117956786e4356a27d1dffe0560, c1e7d6ec47169ffb1118c4be5ecb492cd1ea34f3f3dd124500d337af3e980436, 15f15b643eafcc50777bed33eda25158c7f58f4dbaaaa511072ef913a302a8da, daba93cf353585a67ed893625755077a2d351ba46ec5ea86b5bd0b45b84bc7c5, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0, 16f9674ea7c40a0e474966f59c413518509e295608c7ecc37c6096b034b88918, 2e3bc3b059733b4db846d3227abbfa6a7914b551f0175d6f77e22d08b57d49e3, a0c5b1fdcb95037e57dd502d848aa3137882d7af6fbf301262e8cd35db7f58b7, 2df508247a4e739b086c9de47d91a26ea7aee4d5cf9bc5cc70b5ad2dc7f102c6, d2b080b9af5d39d72af149afb065e769b1da8005edfe84237942a1b99f4fa36c, 793aa21ed7432ef2b0eda8d80036361878f728dbc4081d72f80fa3694702a4d8, 35f5c781d61d398ce47a8881228346a81afb4915bf083518bf2b4cc8d6a2685b, db1d98e9cca11beea4cfd1bfbe097dffd9fc4cc8b1b02e781863658d8c6f16c7, 410cd107dfd37752936bd20d022ea614cd373aa9d37db255f65dc434e653236a, 3b6d61add64402dc74d237e69d701ad2b0bea9a525798a376cd13f2090bb39ee, 969cfeddc1c90d36478f636ee31326e8f381518e725f88662cc28da439038001, ee8f394d9e192c453d47a0c57261a03921dcbb97248a67427cb6fc6d8833c8a0, 5450eca67cb31e326801df019d9a030d3bef8b04af6c91dadf760d62e2ca3ab1, a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044, c328f48c5f4a2c2441bcd0b0c0551547ca254f7ebbb46d30d357e962d8330063, 8279ce0eb52a9f5b5ab02322d1bb7cc9cb5b242b7359c3d4d754687069fcb7b8, 967882624ba26c4fcd6806791aa4994b5bf64ca4b1e66dd8d24f1fa54b3a43f0

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

September 18, 2023 . 7:30 AM

More at www.hivepro.com