Date of Publication
September 2, 2025

Hive Pro

HiveForce Labs

MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

AUGUST 2025

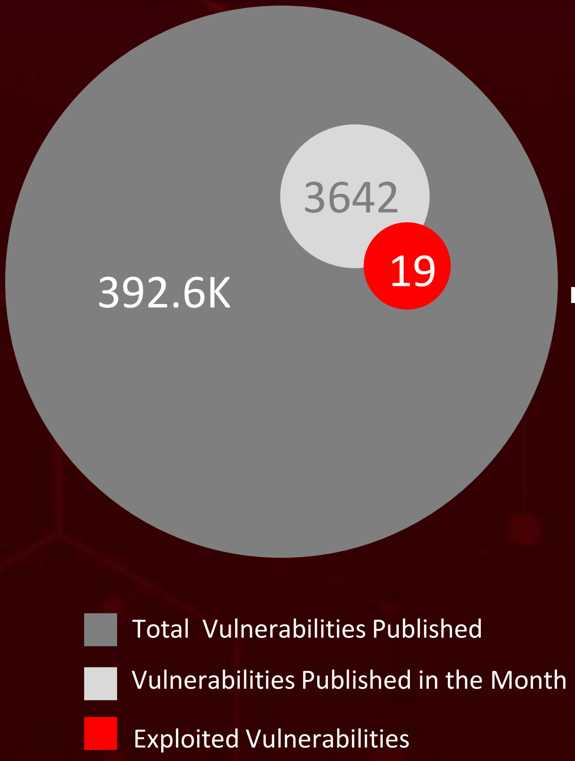
Table Of Contents

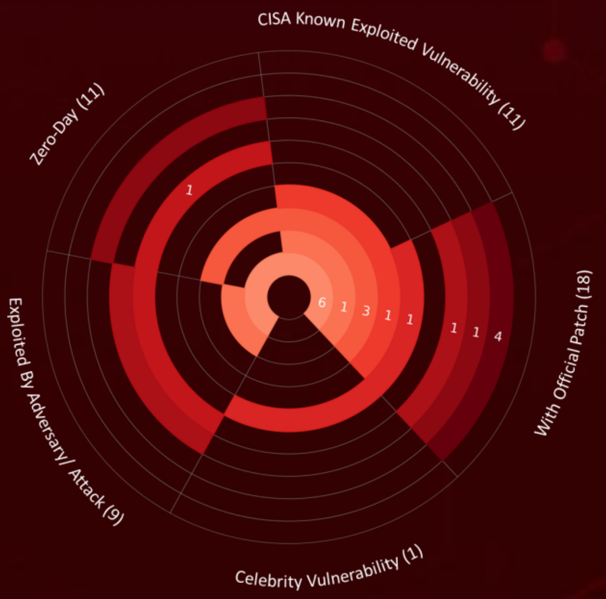
Summary

August proved to be a turbulent month for cybersecurity, marked by the emergence of a celebrity vulnerability called **BadSuccessor** alongside **eleven** newly discovered zero-days. Among the most pressing was **CVE-2025-7775**, a memory overflow flaw in Citrix NetScaler ADC and NetScaler Gateway that has already been weaponized in real-world attacks. The flaw enables unauthenticated remote code execution (RCE) or denial of service (DoS), making it a high-value target for threat actors. Another urgent case was **CVE-2025-43300**, a critical zero-day in Apple's Image I/O framework. With little or no user interaction required, attackers can exploit this flaw by simply delivering a malicious image file, Apple has confirmed is being leveraged in targeted campaigns.

At the same time, state-aligned groups escalated their global operations. **Salt Typhoon**, a Chinese state-sponsored threat actor, widened its reach across more than 600 organizations in 80 countries, including 200 in the United States. Meanwhile, **Storm-0501**, pivoted away from conventional ransomware toward sophisticated cloud-focused attacks, taking advantage of identity misconfigurations and the fractured defenses of hybrid infrastructures. These shifts highlight how adversaries are adapting their strategies to exploit weaknesses in modern enterprise environments.

Elsewhere, Russian operations continued to loom large. **Static Tundra**, a Moscow-linked espionage group, was observed exploiting Cisco IOS's long-standing Smart Install vulnerability (**CVE-2018-0171**), deploying advanced implants and custom tooling to seize control of unpatched devices. On another front, the cybercriminal collective **COOKIE SPIDER** unleashed **SHAMOS**, a customized variant of the Atomic macOS Stealer (AMOS), luring victims through malvertising campaigns and fraudulent tech support websites. Together, these campaigns underscore the urgency for organizations to reinforce their defenses and remain vigilant in a digital arena where threats grow sharper and more relentless with each passing month.





Insights

In August 2025, a geopolitical cybersecurity landscape unfolds, revealing **United Kingdom, Singapore, United States, Canada** and **Switzerland** as the top-targeted countries

Highlighted in **August 2025** is a cyber battleground encompassing the **Defense, Media, Manufacturing, Telecommunications,** and **Financial** sectors, designating them as the top industries

SafePay a fast-rising ransomware group, has surged into 2025 as one of the most aggressive crews, racking up over 200 attacks.

CVE-2025-8088 a zero-day in WinRAR, is under active exploitation, with groups like RomCom and Paper Werewolf.

Crypto24 ransomware has rapidly escalated into a global menace - hitting critical industries across Asia, Europe, and the U.S. with a lethal mix of trusted IT tools and custom malware.

Static Tundra exploits the long-standing Cisco IOS flaw CVE-2018-0171, turning it into a gateway for planting persistent backdoors.

CVE-2025-43300: A critical Apple Image I/O zero-day that turns a single malicious image into a silent code execution weapon.

ZipLine campaign targets U.S. supply chain manufacturers, using “Contact Us” forms to spark business-like conversations and slowly build trust before striking.

Salt Typhoon, is sweeping across the globe, disrupting 600+ organizations in 80 countries, with 200 hits in the U.S. alone.

Storm-0501, has pivoted from classic ransomware to the cloud, exploiting identity flaws and weak hybrid security to breach targets.

Threat Landscape

19 Vulnerabilities

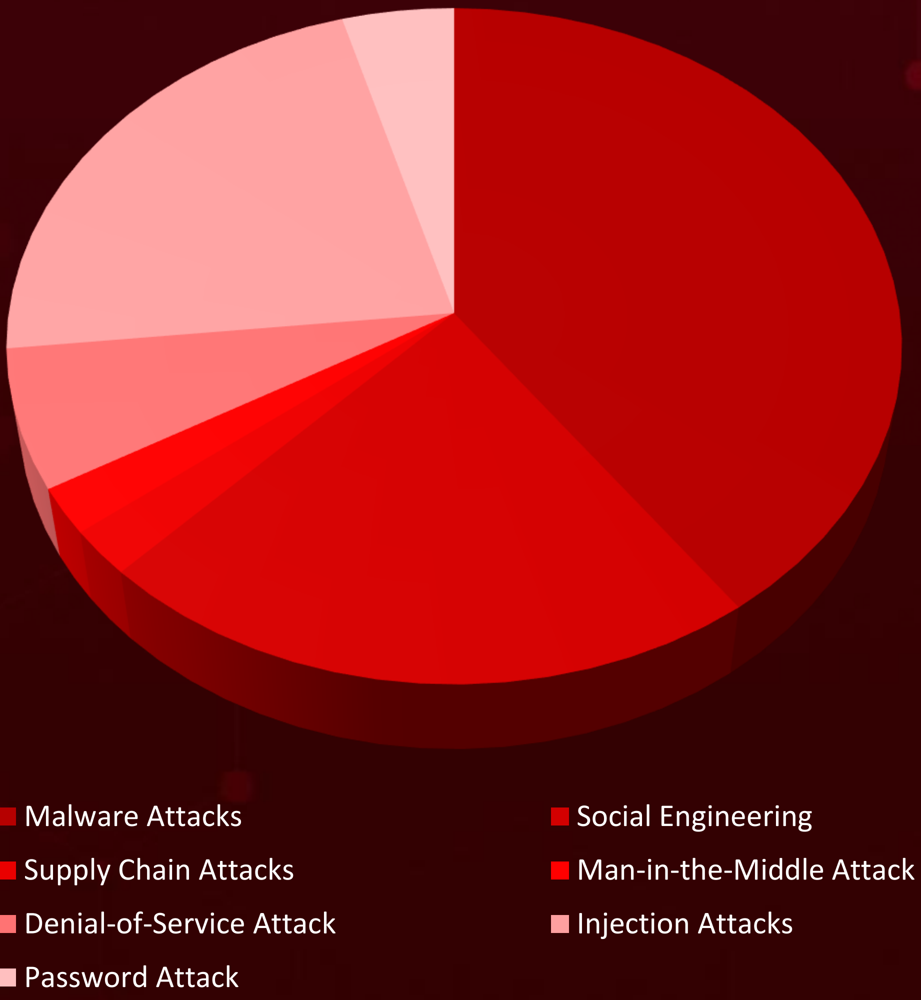
195 MITRE ATT&CK TTPs

55 Industries

08 Adversaries

195 Countries

25 Attacks



Celebrity Vulnerabilities

CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53779	⊗	Windows Server 2025	-
	CISA KEV		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
BadSuccessor (Windows Kerberos Elevation of Privilege Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-23	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-53779

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-49533	Adobe Experience Manager (MS) Remote Code Execution Vulnerability	Adobe Experience Manager (AEM)	✗	✗	✓
CVE-2025-54253	Adobe Experience Manager (MS) Misconfiguration Vulnerability	Adobe Experience Manager (AEM)	✗	✗	✓
CVE-2025-54254	Adobe Experience Manager (MS) Improper Restriction of XML External Entity Vulnerability	Adobe Experience Manager (AEM)	✗	✗	✓
CVE-2025-54948	Trend Micro Apex One OS Command Injection Vulnerability	Trend Micro Apex One	✓	✓	✓
CVE-2025-54987	Trend Micro Apex One Management Console Command Injection RCE Vulnerability	Trend Micro Apex One	✓	✗	✓
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop.sys	✓	✗	✗
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	WinRAR	✓	✓	✓
CVE-2025-6218	RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	WinRAR	✗	✗	✓
CVE-2025-25256	Fortinet FortiSIEM OS Command Injection Vulnerability	FortiSIEM	✗	✗	✓
CVE-2025-53779	BadSuccessor (Windows Kerberos Elevation of Privilege Vulnerability)	Windows Server 2025	✗	✗	✓
CVE-2025-32433	Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	All Erlang/OTP SSH servers	✗	✓	✓
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-43300	Apple iOS, iPadOS, and macOS Out-of- Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS	✓	✓	✓
CVE-2025-7775	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco IOS XE Software	✓	✓	✓
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE Software	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
ApolloShadow	Backdoor	-	-	-	Phishing
Warlock	Ransomware	CVE-2025-53770	Microsoft SharePoint Server	✓	Exploiting vulnerabilities
4L4MD4R	Ransomware	CVE-2025-53770	Microsoft SharePoint Server	✓	Exploiting vulnerabilities
RoKRAT	RAT	-	-	-	Phishing
Plague	Backdoor	-	Linux	-	Compromised Linux PAM module installation
SafePay	Ransomware	-	Windows	-	Compromised VPN or RDP credentials
Qdoor	Backdoor	-	Windows	-	Via mlicious DLL injection
MedusaLocker	Ransomware	CVE-2025-7771	Windows	✗	Exploiting vulnerabilities
CastleBot	MaaS	-	-	-	Fake software installers via SEO poisoning
DarkCloud	Stealer	-	Microsoft Windows	-	Phishing Emails
Efimer	Trojan	-	-	-	Phishing Emails, Compromised WordPress sites, fake torrent downloads
Charon	Ransomware	-	Microsoft Windows	-	-
SWORDLDR	Loader	-	Microsoft Windows	-	-
Mythic	Framework	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SnipBot	RAT	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting Vulnerability
RustyClaw	Downloader	CVE-2025-8088	RARLAB WinRAR	✓	Exploiting Vulnerability
PS1Bot	Framework	-	-	-	Social Engineering
Noodlophile	Stealer	-	-	-	Spear phishing emails
GodRAT	RAT	-	Windows	-	Social Engineering
AsyncRAT	RAT	-	Windows	-	Social Engineering
Crypto24	Ransomware	-	Windows	-	-
SYNful Knock	Backdoor	CVE-2018-0171	Cisco IOS and IOS XE Software	✓	Exploiting Vulnerability
QuirkyLoader	Loader	-	-	-	Phishing
SHAMOS	Stealer	-	-	-	Malvertising and fake support websites
MixShell	Backdoor	-	-	-	Social Engineering

Adversaries Summary

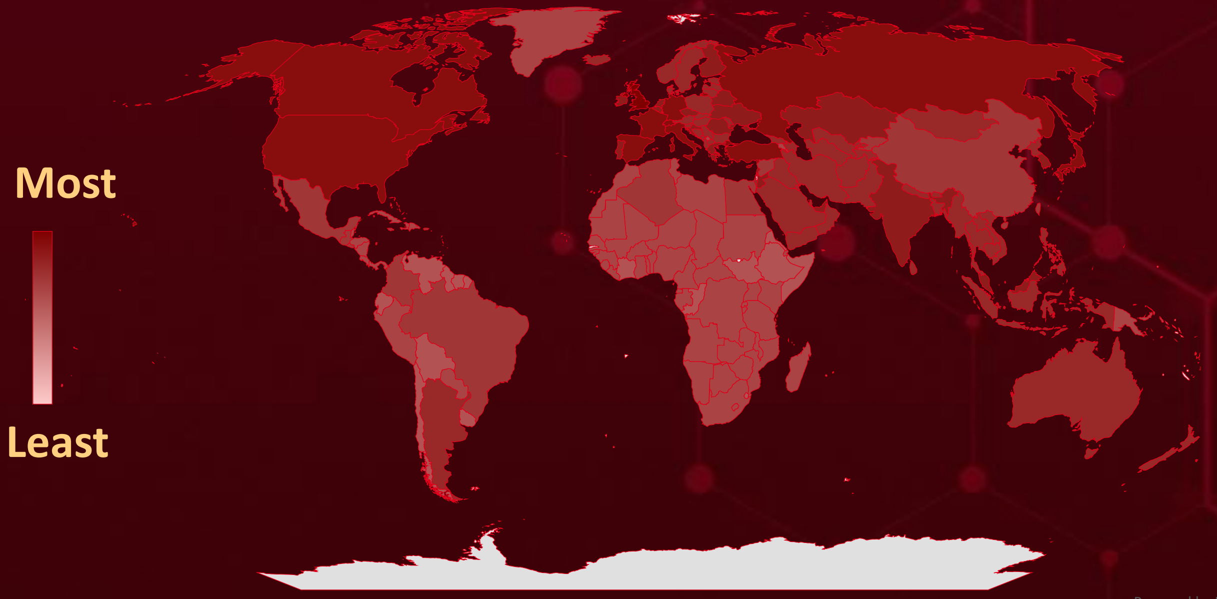
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Secret Blizzard	Information theft and espionage	Russia	-	ApolloShadow	-
APT37	Information theft and espionage	North Korea	-	RoKRAT	-
RomCom	Information theft and espionage, Financial gain	Russia	CVE-2025-8088	Mythic agents, SnipBot variants, and RustyClaw downloaders	RARLAB WinRAR
Paper Werewolf	Espionage and Destruction	-	CVE-2025-8088, CVE-2025-6218	-	RARLAB WinRAR
Static Tundra	Information Theft and Espionage	Russia	CVE-2018-0171	SYNful Knock	Cisco IOS and IOS XE Software
Cookie Spider	Information Theft	-	-	SHAMOS	-
Salt Typhoon	Information theft and espionage	China	CVE-2024-21887 CVE-2023-46805 CVE-2024-3400 CVE-2023-20273 CVE-2023-20198 CVE-2018-0171	-	Ivanti Connect Secure and Policy Secure, Palo Alto Networks PAN-OS, Cisco IOS and IOS XE Software
Storm-0501	Financial Theft	-	-	-	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Web Content Management System	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier
TREND MICRO	Endpoint Security Solution	Trend Micro Apex One Management Server Version 14039 and below
	System Utility Software	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier
	File Compression / Archiving Software	WinRAR versions before 7.13, WinRAR Version Prior to 7.12
FORTINET	SIEM (Security Information and Event Management)	FortiSIEM Versions 7.3.0 through 7.3.1, 7.2.0 through 7.2.5, 7.1.0 through 7.1.7, 7.0.0 through 7.0.3, 6.7.0 through 6.7.9, FortiSIEM 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4 All Versions
Microsoft	Server	Windows Server 2025
ERLANG	SSH Server Software	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier
CISCO	Network Operating Systems	Cisco IOS and IOS XE Software
	Operating System	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
citrix	Application Delivery and Remote Access solution	Citrix NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1- 37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1- 55.330-FIPS and NDcPP
ivanti	Secure access and network security solutions	Ivanti Connect Secure and Policy Secure
paloalto NETWORKS	Network Security Operating System	Palo Alto Networks PAN-OS

Targeted Countries

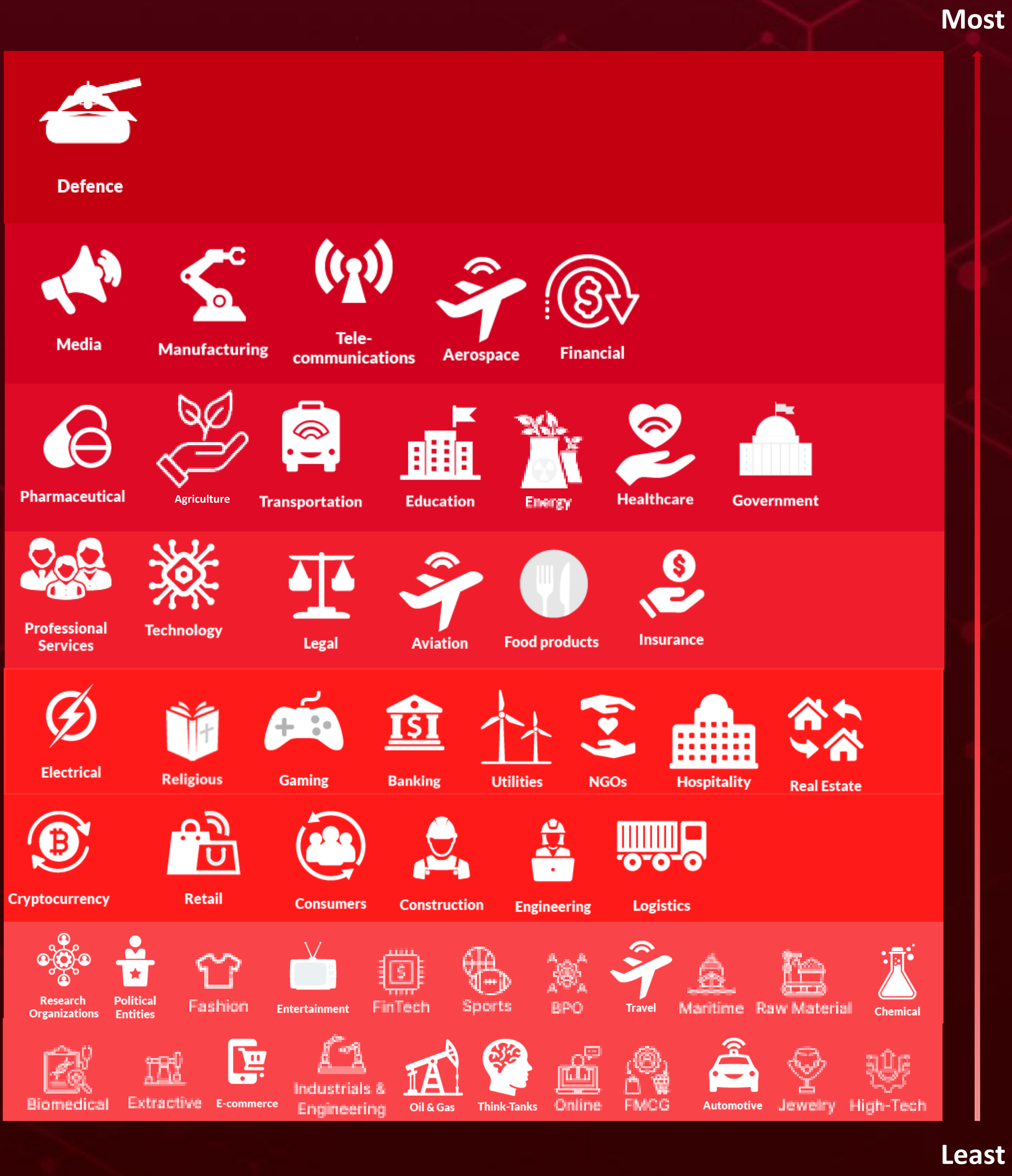


Powered by Bing

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

Color	Countries
🟥	United Kingdom
🟥	Singapore
🟥	United States
🟥	Canada
🟥	Switzerland
🟥	Cyprus
🟥	Russia
🟥	France
🟥	Spain
🟥	Germany
🟥	Turkey
🟥	Italy
🟥	Japan
🟥	Ukraine
🟥	South Korea
🟥	Finland
🟥	Belgium
🟥	Greece
🟥	Czech Republic
🟥	Croatia
🟥	Kazakhstan
🟥	Brunei
🟥	Malaysia
🟥	Belarus
🟥	Netherlands
🟥	India
🟥	Portugal
🟥	United Arab Emirates
🟥	Republic of Ireland
🟥	Romania
🟥	Jordan
🟥	Lebanon
🟥	Myanmar
🟥	Slovakia
🟥	Palestine
🟥	Cambodia
🟥	Bosnia and Herzegovina
🟥	Andorra
🟥	North Macedonia
🟥	Denmark
🟥	Albania
🟥	Estonia
🟥	Sweden
🟥	Argentina
🟥	Yemen
🟥	Georgia
🟥	New Zealand
🟥	Hungary
🟥	Oman
🟥	Iceland
🟥	Poland
🟥	Australia
🟥	Saudi Arabia
🟥	Indonesia
🟥	Bhutan
🟥	Iran
🟥	Thailand
🟥	Iraq
🟥	Uzbekistan
🟥	Israel
🟥	Montenegro
🟥	Austria
🟥	Nepal
🟥	Azerbaijan
🟥	North Korea
🟥	Bahrain
🟥	Norway
🟥	Kuwait
🟥	Pakistan
🟥	Laos
🟥	Philippines
🟥	Latvia
🟥	Qatar
🟥	Afghanistan
🟥	San Marino
🟥	Liechtenstein
🟥	Serbia
🟥	Lithuania
🟥	Slovenia
🟥	Luxembourg
🟥	Sri Lanka
🟥	Bangladesh
🟥	Tajikistan
🟥	Maldives
🟥	Timor-Leste
🟥	Malta
🟥	Turkmenistan
🟥	Turkmenistan
🟥	Moldova
🟥	Vietnam
🟥	Monaco
🟥	Mongolia
🟥	Bulgaria
🟥	Curacao
🟥	Colombia
🟥	Hong Kong
🟥	Egypt
🟥	Taiwan
🟥	El Salvador
🟥	Holy See
🟥	Mexico
🟥	China
🟥	Barbados
🟥	Syria
🟥	Guatemala
🟥	Jamaica
🟥	Kyrgyzstan
🟥	Brazil

Targeted Industries



Most

Defence

Media, Manufacturing, Tele-communications, Aerospace, Financial

Pharmaceutical, Agriculture, Transportation, Education, Energy, Healthcare, Government

Professional Services, Technology, Legal, Aviation, Food products, Insurance

Electrical, Religious, Gaming, Banking, Utilities, NGOs, Hospitality, Real Estate

Cryptocurrency, Retail, Consumers, Construction, Engineering, Logistics

Research Organizations, Political Entities, Fashion, Entertainment, FinTech, Sports, BPO, Travel, Maritime, Raw Material, Chemical

Biomedical, Extractive, E-commerce, Industrials & Engineering, Oil & Gas, Think-Tanks, Online, FMCG, Automotive, Jewelry, High-Tech

Least

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information	T1071 Application Layer Protocol	T1082 System Information Discovery	T1204 User Execution
T1059.001 PowerShell	T1036 Masquerading	T1068 Exploitation for Privilege Escalation	T1071.001 Web Protocols	T1190 Exploit Public-Facing Application
T1574 Hijack Execution Flow	T1566 Phishing	T1588 Obtain Capabilities	T1041 Exfiltration Over C2 Channel	T1021 Remote Services
T1588.006 Vulnerabilities	T1562 Impair Defenses	T1587.004 Exploits	T1574.001 DLL	T1547 Boot or Logon Autostart Execution
T1140 Deobfuscate/ Decode Files or Information	T1203 Exploitation for Client Execution	T1055 Process Injection	T1070 Indicator Removal	T1005 Data from Local System

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Warlock	SHA256	da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb
4L4MD4R	SHA256	33067028e35982c7b9fdcfe25eb40294635424511fdff454007832cf953feaf1e
	Domain	bpp[.]theinnovationfactory[.]it
	IPv4	145[.]239[.]97[.]206
SafePay	SHA256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526, 4fe8c6ccdfbcbf6714472e805447fd727d3e46525bd44baf08e5887f890ffb88, 22df7d07369d206f8d5d02cf6d365e39dd9f3b5c454a8833d0017f4cf9c35177,
		0f23a313f79d54ae2102f193d3de1a6a98791c27921f28a4fab1092bcb43e5ee, 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917, f0127e786c9fb7bf2c8c999202d95c977af4c26cc27302a6ee352cfd62869e7b, 94244ec2480addeaebb43aebbe48cee94f7f429231aa054f4c26f671653163b0, b3045308a07e46c9f7dd98d352e964f242307ce30df8087dc751488118b5b959, ba1b89023581a0bc7a75f8ede9ec6115d5dda98c0145634f1b98978fbc79c956, 7f33c939f7aaf46945d58ed7fd0d1f5c7e3de1ff6a1a591ecc1992dab2a65078, fa74ac0e05b6209b7691511572386f97464ff5728732de99ddd6b5449ffae386, 2f49bff45cc091a7bf52dcd061d24f9a7f2cf0ca9b3c12123bd3cf2fac56b481
	TOR Address	safepaypfxntwixwjrlcscft433ggemlhgkkdupi2ynhtcmvdgubmoyd[.]onion
Qdoor	SHA256	0cc25cf9f5d4f02c1a2ed014e2d4acb0d383f01c9bb1852a10b933eec17c1f20, 5d2e7ed8f77bc95302e693312f9a154f0afb698a05796561e277c037deb15a9d, 6d208e99cfac9b2a32df042889636db6217cd12de1980aca7d9678160bf58d4d, 87db51984bfcadf9ee96183f0fe0fb5129b4cfe5a23a68c272b94299267779ea,

Attack Name	TYPE	VALUE
MedusaLocker	SHA256	c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7
Charon	SHA256	80711e37f226ef1dc86dc80a8cbc0b2ec895b361e9ade85da793d94b1d876be8, 739e2cac9e2a15631c770236b34ba569aad1d1de87c6243f285bf1995af2cdc2
	SHA1	92750eb5990cdcda768c7cb7b654ab54651c058a, a1c6090674f3778ea207b14b1b55be487ce1a2ab
SWORDLDR	SHA256	E0a23c0d99c45d40f6ef99c901bacf04bb12e9a3a15823b663b392abadd2444e
	SHA1	21b233c0100948d3829740bd2d2d05dc35159ccb
PS1Bot	SHA256	809f4ffef71ab43d692d4fececf1dfefffb0854ae1f15486960b1c198c47c69f
GodRAT	MD5	d09fd377d8566b9d7a5880649a0192b4, e723258b75fee6fbd8095f0a2ae7e53c, 318f5bf9894ac424fd4faf4ba857155e, 512778f0de31fcce281d87f00affa4a8, 6cad01ca86e8cd5339ff1e8fff4c8558, 58f54b88f2009864db7e7a5d1610d27d, 64dfcdd8f511f4c71d19f5a58139f2c0, 8008375eec7550d6d8e0eaf24389cf81, 04bf56c6491c5a455efea7dbf94145f1, 5f7087039cb42090003cc9dbb493215e
	SHA256	0E2889F6475AEA625D18B200A2CACDAC745ECB22044F6366F21AFC2E24046025, C52FB4EDDF64779B7BEDA43D26618251EEFE84BBB7F1C8EBB725E5E2DFDCFE4A, 2E33A3C604C4212547BDBB31BD842B365EF28EB7B9A84564FB8EF3C0268F6268, 51B7478388593F90516D04053B95DD0861D93D6195341B36272D2474D196BA86, CED343EE088F8FDDAF74D3B85C0D9176A3DB852E580467CA6C60EC86BD5E2132, 67C713A44186315D7CBFEC4745B7DD199D86711F48C5F0778A71871AC3B02624, B673444DAF876EEFF6AA81BFCD86F68FA7E5C4C48EFFF183D94EDFBB57D93EF5

Attack Name	TYPE	VALUE
GodRAT	IPV4	103[.]237[.]92[.]191, 118[.]99[.]3[.]33, 118[.]107[.]46[.]174, 154[.]91[.]183[.]174
AsyncRAT	MD5	605f25606bb925d61ccc47f0150db674, 961188d6903866496c954f03ecff2a72, 4ecd2cf02bdf19cdbc5507e85a32c657, 17e71cd415272a6469386f95366d3b64
	SHA256	ED1DFD2E913E1C53D9F9AB5B418F84E0F401ABFDF8E3349E1FCFC98663DCB23F, C5F5D5A9BA824E235ABD02E9D09052CA8A17B8C18253C7B25727A17DF675E66B, 8A1A19741DC3626CFF78E1C54DE827058060A42F3ACADDF6D5C3DEBE7071185B
	Domain	wuwu6[.]cfd
	IPv4	156[.]241[.]134[.]49, 47[.]238[.]124[.]68
Crypto24 Ransomware	SHA256	10c3317566f52eaeb45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b, 0e36b1837e5a2cbd14fac2c3b709a5470b7b488bd15898d30840ec60448e83e0, 3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac, 686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac, 24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49533	✗	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:experience_manager:*:*:*:*:-:*:*:*	-
Adobe Experience Manager (MS) Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54253	✗	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:experience_manager:*:*:*:*:-:*:*:*	-
Adobe Experience Manager (MS) Misconfiguration Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-16	T1068: Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54254	✗	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:experience_manager:*:*:*:*:-:*:*:*	-
Adobe Experience Manager (MS) Improper Restriction of XML External Entity Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54948	✗	Trend Micro Apex One Management Server Version 14039 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	-
Trend Micro Apex One OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting; T1203 : Exploitation for Client Execution	https://success.trendmicro.com/en-US/solution/KA-0020652

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54987	✗	Trend Micro Apex One Management Server Version 14039 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	-
Trend Micro Apex One Management Console Command Injection RCE Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting; T1203 : Exploitation for Client Execution	https://success.trendmicro.com/en-US/solution/KA-0020652

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-7771	✗	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:techpowerup:throttlestop:*:*:*:*:*:*:*	MedusaLocker ransomware
TechPowerUp ThrottleStop Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-782	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-8088	✗	WinRAR versions before 7.13	RomCom, Paper Werewolf
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Mythic agents, SnipBot variants, and RustyClaw downloaders
RARLAB WinRAR Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2025-6218	✗	WinRAR Version Prior to 7.12	Paper Werewolf
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*	-
RARLAB WinRAR Directory Traversal Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-25256	✗	FortiSIEM Versions 7.3.0 through 7.3.1, 7.2.0 through 7.2.5, 7.1.0 through 7.1.7, 7.0.0 through 7.0.3, 6.7.0 through 6.7.9, FortiSIEM 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4 All Versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*	-
Fortinet FortiSIEM OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1588.005: Exploits, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-152

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32433	✗	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	-
Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1210: Exploitation of Remote Services, T1078: Valid Accounts	https://github.com/erlang/otp/releases, https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0171	✗	Cisco IOS and IOS XE Software	Static Tundra, Salt Typhoon
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios:15.2\(5\)e:*:*:*:*:*:*:*	SYNful Knock
Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-20	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-43300	☒	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.	-
	ZERO-DAY		
	✓	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 Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://support.apple.com/en-us/124925 , https://support.apple.com/en-us/124926 , https://support.apple.com/en-us/124927 , https://support.apple.com/en-us/124928 , https://support.apple.com/en-us/124929

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-7775	✗	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-119	T1059: Command and Scripting Interpreter;
		T1499: Endpoint Denial of Service;
		T1190: Exploit Public-Facing Application
			https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗	Ivanti Connect Secure and Policy Secure	Salt Typhoon
	ZERO-DAY	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
	✓		
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter; T1133: External Remote Service	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46805	✗	Ivanti Connect Secure and Policy Secure	Salt Typhoon
	ZERO-DAY	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
	✓		
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400	✗	Palo Alto Networks PAN-OS	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77 CWE-20	T1190 : Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20273	✗	Cisco IOS XE Software	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	-
Cisco IOS XE Web UI Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20198	✗	Cisco IOS XE Software	Salt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	-
Cisco IOS XE Web UI Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-420	T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ApolloShadow	ApolloShadow is a modular backdoor designed to target Windows systems, typically delivered through phishing emails, fake software updates, or trojanized application downloads. Once it infects a device, it establishes persistence through techniques like registry modifications and DLL side-loading. The malware conducts system reconnaissance, steals user credentials, and may deploy additional payloads. It communicates with a command-and-control (C2) server over encrypted HTTPS channels to exfiltrate stolen data.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Secret Blizzard			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Warlock	Warlock is a relatively new ransomware-as-a-service (RaaS) operation that debuted in June 2025 with an ad on a Russian cybercrime forum ("if you want a Lamborghini, please call me") and swiftly garnered attention by targeting businesses, governments, and other institutions via SharePoint zero-days.	Exploiting vulnerabilities	CVE-2025-53770
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss, Data Encryption, and Exfiltration	Microsoft SharePoint Server
ASSOCIATED ACTOR			**PATCH LINK**
Storm-2603			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

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
4L4MD4R	4L4MD4R is a Golang-based ransomware exploiting Microsoft SharePoint flaws to encrypt files and demand 0.005 BTC ransom.It has impacted over 148 organizations worldwide, including U.S. agencies, since its discovery in July 2025.	Exploiting vulnerabilities	CVE-2025-53770
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss, Data Encryption, and Exfiltration	Microsoft SharePoint Server
ASSOCIATED ACTOR			**PATCH LINK**
Storm-2603			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RoKRAT	RoKRAT is a remote access trojan used by APT37 for espionage, data theft, and surveillance. It hides communications via cloud services and, in newer versions, uses techniques like steganography and fileless execution to evade detection.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage, data exfiltration, surveillance	-
ASSOCIATED ACTOR			**PATCH LINK**
APT37			-

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 CVE
Plague	Plague is a stealthy Linux backdoor masquerading as a PAM (Pluggable Authentication Module) that bypasses authentication to grant persistent, hidden SSH access. It evades detection with advanced obfuscation, anti-debugging techniques, session log erasure, and invisibility to antivirus scanners.	Compromised Linux PAM module installation	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Unauthorized SSH access, data theft, system compromise	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SafePay	SafePay is a emerging ransomware threat that employs double extortion, encrypting files (appending .safepay) while exfiltrating sensitive data to coerce payment. It typically infiltrates networks via compromised VPN or RDP access, then disables security defenses and moves quickly from initial access to encryption.	Compromised VPN or RDP credentials	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		File encryption, data theft, ransom extortion	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Qdoor	QDoor is a Rust-based network tunneling backdoor used by the BlackSuit ransomware group, designed to proxy traffic between a victim's network and a command-and-control (C2) server, enabling stealthy remote access.	Via mlicious DLL injection	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		Stealthy remote access, network traffic tunneling	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MedusaLocker	MedusaLocker is a ransomware family that encrypts files, disrupts operations, and demands ransom, often run as a Ransomware-as-a-Service.It spreads through compromised RDP, phishing, and lateral movement tools while disabling recovery options.	Exploiting vulnerabilities	CVE-2025-7771
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		File encryption, operational disruption, ransom extortion	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CastleBot	CastleBot is a malware framework offered as part of a Malware-as-a-Service operation. It operates in multiple stages: starting with a lightweight "stager," followed by a "loader," and finishing with a core backdoor. The core backdoor can steal information, install additional malware, and set up the system for potential ransomware attacks.	Fake software installers via SEO poisoning	-
		IMPACT	AFFECTED PLATFORM
TYPE		Remote Access, Installation of Additional Malware	-
MaaS			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkCloud	DarkCloud, a Windows-based information stealer first spotted in 2022, reappeared in 2025 with enhanced delivery and obfuscation techniques, including ConfuserEx-protected files and a VB6 payload. It uses JavaScript and PowerShell to deploy a fileless .NET DLL, maintain persistence, and inject its payload into MSBuild.exe. DarkCloud then steals browser credentials and payment information, exfiltrating the data via FTP or SMTP.	Phishing Emails	-
		IMPACT	AFFECTED PLATFORM
TYPE		Information Theft, Persistence on the System, Decreased System Performance	Microsoft Windows
Stealer			
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 CVE
Efimer	The Efimer Trojan is a highly evasive cryptocurrency-stealing malware. It monitors clipboard activity to intercept and replace wallet addresses, captures recovery phrases, and uses the Tor network to conceal its communications. Efimer silently executes in the background. When run with administrative privileges, it bypasses security, establishes persistence through Windows registry modifications.	Phishing Emails, Compromised WordPress sites, fake torrent downloads	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Cryptocurrency Theft, Bypasses Windows Defender, Persistence through Windows Registry	-
Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Charon	Charon is a ransomware strain linked to advanced APT-style attacks. The attackers used DLL sideloading, a technique also seen in Earth Baxia campaigns. While DLL sideloading is widely used, its execution here shows high-level sophistication, with coordinated toolchains and encrypted payloads. Charon's deployment involves a multi-stage process for extracting and delivering its payload.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Encryption, Disruption of Operations, Financial Loss	Microsoft Windows
Ransomware			
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 CVE
SWORDLDR	SWORDLDR is a loader used in the attack chain to sideload a malicious DLL. It begins by leveraging the legitimate Edge.exe process, which is a browser-related executable, to load msedge.dll, the payload containing SWORDLDR. By disguising itself as a legitimate Windows service, the malware successfully bypasses standard security defenses, allowing it to execute undetected.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Bypassing Security Defenses, Increased Privileges, Malicious Payload Injection	Microsoft Windows
Loader			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Mythic	Mythic is a cross-platform post-exploitation framework that, while originally built for legitimate red-teaming operations, has been weaponized by threat actors like RomCom to control compromised systems. It provides a flexible, plug-and-play command-and-control (C2) platform, allowing operators to easily add new agents, communication channels, and custom payloads on the fly. Mythic enables attackers to coordinate tasks, maintain persistence, and expand their capabilities across victim environments with remarkable efficiency.	Exploiting Vulnerability	CVE-2025-8088
		IMPACT	AFFECTED PRODUCT
TYPE		Remote Command and Control, Persistence, Exposure of Confidential Business Information	RARLAB WinRAR
Framework			
ASSOCIATED ACTOR			PATCH LINK
RomCom			https://www.win-rar.com/download.html?&L=0

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 CVE
SnipBot	SnipBot, a newly identified variant of the RomCom malware family, employs advanced infection and evasion techniques. Typically delivered via phishing emails disguised as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. This malware demonstrates capabilities for remote command execution and data exfiltration, while using anti-sandbox methods to evade detection.	Exploiting Vulnerability	CVE-2025-8088
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Remote Command Execution, Payload Delivery, System Resource Utilization	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINK**
RomCom			https://www.win-rar.com/download.html?&L=0

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RustyClaw	RustyClaw is a malware downloader built in Rust, incorporating advanced anti-analysis measures. Before initiating its malicious actions, the malware verifies the system's keyboard layout against specific language codes. Additionally, it generates a hash of its file name and compares it to a hardcoded value to prevent execution in sandbox environments with randomized file names. Once these checks are successful, RustyClaw can optionally display a decoy PDF to the infected user while downloading the next-stage implant to proceed with the attack.	Exploiting Vulnerability	CVE-2025-8088
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Downloader		Bypassing Sandboxing and Detection, Persistence	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINK**
RomCom			https://www.win-rar.com/download.html?&L=0

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">PS1Bot</td><td rowspan="6">PS1Bot is a multi-stage malware framework built in PowerShell and C# that operates with a modular design, allowing attackers to load different components as needed. These modules enable a wide range of malicious activities, from stealing sensitive information and logging keystrokes to conducting reconnaissance and maintaining long-term access on compromised machines. What makes PS1Bot particularly dangerous is its focus on stealth, it avoids leaving obvious traces on infected systems and relies heavily on in-memory execution, ensuring that follow-on payloads can run without ever being written to disk.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Data Theft, Persistence</td><td rowspan="2">-</td></tr>
<tr><td>Framework</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Noodlophile</td><td rowspan="6">Noodlophile Stealer is a powerful data-harvesting malware designed to aggressively target browser-based information and sensitive system details. Once active, it siphons credentials, cookies, credit card data, system metadata, and even security configurations from multiple browsers, giving attackers deep access to a victim’s digital footprint. To strengthen its stealth, the stealer sometimes deploys a .NET executable that disables monitoring mechanisms and security defenses.</td><td>Spear phishing emails</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td><b>TYPE</b></td><td rowspan="4">Steal Data</td><td rowspan="2">-</td></tr>
<tr><td>Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GodRAT	GodRAT is a newly uncovered Remote Access Trojan (RAT) built on the Gh0st RAT codebase. To avoid detection, its operators cleverly used steganography to hide malicious shellcode inside image files, which then retrieved the GodRAT payload from a Command-and-Control (C2) server. Once deployed, GodRAT can be extended with plugins, such as a FileManager module that lets attackers browse, modify, and control files on the victim's system. Sharing striking similarities with AwesomePuppet, a Gh0st RAT-based backdoor, GodRAT appears to be its evolutionary successor, carrying forward the same core design while adopting new tactics to stay effective in today's threat landscape.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is a publicly available remote access trojan (RAT) on GitHub. A modified version ensures persistence by creating a scheduled task that triggers at startup. Upon activation, a complex sequence initiates AsyncRAT within Windows Sandbox, which must be manually enabled and requires a reboot.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Remote Control, Information Theft	Windows
RAT			
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 CVE
Crypto24	Crypto24 ransomware, first observed in late 2024, has quickly risen as a significant global cyber threat. The operators behind it plan their campaigns with precision, often launching attacks during off-peak hours to slip past defenses and cause maximum disruption. Their arsenal combines legitimate tools with custom malware, enabling them to infiltrate networks, move laterally, and evade detection. Tactics include using PSExec for internal propagation, AnyDesk for persistent remote access, keyloggers to steal credentials, and multiple backdoors to maintain control.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data Theft, Encrypt Data, System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SYNful Knock	SYNful Knock is a stealthy modular backdoor implant that attackers insert into a modified Cisco IOS image and deploy onto compromised network devices. Once installed, it grants persistent access that survives reboots, allowing adversaries to maintain long-term control while remaining difficult to detect.	Exploiting Vulnerability	CVE-2018-0171
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		System Compromise	Cisco IOS and IOS XE Software
ASSOCIATED ACTOR			PATCH LINK
Static Tundra			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

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 CVE
QuirkyLoader	QuirkyLoader is a stealthy malware loader distributed primarily through phishing emails containing malicious archive files. When executed, it leverages techniques like DLL side-loading and process hollowing to covertly inject encrypted payloads into legitimate Windows processes, enabling the delivery of information stealers and remote access trojans (RATs). QuirkyLoader particularly distinctive is its DLL module, developed in C#.NET with Ahead-of-Time (AOT) compilation. This approach first converts C# code into Microsoft Intermediate Language (MSIL) before compiling it into native machine code, giving the loader both efficiency and an added layer of complexity that hinders detection and analysis.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads other Payloads	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SHAMOS	SHAMOS is a macOS malware variant of the Atomic macOS Stealer (AMOS), distributed by the cybercriminal group COOKIE SPIDER. It spreads through malvertising and fake support websites, tricking users into running one-line terminal commands that install the stealer. Once active, it evades detection, establishes persistence, and exfiltrates sensitive data like credentials, notes, and crypto wallet files.	Malvertising and fake support websites	-
TYPE		IMPACT	AFFECTED PLATFORM
Stealer		Data theft	-
ASSOCIATED ACTOR			PATCH LINK
COOKIE SPIDER			-

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 CVE
MixShell	MixShell is a sophisticated, in-memory malware delivered through a multi-stage phishing campaign known as "ZipLine." It uses DNS tunneling for stealthy communication and is designed for remote command execution and data theft.	Social-engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Pensive Ursa, Blue Python, G0010, Hippo Team, Pfinet, Snake, UAC-0003, UAC-0024, UAC-0144, Uroburos)	Russia	Diplomats	Moscow
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	ApolloShadow	-

TTPs

TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1557: Adversary-in-the-Middle; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1068: Exploitation for Privilege Escalation; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1112: Modify Registry; T1070: Indicator Removal; T1070.004: File Deletion; T1136: Create Account; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1553: Subvert Trust Controls; T1553.004: Install Root Certificate; T1087: Account Discovery; T1071: Application Layer Protocol; T1082: System Information Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
APT37 (aka Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt)	North Korea	-	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RoKRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution: T1027: Obfuscated Files or Information; T1027.003: Steganography; T1140: Deobfuscate/Decode Files or Information; T1574: Hijack Execution Flow; T1574.001: DLL; T1036: Masquerading; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1218: System Binary Proxy Execution; T1218.011: Rundll32

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="5">RomCom (aka Tropical Scorpius, Void Rabisu, DEV-0978, Storm-0978, UNC2596, CIGAR, UAC-0180)</td><td>Russia</td><td rowspan="3">Financial, Manufacturing, Defense, Logistics</td><td rowspan="3">Europe, Canada</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage, Financial gain</td></tr>
<tr><td><b>TARGETED CVE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td>CVE-2025-8088</td><td>Mythic agents, SnipBot variants, and RustyClaw downloaders</td><td>RARLAB WinRAR</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1587.001: Malware; T1587.004: Exploits; T1588.005: Exploits; T1588.006: Vulnerabilities; T1608: Stage Capabilities; T1566.001: Spearphishing Attachment; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1546.015: Component Object Model Hijacking; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1036.001: Invalid Code Signature; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1555.003: Credentials from Web Browsers; T1552.001: Credentials In Files; T1087: Account Discovery; T1518: Software Discovery; T1021: Remote Services; T1560: Archive Collected Data; T1185: Man in the Browser; T1005: Data from Local System; T1114.001: Local Email Collection; T1113: Screen Capture; T1071.001: Web Protocols; T1573.002: Asymmetric Cryptography; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="6">Paper Werewolf (aka GOFFEE)</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Russia</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Espionage and Destruction</td></tr>
<tr><td><b>TARGETED CVE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCT</b></td></tr>
<tr><td>CVE-2025-8088,
CVE-2025-6218</td><td>-</td><td>RARLAB WinRAR</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566.001: Spearphishing Attachment; T1566: Phishing; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1564: Hide Artifacts; T1564.003: Hidden Window; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1095: Non-Application Layer Protocol</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Static Tundra	Russia	Telecommunications, Higher Education, Manufacturing	North America, Asia, Africa, Europe
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2018-0171	SYNful Knock	Cisco IOS and IOS XE Software
TTPs			
TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1601: Modify System Image; T1596: Search Open Technical Databases; T1596.005: Scan Databases; T1543: Create or Modify System Process; T1210: Exploitation of Remote Services; T1587: Develop Capabilities; T1587.004: Exploits; T1018: Remote System Discovery; T1046: Network Service Discovery; T1040: Network Sniffing; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1542.005: TFTP Boot; T1068: Exploitation for Privilege Escalation; T1543.003: Windows Service; T1036: Masquerading; T1105: Ingress Tool Transfer; T1601.002: Downgrade System Image; T1552.001: Credentials In Files; T1016: System Network Configuration Discovery; T1602.002: Network Device Configuration Dump; T1059: Command and Scripting Interpreter; T1571: Non-Standard Port; T1048: Exfiltration Over Alternative Protocol			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Cookie Spider	-	All	Worldwide (Except Russia)
	MOTIVE		
	Information Theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	SHAMOS	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0010: Exfiltration; TA0006: Credential Access; TA0005: Defense Evasion; TA0003: Persistence; TA0009: Collection; T1041: Exfiltration Over C2 Channel; T1583.001: Domains; T1583: Acquire Infrastructure; T1189: Drive-by Compromise; T1204: User Execution; T1027.010: Command Obfuscation; T1027: Obfuscated Files or Information; T1105: Ingress Tool Transfer; T1059.002: AppleScript; T1059: Command and Scripting Interpreter; T1555: Credentials from Password Stores; T1555.001: Keychain; T1005: Data from Local System			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Salt Typhoon (aka GhostEmperor, OPERATOR PANDA, RedMike, UNC5807, FamousSparrow)	China	Telecommunications, Government, Transportation, Lodging, Military	United States, Australia, Canada, New Zealand, United Kingdom
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2024-21887 CVE-2023-46805 CVE-2024-3400 CVE-2023-20273 CVE-2023-20198 CVE-2018-0171	-	Ivanti Connect Secure and Policy Secure, Palo Alto Networks PAN-OS, Cisco IOS XE Software

TTPs
TA0043: Reconnaissance; TA0042: Resource Development; 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; T1090: Proxy; T1090.003: Multi-hop Proxy; T1071: Application Layer Protocol; T1595: Active Scanning; T1590: Gather Victim Network Information; T1590.004: Network Topology; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1584: Compromise Infrastructure; T1584.008: Network Devices; T1588: Obtain Capabilities; T1588.005: Exploits; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1199: Trusted Relationship; T1569: System Services; T1609: Container Administration Command; T1059: Command and Scripting Interpreter; T1059.006: Python; T1059.008: Network Device CLI; T1136: Create Account; T1136.001: Local Account; T1543: Create or Modify System Process; T1543.005: Container Service; T1098: Account Manipulation; T1098.004: SSH Authorized Keys; T1068: Exploitation for Privilege Escalation; T1110: Brute Force; T1110.002: Password Cracking; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1562.004: Disable or Modify System Firewall; T1610: Deploy Container; T1070: Indicator Removal; T1070.009: Clear Persistence; T1599: Network Boundary Bridging; T1040: Network Sniffing; T1556: Modify Authentication Process; T1003: OS Credential Dumping; T1082: System Information Discovery; T1016: System Network Configuration Discovery;T1021: Remote Services; T1021.004: SSH; T1560: Archive Collected Data; T1602.001: SNMP (MIB Dump); T1602.002: Network Device Configuration Dump; T1005: Data from Local System; T1571: Non-Standard Port; T1572: Protocol Tunneling; T1095: Non-Application Layer Protocol; T1048: Exfiltration Over Alternative Protocol

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Storm-0501	-	Critical infrastructure, Government, Law enforcement, Energy, Aerospace, Defense, Healthcare, and Financial services, Agriculture, Media, and Consumer goods	Worldwide
	MOTIVE		
	Financial Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	-

TTPs
TA0040: Impact; TA0001: Initial Access; TA0002: Execution; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0010: Exfiltration; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; T1567.002: Exfiltration to Cloud Storage; T1530: Data from Cloud Storage; T1486: Data Encrypted for Impact; T1485: Data Destruction; T1484: Domain Policy Modification; T1134: Access Token Manipulation; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1484.002: Domain Trust Modification; T1134.002: Create Process with Token; T1003.006: DCSync; T1482: Domain Trust Discovery; T1059: Command and Scripting Interpreter; T1133: External Remote Services; T1078: Valid Accounts; T1078.004: Cloud Accounts; T1059.009: Cloud API; T1098.003: Additional Cloud Roles; T1098: Account Manipulation; T1003: OS Credential Dumping; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1136.001: Local Account; T1059.001: PowerShell; T1136: Create Account; T1087: Account Discovery; T1087.002: Domain Account; T1021: Remote Services; T1567: Exfiltration Over Web Service; T1053.005: Scheduled Task; T1053: Scheduled Task/Job

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1199: Trusted Relationship	
	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
		T1059.008: Network Device CLI
		T1059.009: Cloud API
	T1106: Native API	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
	T1609: Container Administration Command	
	T1610: Deploy Container	
TA0003: Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1133: External Remote Services	
	T1136: Create Account	T1136.002: Domain Account
		T1136.003: Cloud Account

Tactic	Technique	Sub-technique
TA0003: Persistence	T1505: Server Software Component	T1505.003: Web Shell
		T1505.004: IIS Components
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1556: Modify Authentication Process	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1542.005: TFTP Boot
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	T1098.003 : Additional Cloud Roles
		T1098.004: SSH Authorized Keys
	T1134: Access Token Manipulation	T1134.002: Create Process with Token
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
		T1484.002: Domain Trust Modification
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
		T1484.002: Domain Trust Modification
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
		T1027.010: Command Obfuscation
		T1027.011: Fileless Storage
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.001: Invalid Code Signature
		T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.004: File Deletion
		T1070.009: Clear Persistence
	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.003: Local Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	T1134.002: Create Process with Token
	T1497: Virtualization/Sandbox Evasion	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.003: Impair Command History Logging
		T1562.004: Disable or Modify System Firewall
		T1562.006: Indicator Blocking
	T1564: Hide Artifacts	T1564.003: Hidden Window
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1599: Network Boundary Bridging	
	T1601: Modify System Image	T1601.002: Downgrade System Image
	T1610: Deploy Container	
	T1620: Reflective Code Loading	
		T1542.005: TFTP Boot
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.006: DCSync
	T1040: Network Sniffing	
	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	T1110.002: Password Cracking
	T1552: Unsecured Credentials	T1552.001: Credentials In Files

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1555: Credentials from Password Stores	T1555.001: Keychain T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
TA0007: Discovery	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	T1518.001: Security Software Discovery
		T1614.001: System Language Discovery
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol T1021.002: SMB/Windows Admin Shares T1021.004: SSH
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.001: Local Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1185: Browser Session Hijacking	
	T1530: Data from Cloud Storage Object	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
		T1602.002: Network Device Configuration Dump

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.002: File Transfer Protocols
		T1071.003: Mail Protocols
		T1071.004: DNS
	T1090: Proxy	T1090.001: Internal Proxy
		T1090.003: Multi-hop Proxy
	T1095: Non-Application Layer Protocol	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1499: Endpoint Denial of Service	
	T1531: Account Access Removal	
	T1565: Data Manipulation	
	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server
		T1584.006: Web Services
	T1586: Compromise Accounts	
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.006: SEO Poisoning
TA0043: Reconnaissance	T1590: Gather Victim Network Information	T1590.004: Network Topology
	T1594: Search Victim-Owned Websites	
	T1595: Active Scanning	
	T1596: Search Open Technical Databases	T1596.005: Scan Databases
		T1598.002: Spearphishing Attachment

Top 5 Takeaways

#1

In **August 2025, eleven zero-day** vulnerabilities were discovered, with the '**One Celebrity Vulnerability**' taking center stage. This included a flaw named **BadSuccessor.**

#2

Ransomware continued its surge, with relentless strains like **SafePay, MedusaLocker, Charon**, and **Crypto24** claiming new victims. As attacks grow more sophisticated, organizations must act quickly by strengthening defenses, securing backups, and refining disaster recovery plans to stay ahead of the threat.

#3

A diverse array of malware families was also detected actively targeting victims in real-world environments. These included **Plague, CastleBot, DarkCloud, GodRAT**, and **SHAMOS**.

#4

Cyber threat activity in August 2025 was predominantly concentrated in the **United Kingdom, Singapore, United States, Canada,** and **Switzerland**, where malicious campaigns spanned ransomware, botnets, and custom malware deployments.

#5

Key sectors under attack included **Defense, Media, Manufacturing, Telecommunications**, and **Financial services**, with attackers focusing on disrupting critical operations and stealing sensitive information.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **19 significant vulnerabilities** and block the indicators related to the **8 active threat actors, 25 active malware,** and **195 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 **19 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).

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
ApolloShadow	SHA256	13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20
Warlock	SHA256	da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb
4L4MD4R	SHA256	33067028e35982c7b9fdcfe25eb4029463542451fdff454007832cf953feaf1e
	Domain	bpp[.]theinnovationfactory[.]it
	IPv4	145[.]239[.]97[.]206
RoKRAT	MD5	a2ee8d2aa9f79551eb5dd8f9610ad557, ae7e18a62abb7f93b657276dcae985b9, d5fe744b9623a0cc7f0ef6464c5530da, 5ed95cde6c29432a4f7dc48602f82734, 16a8aaaf2e3125668e6bfb1705a065f9, 64d729d0290e2c8ceaa6e38fa68e80e9, e4813c34fe2327de1a94c51e630213d1
Plague	SHA256	85c66835657e3ee6a478a2e0b1fd3d87119bebadc43a16814c30eb94c53766bb, 7c3ada3f63a32f4727c62067d13e40bcb9aa9cbec8fb7e99a319931fc5a9332e, 9445da674e59ef27624cd5c8ffa0bd6c837de0d90dd2857cf28b16a08fd7dba6, 5e6041374f5b1e6c05393ea28468a91c41c38dc6b5a5230795a61c2b60ed14bc, 6d2d30d5295ad99018146c8e67ea12f4aaa2ca1a170ad287a579876bf03c2950, e594bca43ade76bbaab2592e9eabeb8dca8a72ed27afd5e26d857659ec173261, 14b0c90a2eff6b94b9c5160875fcf29aff15dcfdfd3402d953441d9b0dca8b39
SafePay	SHA256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526, 4fe8c6ccdfbcbf6714472e805447fd727d3e46525bd44baf08e5887f890ffb88, 22df7d07369d206f8d5d02cf6d365e39dd9f3b5c454a8833d0017f4cf9c35177,

Attack Name	TYPE	VALUE
SafePay	SHA256	0f23a313f79d54ae2102f193d3de1a6a98791c27921f28a4fab1092bcb43e5ee, 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917, f0127e786c9fb7bf2c8c999202d95c977af4c26cc27302a6ee352cfd62869e7b, 94244ec2480addeaebb43aebbe48cee94f7f429231aa054f4c26f671653163b0, b3045308a07e46c9f7dd98d352e964f242307ce30df8087dc751488118b5b959, ba1b89023581a0bc7a75f8ede9ec6115d5dda98c0145634f1b98978fbc79c956, 7f33c939f7aaf46945d58ed7fd0d1f5c7e3de1ff6a1a591ecc1992dab2a65078, fa74ac0e05b6209b7691511572386f97464ff5728732de99ddd6b5449ffae386, 2f49bff45cc091a7bf52dcd061d24f9a7f2cf0ca9b3c12123bd3cf2fac56b481
	TOR Address	safepaypfxntwixwjrlcscft433ggemlhgkkdupi2ynhtcmvdgubmoyd[.]onion
Qdoor	SHA256	0cc25cf9f5d4f02c1a2ed014e2d4acb0d383f01c9bb1852a10b933eec17c1f20, 5d2e7ed8f77bc95302e693312f9a154f0afb698a05796561e277c037deb15a9d, 6d208e99cfac9b2a32df042889636db6217cd12de1980aca7d9678160bf58d4d, 87db51984bfcadf9ee96183f0fe0fb5129b4cfe5a23a68c272b94299267779ea,
MedusaLocker	SHA256	c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7
CastleBot	URLs	hxxp[:]//173[.]44[.]141[.]89/service/download/data_4x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/download/data_3x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/,

Attack Name	TYPE	VALUE
CastleBot	URL	hxxp[:]//mhousecreative [.]com/service/, hxxp[:]//80[.]77[.]23[.]48/service/, hxxp[:]//62[.]60[.]226[.]73/service/, hxxp[:]//107[.]158[.]128[.]45/service/, hxxp[:]//62[.]60[.]226[.]73/service/
	SHA256	202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04, d6eea6cf20a744f3394fb0c1a30431f1ef79d6992b552622ad17d86490b7aa7b, cbaf513e7fd4322b14adcc34b34d793d79076ad310925981548e8d3cff886527, e6aab1b6a150ee3cbc721ac2575c57309f307f69cd1b478d494c25cde0baaf85, b45cce4ede6ffb7b6f28f75a0cbb60e65592840d98dcb63155b9fa0324a88be2, 8bf93cef46fda2bdb9d2a426fbcd35ffedea9ed9bd97bf78cc51282bd1fb2095, 53dddae886017fbfbb43ef236996b9a4d9fb670833dfa0c3eac982815dc8d2a5
DarkCloud	SHA256	bd8c0b0503741c17d75ce560a10eeeaa0cdd21dff323d9f1644c62b7b8eb43d9, 9588c9a754574246d179c9fb05fea9dc5762c855a3a2a4823b402217f82a71c1, 6b8a4c3d4a4a0a3aea50037744c5fec26a38d3fb6a596d006457f1c51bbc75c7, f6d9198bd707c49454b83687af926ccb8d13c7e43514f59eac1507467e8fb140, 24552408d849799b2cac983d499b1f32c88c10f88319339d0eec00fb01bb19b4, ce3a3e46ca65d779d687c7e58fb4a2eb784e5b1b4cebe33dbb2bf37cccb6f194, 381aa445e173341f39e464e4f79b89c9ed058631bcbbb2792d9ecbdf9ffe027d, 82ba4340be2e07bb74347ade0b7b43f12cf8503a8fa535f154d2e228efbef69c
Efimer	MD5	39fa36b9bfcf6fd4388eb586e2798d1a, 16057e720be5f29e5b02061520068101, 100620a913f0e0a538b115dbace78589
	SHA256	6199960f2ec96d4851e4f36d5a5095922e422e3b4265bdb537ccdbb8d44ac8dc, 3e9e666b06d3708ab9591454ac119e276bcaea7f7e6c4b8e5c349c9baa3c0faa, 006c397ec5b65e0c646598ee6014813ff601802d927fb90571e5ad1204d7f70f
Charon	SHA256	80711e37f226ef1dc86dc80a8cbc0b2ec895b361e9ade85da793d94b1d876be8, 739e2cac9e2a15631c770236b34ba569aad1d1de87c6243f285bf1995af2cdc2

Attack Name	TYPE	VALUE
Charon	SHA1	92750eb5990cdcda768c7cb7b654ab54651c058a, a1c6090674f3778ea207b14b1b55be487ce1a2ab
SWORDLDR	SHA256	e0a23c0d99c45d40f6ef99c901bacf04bb12e9a3a15823b663b392abadd2444e
	SHA1	21b233c0100948d3829740bd2d2d05dc35159ccb
Mythic	SHA256	e0cbe8f18315a2ee781de48565dc8a087a1564557c42c66067f65c267120c894
	SHA1	ae687bef963cb30a3788e34cc18046f54c41ffba
	IPv4	194[.]36[.]209[.]127
	Domain	srlaptop[.]com
SnipBot	SHA256	8082956ace8b016ae8ce16e4a777fe347c7f80f8a576a6f935f9d636a30204e7
	SHA1	1aea26a2e2a7711f89d06165e676e11769e2fd68
	IPv4	185[.]173[.]235[.]134
	Domain	campanole[.]com
RustyClaw	SHA256	0517d413beb3e124e773d7ccc1983b226d6593d1f46a81ba7e79a8b48d6242fa
	SHA1	ab79081d0e26ea278d3d45da247335a545d0512e
	IPv4	85[.]158[.]108[.]62
	Domain	melamorri[.]com
PS1Bot	SHA256	809f4ffef71ab43d692d4fececf1dfefffb0854ae1f15486960b1c198c47c69f
Noodlophile	SHA256	8773071c5a06eafa8b6a4dc102422583c0fe18890667b9fff53f5d5e78991d81, 4b7d98e3bf3b6c1c20e735e21b8f98c15f2ed032ce1a54a09deb303d22bebac5, 6082396e63f134eed71fb16e30e975cc43810c0b091cd0387966df934d88fcd0, ac358f3465c63f41eea6539a42fd4ee8b32ca63cbb52ec3de7df303314543f30, 0009e715036493ca4bada2c99287654f57e66173c10c6aae424d1cce16f0dd51, 11c873cee11fd1d183351c9cdf233cf9b29e28f5e71267c2cb1f373a564c6a73
GodRAT	MD5	d09fd377d8566b9d7a5880649a0192b4, e723258b75fee6fbd8095f0a2ae7e53c, 318f5bf9894ac424fd4faf4ba857155e, 512778f0de31fcce281d87f00affa4a8, 6cad01ca86e8cd5339ff1e8fff4c8558, 58f54b88f2009864db7e7a5d1610d27d, 64dfcdd8f511f4c71d19f5a58139f2c0, 8008375eec7550d6d8e0eaf24389cf81, 04bf56c6491c5a455efea7dbf94145f1, 5f7087039cb42090003cc9dbb493215e

Attack Name	TYPE	VALUE
GodRAT	SHA256	0E2889F6475AEA625D18B200A2CACDAC745ECB22044F6366F21AFC2E24046025, C52FB4EDDF64779B7BEDA43D26618251EEFE84BBB7F1C8EBB725E5E2DFDCFE4A, 2E33A3C604C4212547BDBB31BD842B365EF28EB7B9A84564FB8EF3C0268F6268, 51B7478388593F90516D04053B95DD0861D93D6195341B36272D2474D196BA86, CED343EE088F8FDDAF74D3B85C0D9176A3DB852E580467CA6C60EC86BD5E2132, 67C713A44186315D7CBFEC4745B7DD199D86711F48C5F0778A71871AC3B02624, B673444DAF876EEFF6AA81BFCD86F68FA7E5C4C48EFFF183D94EDFBB57D93EF5
	IPV4	103[.]237[.]92[.]191, 118[.]99[.]3[.]33, 118[.]107[.]46[.]174, 154[.]91[.]183[.]174
AsyncRAT	MD5	605f25606bb925d61ccc47f0150db674, 961188d6903866496c954f03ecff2a72, 4ecd2cf02bdf19cdbc5507e85a32c657, 17e71cd415272a6469386f95366d3b64
	SHA256	ED1DFD2E913E1C53D9F9AB5B418F84E0F401ABFDF8E3349E1FCFC98663DCB23F, C5F5D5A9BA824E235ABD02E9D09052CA8A17B8C18253C7B25727A17DF675E66B, 8A1A19741DC3626CFF78E1C54DE827058060A42F3ACADDF6D5C3DEBE7071185B
	Domain	wuwu6[.]cfd
	IPv4	156[.]241[.]134[.]49, 47[.]238[.]124[.]68
Crypto24 Ransomware	SHA256	10c3317566f52eaeb45294a544c8038cf132240a9d12aef95c0658d6a49f4d91, 79e349ed7488a90438fd4b72da5cfd8d844509aa48973a9aa1a9852d801dc08b, 0e36b1837e5a2cbd14fac2c3b709a5470b7b488bd15898d30840ec60448e83e0, 3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac, 686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac, 24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73

Attack Name	TYPE	VALUE
QuirkyLoader	SHA256	011257eb766f2539828bdd45f8aa4ce3c4048ac2699d988329783290a7b4a0d3, 0ea3a55141405ee0e2dfbf333de01fe93c12cf34555550e4f7bb3fdec2a7673b, a64a99b8451038f2bbcd322fd729edf5e6ae0eb70a244e342b2f8eff12219d03, 9726e5c7f9800b36b671b064e89784fb10465210198fbbb75816224e85bd1306, a1994ba84e255eb02a6140cab9fc4dd9a6371a84b1dd631bd649525ac247c111, d954b235bde6ad02451cab6ee1138790eea569cf8fd0b95de9dc505957c533cd, 5d5b3e3b78aa25664fb2bfdbf061fc1190310f5046d969adab3e7565978b96ff, 6f53c1780b92f3d5affcf095ae0ad803974de6687a4938a2e1c9133bf1081eb6, ea65cf2d5634a81f37d3241a77f9cd319e45c1b13ffbaf5f8a637b34141292eb, 1b8c6d3268a5706fb41ddfff99c8579ef029333057b911bb4905e24aacc05460, d0a3a1ee914bcbfcf709d367417f8c85bd0a22d8ede0829a66e5be34e5e53bb9, b22d878395ac2f2d927b78b16c9f5e9b98e006d6357c98dbe04b3fd78633ddde, a83aa955608e9463f272adca205c9e1a7cbe9d1ced1e10c9d517b4d1177366f6, 3391b0f865f4c13dcd9f08c6d3e3be844e89fa3afbcd95b5d1a1c5abcacf41f4, b2fdf10bd28c781ca354475be6db40b8834f33d395f7b5850be43ccace722c13, bf3093f7453e4d0290511ea6a036cd3a66f456cd4a85b7ec8fbfea6b9c548504, 97aee6ca1bc79064d21e1eb7b86e497adb7ece6376f355e47b2ac60f366e843d, b42bc8b2aeec39f25babdcbbdaab806c339e4397debfde2ff1b69dca5081eb44, 5aaf02e4348dc6e962ec54d5d31095f055bd7fb1e58317682003552fd6fe25dc, 8e0770383c03ce69210798799d543b10de088bac147dce4703f13f79620b68b1, 049ef50ec0fac1b99857a6d2beb8134be67ae67ae134f9a3c53699cdaa7c89ac, cba8bb455d577314959602eb15edcaa34d0b164e2ef9d89b08733ed64381c6e0
	IPv4	103[.]75[.]77[.]90,161[.]248[.]178[.]212

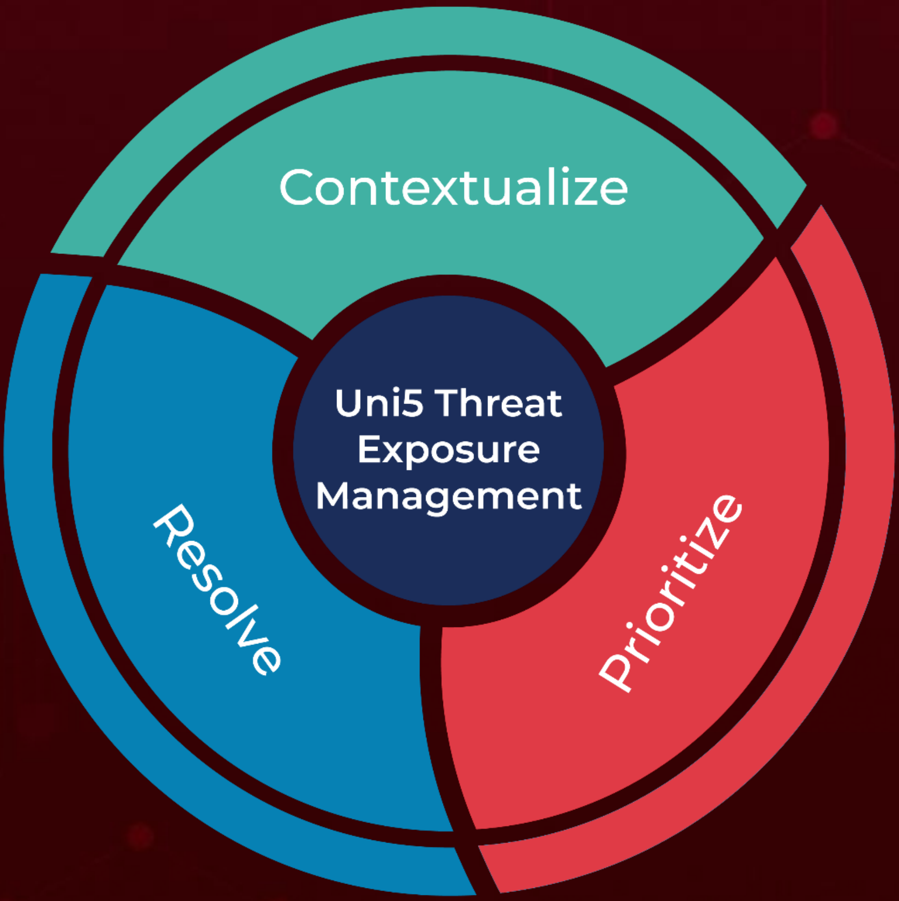
Attack Name	TYPE	VALUE
SHAMOS	SHA256	4549e2599de3011973fde61052a55e5cdb770348876abc82de14c2d99575790f, b01c13969075974f555c8c88023f9abf891f72865ce07efbcee6c2d906d410d5, a4e47fd76dc8ed8e147ea81765edc32ed1e11cff27d138266e3770c7cf953322, 95b97a5da68fcb73c98cd9311c56747545db5260122ddf6fae7b152d3d802877
	URLs	hxxps[:]//icloudservers[.]com/gm/update, hxxps[:]//macostutorial[.]com/iterm2/update
MixShell	SHA256	d39e177261ce9a354b4712f820ada3ee8cd84a277f173ecfbd1bf6b100ddb713

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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 2, 2025 • 4:45 AM

More at www.hivepro.com