Date of Publication
September 8, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

1 to 7 SEPTEMBER 2025

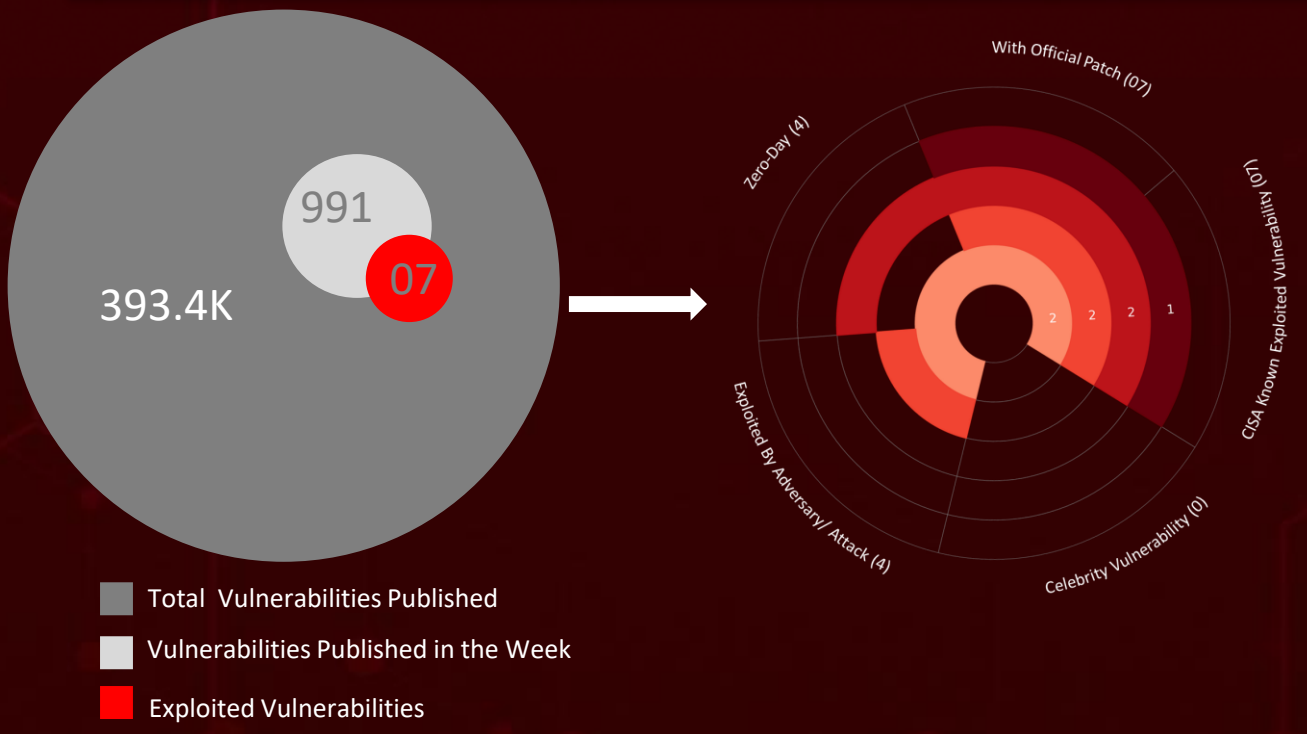
Table Of Contents

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **ten** major attacks were detected, **seven** critical vulnerabilities were actively exploited, and **three** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

Among the most alarming discoveries is a zero-day vulnerability in Sitecore, **CVE-2025-53690**, actively exploited in the wild. By leveraging a hidden ViewState deserialization flaw, attackers deployed the **WEEPSTEEL** malware, quietly mapping networks, exfiltrating configuration files, and probing deep into Active Directory environments. Meanwhile, a flaw in WhatsApp's iOS and macOS apps (**CVE-2025-55177**) has been exploited in targeted zero-day campaigns, often chained with Apple's CVE-2025-43300, demonstrating how attackers are blending multiple vulnerabilities to maximize impact.

The threat landscape is further complicated by emerging actors like **GhostRedirector**, a China-aligned group targeting Windows servers globally since 2024, which has compromised at least 65 servers by mid-2025. Using SQL injection flaws, public exploits, and deploying backdoors like **Rungan** alongside IIS malware **Gamshen**, the group exemplifies the growing scale of cyber aggression. Meanwhile, the **Quad7** botnet is actively exploiting two critical TP-Link router flaws (**CVE-2023-50224** and **CVE-2025-9377**) to steal credentials and launch large-scale password spray attacks on Microsoft 365 accounts. Collectively, these developments highlight the urgent need for proactive defense, rapid patching, and resilient cybersecurity strategies in an increasingly hostile digital environment.



High Level Statistics

10
Attacks Executed

7
Vulnerabilities Exploited

3
Adversaries in Action

- RokRAT
- NightSpire
- PromptLock
- Rungan
- Gamshen
- Quad 7 (7777)
- WEEPSTEEL
- EARTHWORM
- DWAGENT
- SHARPHOUND

- CVE-2025-7775
- CVE-2024-55591
- CVE-2025-55177
- CVE-2025-43300
- CVE-2023-50224
- CVE-2025-9377
- CVE-2025-53690

- APT37
- GhostRedirector
- Storm-0940

Insights

NightSpire the RaaS newcomer of 2025, is cracking networks wide open by weaponizing FortiOS flaw CVE-2024-55591.

A zero-day in **Sitecore** (**CVE-2025-53690**) is under active attack, with a hidden ViewState deserialization flaw letting hackers run code, deploy WEEPSTEEL malware.

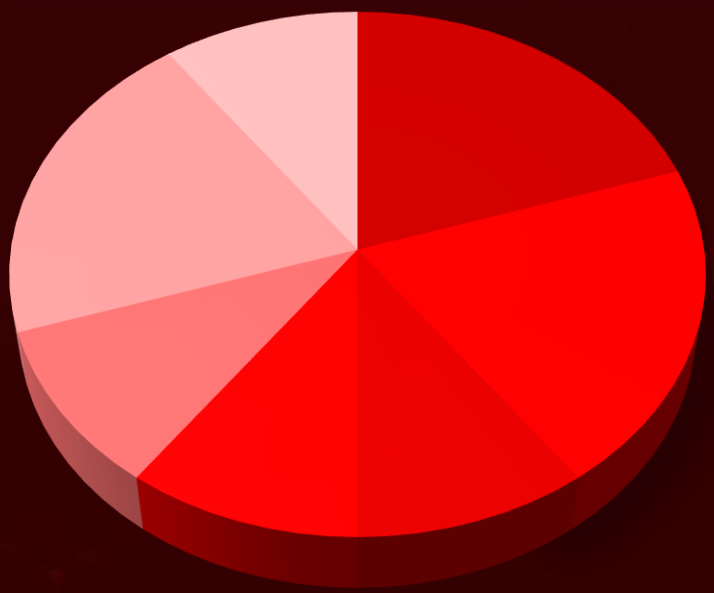
PromptLock, the first AI-powered ransomware written in Golang, uses large language models to spin up malicious code on the fly, making it harder to catch and stop.

CVE-2025-55177, a flaw in WhatsApp's iOS and macOS apps, was hit in targeted zero-day attacks, chained with Apple's CVE-2025-43300 for a powerful exploit combo.

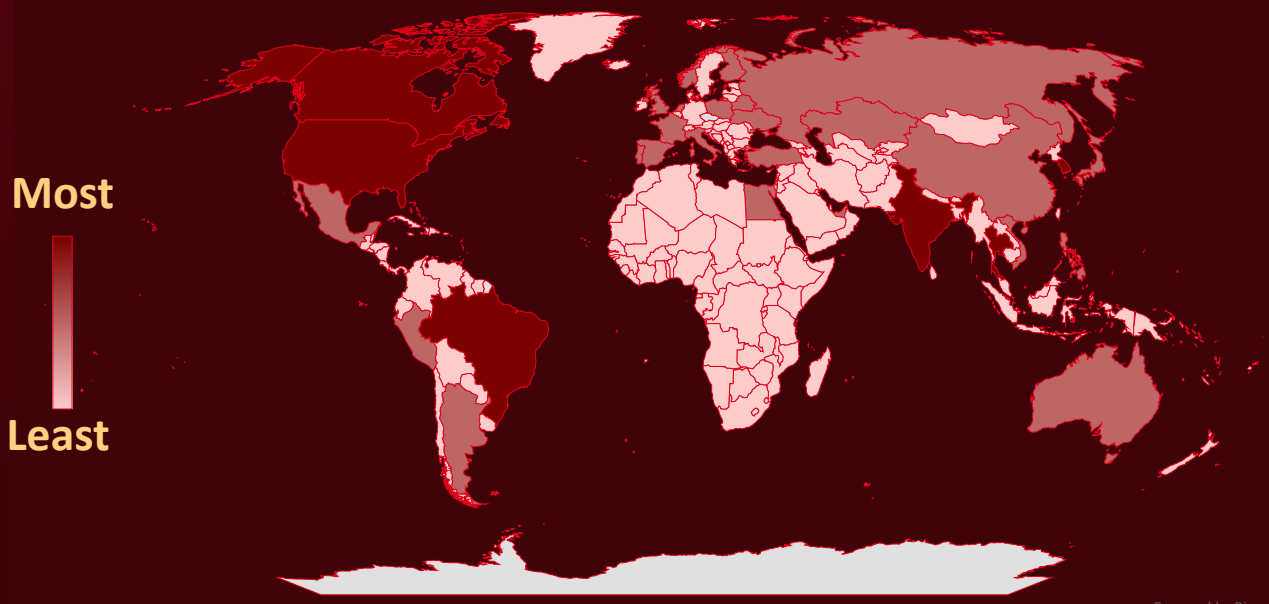
GhostRedirector a China-backed hacker crew, has been hijacking Windows servers globally since 2024, leaving at least 65 victims in its trail by mid-2025.

Quad7 botnet is weaponizing two critical TP-Link router flaws (CVE-2023-50224 and CVE-2025-9377) to steal credentials and run malicious code.

Threat Distribution



Targeted Countries



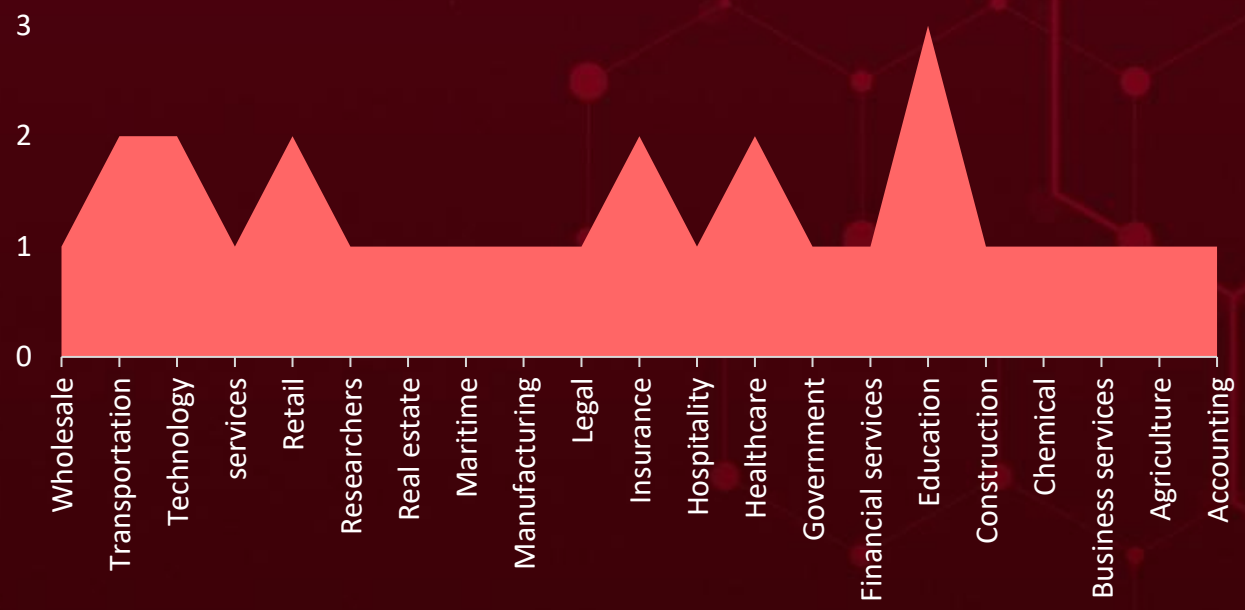
Countries
India
Thailand
South Korea
Brazil
Canada
United States
Peru
Ukraine
Russia
Australia
Netherlands
Belarus
Poland
China
Spain
Egypt
Mexico
Finland
Norway
France
Philippines
Italy
Portugal
Japan
Singapore

Countries
Kazakhstan
Turkey
United Kingdom
United Arab Emirates
Argentina
Vietnam
Solomon Islands
Niger
Mauritius
Central African Republic
Romania
Chad
Tanzania
Chile
Mozambique
Austria
Panama
Colombia
Saudi Arabia
Comoros
State of Palestine
Congo
Turkmenistan
Costa Rica
Monaco

Countries
Côte d'Ivoire
Nepal
Croatia
Bolivia
Cuba
Botswana
Cyprus
Saint Lucia
Czech Republic (Czechia)
Sierra Leone
Denmark
South Sudan
Djibouti
Switzerland
Dominica
Tonga
Dominican Republic
Cameroon
DR Congo
Micronesia
Ecuador
Montenegro
Azerbaijan
Namibia
El Salvador

Countries
New Zealand
Equatorial Guinea
North Korea
Eritrea
Pakistan
Estonia
Paraguay
Eswatini
Brunei
Ethiopia
Rwanda
Fiji
San Marino
Bahamas
Serbia
Bahrain
Slovakia
Gabon
South Africa
Gambia
Sri Lanka
Georgia
Suriname
Germany
Taiwan

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1588
Obtain Capabilities

T1190
Exploit Public-Facing Application

T1203
Exploitation for Client Execution

T1083
File and Directory Discovery

T1068
Exploitation for Privilege Escalation

T1041
Exfiltration Over C2 Channel

T1110
Brute Force

T1090
Proxy

T1588.006
Vulnerabilities

T1059.001
PowerShell

T1071.001
Web Protocols

T1071
Application Layer Protocol

T1078
Valid Accounts

T1588.002
Tool

T1583
Acquire Infrastructure

T1204.001
Malicious Link

T1082
System Information Discovery

T1587.001
Malware

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RokRAT	RokRAT is a sophisticated remote access trojan that collects sensitive system data, captures live screenshots, monitors processes, and maintains encrypted command-and- control communications via cloud APIs on services like Dropbox, pCloud, and Yandex.	Using fake newsletters and weaponized shortcut files	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft	-
RAT			
ASSOCIATED ACTOR			PATCH LINK
APT37			-
IOC TYPE	VALUE		
SHA256	3fa06c290c477c133ca58512c7852fc998632721f2dc3a0984f18fbe86451e18		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
NightSpire	NightSpire is a ransomware group that surfaced in February 2025, quickly making a name for itself with an aggressive strategy and a structured infrastructure resembling the Ransomware-as-a-Service (RaaS) model. The group runs a Dedicated Leak Site (DLS), where it publishes stolen data from victims alongside a countdown timer, using the threat of public exposure as leverage to pressure organizations into paying ransoms.	Exploiting Vulnerability	CVE-2024-55591
		IMPACT	AFFECTED PRODUCT
TYPE		Encrypt data, Data Theft	Fortinet FortiOS and FortiProxy
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535
IOC TYPE	VALUE		
SHA256	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5		

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
PromptLock	PromptLock is the first known AI-powered ransomware written in Golang. Unlike traditional strains, this proof-of-concept demonstrates how large language models can be leveraged to dynamically generate malicious code, significantly complicating detection and defense. It uses Lua scripts in combination with OpenAI's gpt-oss-20b model through the Ollama API, enabling the ransomware to adapt in ways static signature-based tools struggle to keep up with. PromptLock employs the rarely used SPECK 128-bit encryption algorithm, showcasing a future where ransomware constantly evolves.	-	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft	-
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	2755e1ec1e4c3c0cd94ebe43bd66391f05282b6020b2177ee3b939fdd33216f6, 1612ab799df51a7f1169d3f47ea129356b42c8ad81286d05b0256f80c17d4089, b43e7d481c4fdc9217e17908f3a4efa351a1dab867ca902883205fe7d1aab5e7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Rungan	Rungan is a backdoor written in C++ that quietly establishes persistence on compromised servers. It relies on AES encryption in CBC mode to decrypt its strings, helping it evade simple detection techniques. Once active, Rungan can execute attacker-supplied commands on the victim's server, but it doesn't openly beacon; instead, it listens for incoming HTTP requests that match specific hardcoded patterns.	Through SQL injection flaws	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
GhostRedirector			-
IOC TYPE	**VALUE**		
SHA1	28140A5A29EBA098BC6215DDAC8E56EACBB29B69		

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
Gamshen	Gamshen is a malicious IIS module built as a C/C++ DLL, designed to discreetly manipulate web server traffic. Its primary function is to intercept requests coming specifically from the Googlebot search engine crawler, ensuring that only these requests trigger malicious behavior. When activated, Gamshen alters the legitimate server response, dynamically pulling instructions and data from its command-and-control (C&C) server. This selective targeting allows the malware to tamper with search engine visibility while avoiding detection by regular users, making it a stealthy and strategic tool for attackers.	Through SQL injection flaws	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft	Windows
Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
GhostRedirector			-
IOC TYPE	**VALUE**		
SHA1	08AB5CC8618FA593D2DF91900067DB464DC72B3E, 871A4DF66A8BAC3E640B2D1C0AFC075BB3761954		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Quad 7 (7777)	Quad7, also known as 7777, is a botnet identified by the presence of TCP port 7777 left open on compromised devices, often showing a mysterious xlogin: banner. Its primary role is to deploy SOCKS5 proxies across infected systems, which are then abused to relay brute-force attempts against Microsoft 365 accounts worldwide. These attacks are characterized by their unusually slow pace, likely intended to evade detection while steadily targeting organizations across different sectors.	Exploiting Vulnerabilities	CVE-2023-50224 CVE-2025-9377
		IMPACT	**AFFECTED PRODUCT**
TYPE		Network Compromise	TP-Link Multiple Routers
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
Storm-0940			https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware , https://www.tp-link.com/us/support/faq/4308/
IOC TYPE	**VALUE**		
SHA256	f8a78c33d4f37fd5b367f84536a738bc91d50a76a58d1b595c878f4c4d7f4dd1		

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">WEEPSTEEL</td><td rowspan="6">WEEPSTEEL is a malware tool built for internal reconnaissance, showing similarities to the GhostContainer backdoor in its approach. Its primary purpose is to collect detailed information about the compromised environment, including system details, network configurations, and user data. To avoid detection, the gathered information is encrypted and exfiltrated by masquerading as a harmless __VIEWSTATE response, allowing attackers to stealthily extract valuable intelligence from within targeted networks.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-53690</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Data Theft</td><td rowspan="2">Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud</td></tr>
<tr><td>Reconnaissance Tool</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">a566cceaf9a66332470a978a234a8a8e2bbdd4d6aa43c2c75c25a80b3b744307</td></tr>
</table>

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">EARTHWORM</td><td rowspan="6">EARTHWORM is an open-source network tunneling tool that includes a built-in SOCKS v5 server, often abused by attackers to establish covert channels. By tunneling traffic over alternative protocols, it enables communication to and from a victim system while bypassing detection mechanisms and network filtering. This capability also allows threat actors to reach systems that would otherwise be inaccessible, making EARTHWORM a versatile tool for stealthy lateral movement and persistence within compromised environments.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-53690</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Lateral Movement, persistent access</td><td rowspan="2">Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud</td></tr>
<tr><td>Tunneler</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">b3f83721f24f7ee5eb19f24747b7668ff96da7dfd9be947e6e24a688ecc0a52b</td></tr>
<tr><td>IPv4:Port</td><td colspan="3">130[.]33[.]156[.]194[:]443
103[.]235[.]46[.]102[:]80</td></tr>
</table>

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">DWAGENT</td><td rowspan="6">DWAgent, a legitimate remote access tool, abused by attackers to establish persistent control over compromised systems and conduct Active Directory reconnaissance. To ensure redundancy and continued access, the tool was installed as a service running with SYSTEM privileges, allowing it to start automatically and provide elevated persistence.</td><td>Exploiting Vulnerability</td><td>CVE-2025-53690</td></tr>
<tr><td rowspan="2">IMPACT</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">persistent control</td><td rowspan="3">Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud</td></tr>
<tr><td>Remote Access Tool</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
</table>

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">SHARPHOUND</td><td rowspan="5">SHARPHOUND, an open-source Active Directory (AD) reconnaissance tool, was retrieved via a browser and used to map relationships within the domain. As the data collection component of the BLOODHOUND platform, SHARPHOUND gathers extensive information on AD objects, permissions, and trust relationships, providing attackers with a detailed blueprint of the environment to identify potential privilege escalation paths.</td><td>Exploiting Vulnerability</td><td>CVE-2025-53690</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Reconnaissance</td><td rowspan="2">Sitecore Experience Manager (XM), Experience Platform (XP), andExperience Commerce (XC), Managed Cloud</td></tr>
<tr><td>Reconnaissance Tool</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">61f897ed69646e0509f6802fb2d7c5e88c3e3b93c4ca86942e24d203aa878863</td></tr>
</table>

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-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	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1499: Endpoint Denial of Service	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-2024-55591	✗	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	NightSpire ransomware
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190 : Exploit Public-Facing Application, T1133 : External Remote Services	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-55177	✗	WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, WhatsApp for Mac v2.25.21.78	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:iphone_os:*:* cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:macos:*:* cpe:2.3:a:whatsapp:whatsapp_business:*:*:*:*:*:*:iphone_os:*:*	-
Meta Platforms WhatsApp Incorrect Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1204: User Execution; T1204.001: Malicious Link	https://www.whatsapp.com/download

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-2023-50224		TP-Link TL-WR841N routers	Storm-0940
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tp-link:tl-wr841n_firmware:3.16.9:build_200409:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*	Quad 7 (7777)
TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing	https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-9377</td><td>✗</td><td rowspan="2">Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108</td><td rowspan="2">Storm-0940</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:o:tp-link:tl-wr841n_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841n:v9:*:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:tl-wr841nd_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841nd:9:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:archer_c7_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:archer_c7:2.0:*:*:*:*:*:*:*</td><td rowspan="2">Quad 7 (7777)</td></tr>
<tr><td>TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability</td><td>✓</td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-78</td><td>T1190: Exploit Public-Facing; T1059: Command and Scripting Interpreter</td><td>https://www.tp-link.com/us/support/faq/4308/</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-53690</td><td>  </td><td rowspan="2">Sitecore Experience Manager (XM) and Experience Platform (XP) Through Version 9.0, Experience Commerce (XC), Managed Cloud, AD Version 1.4 and earlier</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:sitecore:experience_platform:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_commerce:*:*:*:*:*:*:*:*</td><td rowspan="2">WEEPSTEEL, EARTHWORM, DWAGENT, SHARPHOUND</td></tr>
<tr><td rowspan="2">Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
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, G0067)	North Korea	Academic, Government officials, and Researchers	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RokRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.001: DLL; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1055: Process Injection; T1055.001: Dynamic-link Library Injection; T1055.009: Proc Memory; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1056: Input Capture; T1056.002: GUI Input Capture; T1087: Account Discovery; T1087.001: Local Account; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1082: System Information Discovery; T1123: Audio Capture; T1005: Data from Local System; T1113: Screen Capture; T1102: Web Service; T1102.002: Bidirectional Communication; T1041: Exfiltration Over C2 Channel; T1529: System Shutdown/Reboot

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 GhostRedirector	China	Education, Healthcare, Insurance, Transportation, Technology, Retail	Brazil, Peru, Thailand, Vietnam, United States, Canada, Finland, India, Netherlands, Philippines, Singapore
	MOTIVE		
	Information theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	Rungan, Gamshen	-

TTPs
TA0005: Defense Evasion; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0006: Credential Access; TA0040: Impact; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; T1112: Modify Registry; T1027.009: Embedded Payloads; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation; T1008: Fallback Channels; T1565: Data Manipulation; T1588.002: Tool; T1588: Obtain Capabilities; T1083: File and Directory Discovery; T1219: Remote Access Software; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1587: Develop Capabilities; T1587.001: Malware; T1608.006: SEO Poisoning; T1608: Stage Capabilities; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1134: Access Token Manipulation; T1608.001: Upload Malware; T1608.002: Upload Tool; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1588.003: Code Signing Certificates; T1190: Exploit Public-Facing Application; T1106: Native API; T1559: Inter-Process Communication; T1546: Event Triggered Execution

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-0940	China	All	Worldwide
	MOTIVE		
	Information theft		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2023-50224 CVE-2025-9377	Quad 7 (7777) Botnet	TP-Link Multiple Routers
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0040: Impact; T1078: Valid Accounts; T1110: Brute Force; T1110.003: Password Spraying; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1110: Brute Force; T1087: Account Discovery; T1046: Network Service Discovery; T1090: Proxy; T1090.003: Multi-hop Proxy; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1571: Non-Standard Port; T1496: Resource Hijacking			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actor **APT37, GhostRedirector, Storm-0940,** and malware **RokRAT, NightSpire, PromptLock Ransomware, Rungan, Gamshen, Quad 7 (7777) Botnet, WEEPSTEEL, EARTHWORM, DWAGENT, SHARPHOUND.**

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

- Run a Scan to discover the assets impacted by the **seven exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT37, GhostRedirector, Storm-0940,** and malware **NightSpire, PromptLock Ransomware, Quad 7 (7777) Botnet, EARTHWORM, SHARPHOUND,** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2025-7775: Actively Exploited Critical Flaw in Citrix NetScaler

Operation HanKook Phantom: APT37's Stealthy Espionage Campaign

NightSpire Ransomware Expands Reach with Aggressive Extortion Deadlines

Experimental AI Ransomware PromptLock Sparks Security Concerns

CVE-2025-55177: WhatsApp Zero-Click Flaw Used in Targeted Campaigns

GhostRedirector Targets Windows Servers Globally for SEO Fraud

TP-Link Router End-of-Service Models Exploited in Botnet Operation

Sitecore Zero-Day Powers Reconnaissance Malware

Appendix

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

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

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
RokRAT	SHA256	3fa06c290c477c133ca58512c7852fc998632721f2dc3a0984f18fbe86451e18, 81fb0b9310ec3a4afb7fc107281d5c13f87fcf2b5cd151dd273f8f910a2cffc3, 8de48bd7eca096eb10a5023d245e5cb83e2fce7efdfde91cb86f89623b001535
NightSpire	SHA256	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
PromptLock	SHA256	2755e1ec1e4c3c0cd94ebe43bd66391f05282b6020b2177ee3b939fdd33216f6, 1612ab799df51a7f1169d3f47ea129356b42c8ad81286d05b0256f80c17d4089, b43e7d481c4fdc9217e17908f3a4efa351a1dab867ca902883205fe7d1aab5e7, 09bf891b7b35b2081d3ebca8de715da07a70151227ab55aec1da26eb769c006f, e24fe0dd0bf8d3943d9c4282f172746af6b0787539b371e6626bdb86605ccd70, 1458b6dc98a878f237bfb3c3f354ea6e12d76e340cefe55d6a1c9c7eb64c9aee
Rungan	SHA1	28140A5A29EBA098BC6215DDAC8E56EACBB29B69

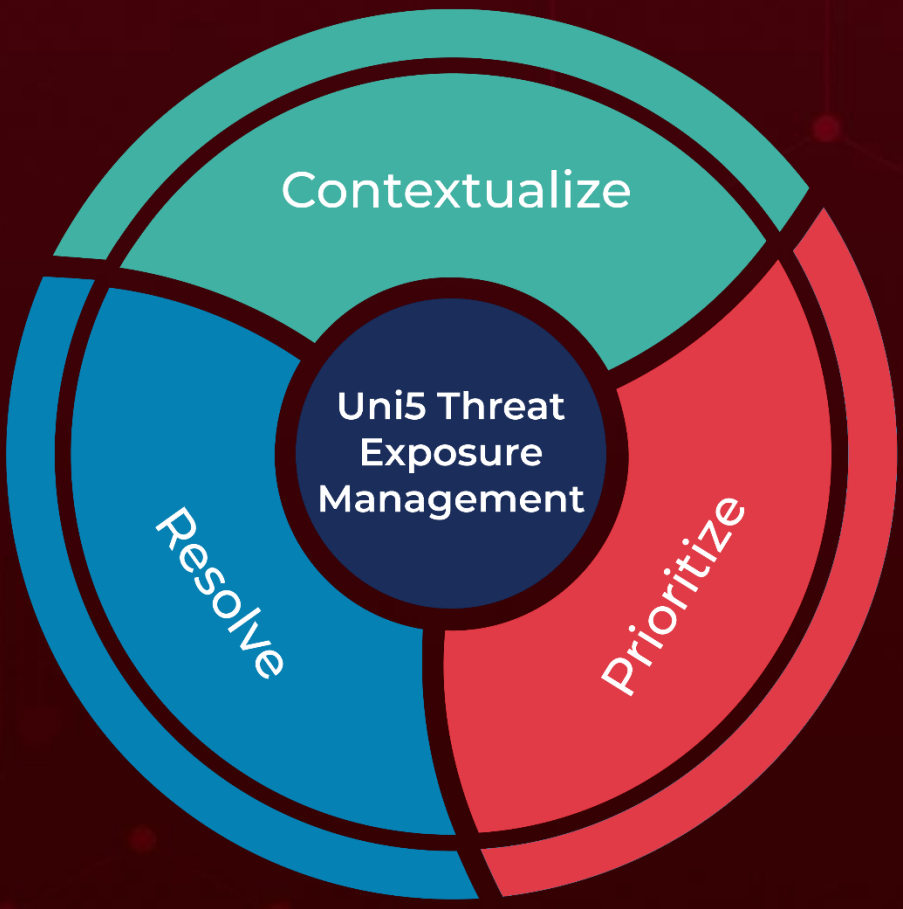
Attack Name	TYPE	VALUE
Gamshen	SHA1	08AB5CC8618FA593D2DF91900067DB464DC72B3E, 871A4DF66A8BAC3E640B2D1C0AFC075BB3761954
	Domain	gobr.868id[.]com, brproxy.868id[.]com
Quad 7	SHA256	f8a78c33d4f37fd5b367f84536a738bc91d50a76a58d1b595c878f4c4d7f4dd1
WEEPSTEEL	SHA256	a566cceaf9a66332470a978a234a8a8e2bbdd4d6aa43c2c75c25a80b3b744307
	MD5	117305c6c8222162d7246f842c4bb014
EARTHWORM	IPv4:Port	130[.]33[.]156[.]194[:]443, 103[.]235[.]46[.]102[:]80
	SHA256	b3f83721f24f7ee5eb19f24747b7668ff96da7dfd9be947e6e24a688ecc0a52b
	MD5	a39696e95a34a017be1435db7ff139d5
SHARPHOUND	MD5	63d22ae0568b760b5e3aabb915313e44
	SHA256	61f897ed69646e0509f6802fb2d7c5e88c3e3b93c4ca86942e24d203aa878863

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 8, 2025 . 7:00 AM

More at www.hivepro.com