

Date of Publication  
August 11, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

4 to 10 AUGUST 2025

# Table Of Contents

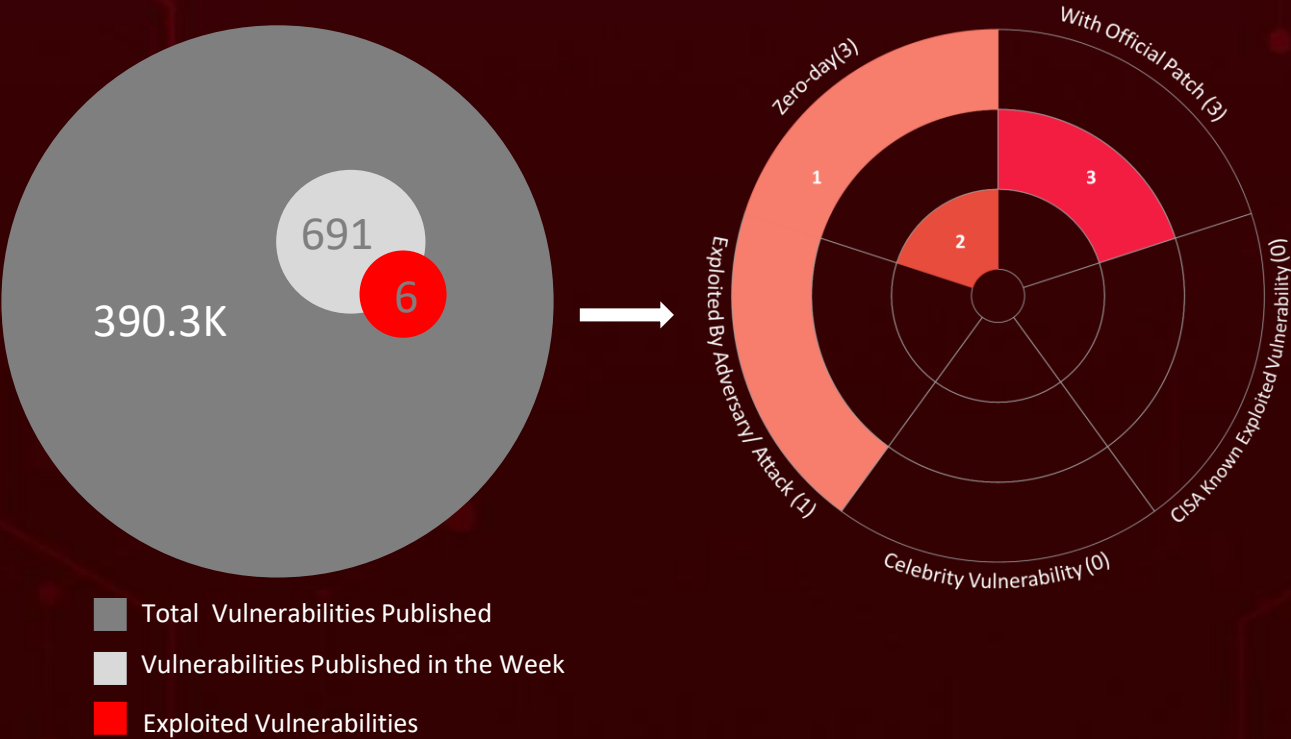
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	13
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	22

# Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **seven** major attacks were detected, **six** critical vulnerabilities were actively exploited, and **one** threat actor was closely monitored, reflecting an alarming escalation in malicious activities.

In August 2025, **Adobe** urgently patched three critical AEM Forms on JEE flaws (CVE-2025-49533, CVE-2025-54253, CVE-2025-54254) enabling remote code execution and file access, after public exploit details emerged. **Trend Micro** found two zero-day flaws in Apex One On-Premise Console, one already exploited, allowing remote code execution without login.

Additionally, **SafePay**, emerged in September 2024, is a fast-growing private ransomware group behind 200+ attacks in 2025, targeting MSPs and SMBs in the US, Germany, and beyond while avoiding CIS countries. A BYOVD attack exploiting ThrottleStop.sys (CVE-2025-7771) lets attackers disable AV/EDR via kernel memory access. In Brazil, it was used with stolen RDP creds to deploy **MedusaLocker**. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

7

Attacks  
Executed

- [Warlock](#)
- [4L4MD4R](#)
- [RoKRAT](#)
- [Plague](#)
- [SafePay](#)
- [Qdoor](#)
- [MedusaLocker](#)

6

Vulnerabilities  
Exploited

- [CVE-2025-49533](#)
- [CVE-2025-54253](#)
- [CVE-2025-54254](#)
- [CVE-2025-54948](#)
- [CVE-2025-54987](#)
- [CVE-2025-7771](#)

1

Adversaries in  
Action

- [APT37](#)



# Insights

## **BYOVD** attack

exploiting ThrottleStop.sys flaw (**CVE-2025-7771**) to disable AV/EDR and enabled MedusaLocker deployment.

## **Malicious npm**

packages targeting WhatsApp integration devs use a whitelist-based kill switch to wipe systems, marking a precise, targeted supply chain attack.

**APT37's** new **RoKRAT** variant uses LNK files and JPEG steganography in a fileless attack to spy on South Korean targets, exfiltrating data via cloud services.

**Adobe** patched three critical AEM Forms on JEE RCE flaws (CVSS up to 10) only after public exploits surfaced.

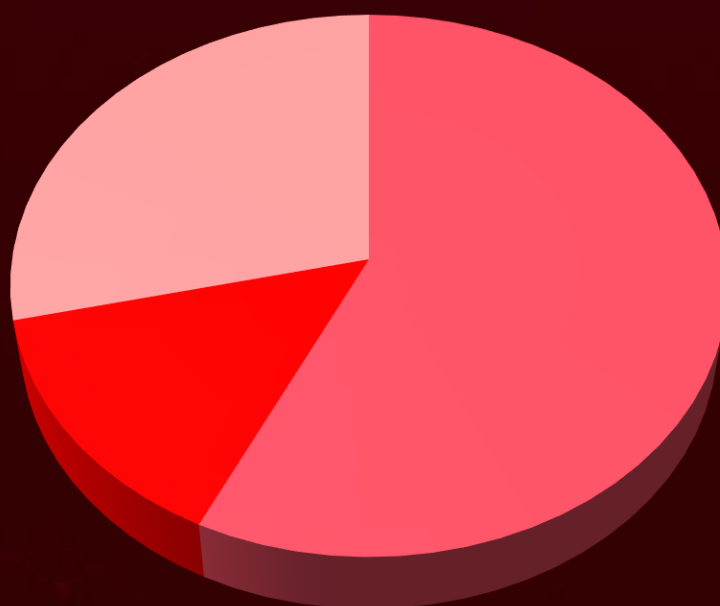
**SafePay** is a ransomware group driving 200+ high-impact attacks in 2025, mainly targeting MSPs and SMBs outside CIS countries.

## **Trend Micro**

### **zero-day** in Apex

One allows RCE without login; temporary fix tool has been issued pending August 2025 patch.

## Threat Distribution



■ Ransomware

■ RAT

■ Backdoor

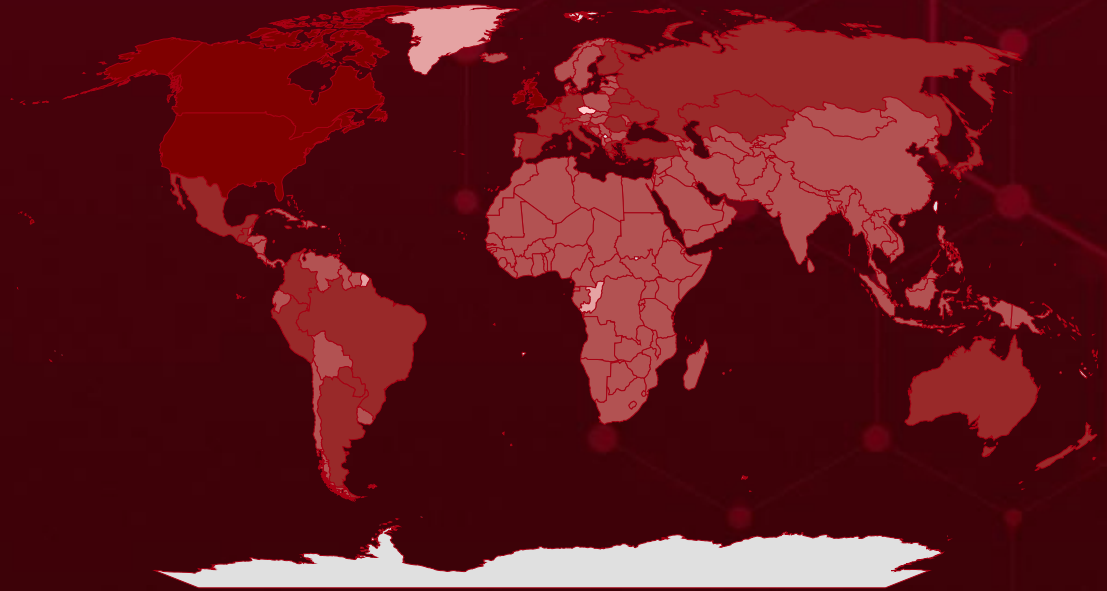


# Targeted Countries

Most



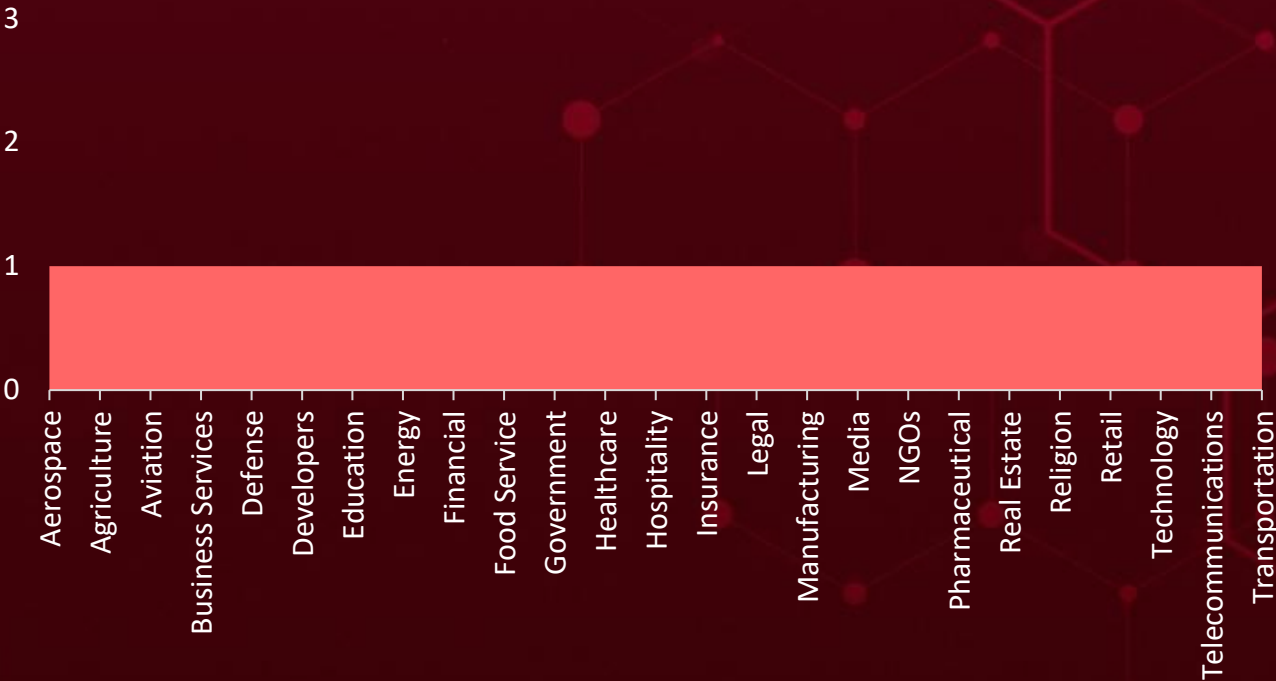
Least



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

Countries	Countries	Countries	Countries
United Kingdom	Croatia	Qatar	Eritrea
Ireland	New Zealand	Cuba	Mongolia
Netherlands	Cyprus	Slovenia	Estonia
Canada	Peru	Austria	Myanmar
United States	El Salvador	Tanzania	Eswatini
Turkey	Russia	Czech Republic (Czechia)	Angola
Paraguay	Finland	Moldova	Ethiopia
Japan	South Korea	Denmark	Nigeria
Argentina	France	Nauru	Fiji
Singapore	Switzerland	Djibouti	Oman
Australia	Germany	North Macedonia	Belize
Italy	Greece	Dominica	Papua New Guinea
Barbados	Ukraine	Cambodia	Benin
Mexico	St. Vincent & Grenadines	Dominican Republic	Poland
Belarus	Palau	Saint Kitts & Nevis	Gabon
Romania	Morocco	DR Congo	Albania
Belgium	Congo	Seychelles	Gambia
Spain	Sao Tome & Principe	Ecuador	Samoa
Brazil	Costa Rica	Chad	Georgia
Guatemala	Turkmenistan	Egypt	Senegal
Brunei	Côte d'Ivoire	Sweden	Bhutan
Jamaica	Nicaragua	Azerbaijan	Central African Republic
Colombia	Armenia	Tonga	Ghana
Kazakhstan		Equatorial Guinea	Somalia

# Targeted Industries



# TOP MITRE ATT&CK TTPs

**T1059**

Command and Scripting Interpreter

**T1190**

Exploit Public-Facing Application

**T1068**

Exploitation for Privilege Escalation

**T1204**

User Execution

**T1566**

Phishing

**T1203**

Exploitation for Client Execution

**T1078**

Valid Accounts

**T1036**

Masquerading

**T1082**

System Information Discovery

**T1027**

Obfuscated Files or Information

**T1204.001**

Malicious Link

**T1588**

Obtain Capabilities

**T1588.005**

Exploits

**T1133**

External Remote Services

**T1059.001**

PowerShell

**T1486**

Data Encrypted for Impact

**T1588.006**

Vulnerabilities

**T1105**

Ingress Tool Transfer

**T1041**

Exfiltration Over C2 Channel

**T1566.001**

Spearphishing Attachment



# ⚔ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Warlock</u>	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			<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770</a>
IOC TYPE	VALUE		
SHA256	da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>4L4MD4R</u>	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			<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770</a>
IOC TYPE	VALUE		
SHA256	33067028e35982c7b9fdcf25eb4029463542451dff454007832cf953feaf1e		

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



NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RoKRAT</u>	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			-
IOC TYPE	VALUE		
MD5	a2ee8d2aa9f79551eb5dd8f9610ad557, ae7e18a62abb7f93b657276dcae985b9, d5fe744b9623a0cc7f0ef6464c5530da, 5ed95cde6c29432a4f7dc48602f82734, 16a8aaaf2e3125668e6bfb1705a065f9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#"><u>Plague</u></a>	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
-			-
IOC TYPE	VALUE		
SHA256	85c66835657e3ee6a478a2e0b1fd3d87119bebadc43a16814c30eb94c53766bb, 7c3ada3f63a32f4727c62067d13e40bcb9aa9cbec8fb7e99a319931fc5a9332e, 9445da674e59ef27624cd5c8ffa0bd6c837de0d90dd2857cf28b16a08fd7dba6, 5e6041374f5b1e6c05393ea28468a91c41c38dc6b5a5230795a61c2b60ed14bc, 6d2d30d5295ad99018146c8e67ea12f4aaa2ca1a170ad287a579876bf03c2950		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#"><u>SafePay</u></a>	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
-			-
IOC TYPE	VALUE		
SHA256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526, 4fe8c6ccdfbcbf6714472e805447fd727d3e46525bd44baf08e5887f890ffb88, 22df7d07369d206f8d5d02cf6d365e39dd9f3b5c454a8833d0017f4cf9c35177, 0f23a313f79d54ae2102f193d3de1a6a98791c27921f28a4fab1092bcb43e5ee, 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917		

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
<a href="#">Qdoor</a>	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
-			-
IOC TYPE	VALUE		
SHA256	0cc25cf9f5d4f02c1a2ed014e2d4acb0d383f01c9bb1852a10b933eec17c1f20, 5d2e7ed8f77bc95302e693312f9a154f0afb698a05796561e277c037deb15a9d, 6d208e99cfac9b2a32df042889636db6217cd12de1980aca7d9678160bf58d4d, 87db51984bfcadf9ee96183f0fe0fb5129b4cfe5a23a68c272b94299267779ea, aee7d7e05e063892f1291a77a8940a9c346c05a68588de89c2a6563ae82ae770		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#">MedusaLocker</a>	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
-			-
IOC TYPE	VALUE		
SHA256	c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516		




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
<u>CVE-2025-49533</u>		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	<a href="https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html">https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-54253</u>		Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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	<a href="https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html">https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-54254</u>		Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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	<a href="https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html">https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html</a>




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





# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
<div></div> <div><u>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)</u></div>	North Korea	-	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	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			

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actor **APT37** and malware **Warlock, 4L4MD4R, RoKRAT, Plague, SafePay, Qdoor, MedusaLocker**.

## Uni5 Users

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

- Running a Scan to discover the assets impacted by the **six exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT37**, and malware **Plague, SafePay**, in Breach and Attack Simulation(BAS).

# Threat Advisories

[RoKRAT Resurfaces: APT37's Fileless Shortcut to Espionage](#)

[Plague in the Shadows: Unmasking a Silent Linux Backdoor](#)

[Adobe Patches Three Critical Flaws in AEM Forms on JEE](#)

[SafePay Ransomware's Rapid Ascent to the Top of the Cybercrime Scene](#)

[Trend Micro Warns of Active Exploits in Apex One Console](#)

[Malicious npm Packages Target WhatsApp Developers with Kill Switch](#)

[MedusaLocker Uses ThrottleStop.sys Flaw to Kill AV on Windows](#)

[Zero Day Watch CVE-2025-53770 Turns SharePoint into a Pivot Point](#)

# 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
<u>Warlock</u>	SHA256	da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb
<u>4L4MD4R</u>	SHA256	33067028e35982c7b9fdcf25eb4029463542451fdff454007832cf953feaf1e
	Domain	bpp[.]theinnovationfactory[.]it
	IPv4	145[.]239[.]97[.]206
<u>RoKRAT</u>	MD5	a2ee8d2aa9f79551eb5dd8f9610ad557,ae7e18a62abb7f93b657276dcae985b9,d5fe744b9623a0cc7f0ef6464c5530da,5ed95cde6c29432a4f7dc48602f82734,16a8aaaf2e3125668e6bfb1705a065f9,64d729d0290e2c8ceaa6e38fa68e80e9,e4813c34fe2327de1a94c51e630213d1
<u>Plague</u>	SHA256	85c66835657e3ee6a478a2e0b1fd3d87119bebadc43a16814c30eb94c53766bb,7c3ada3f63a32f4727c62067d13e40bcb9aa9cbec8fb7e99a319931fc5a9332e,9445da674e59ef27624cd5c8ffa0bd6c837de0d90dd2857cf28b16a08fd7dba6,

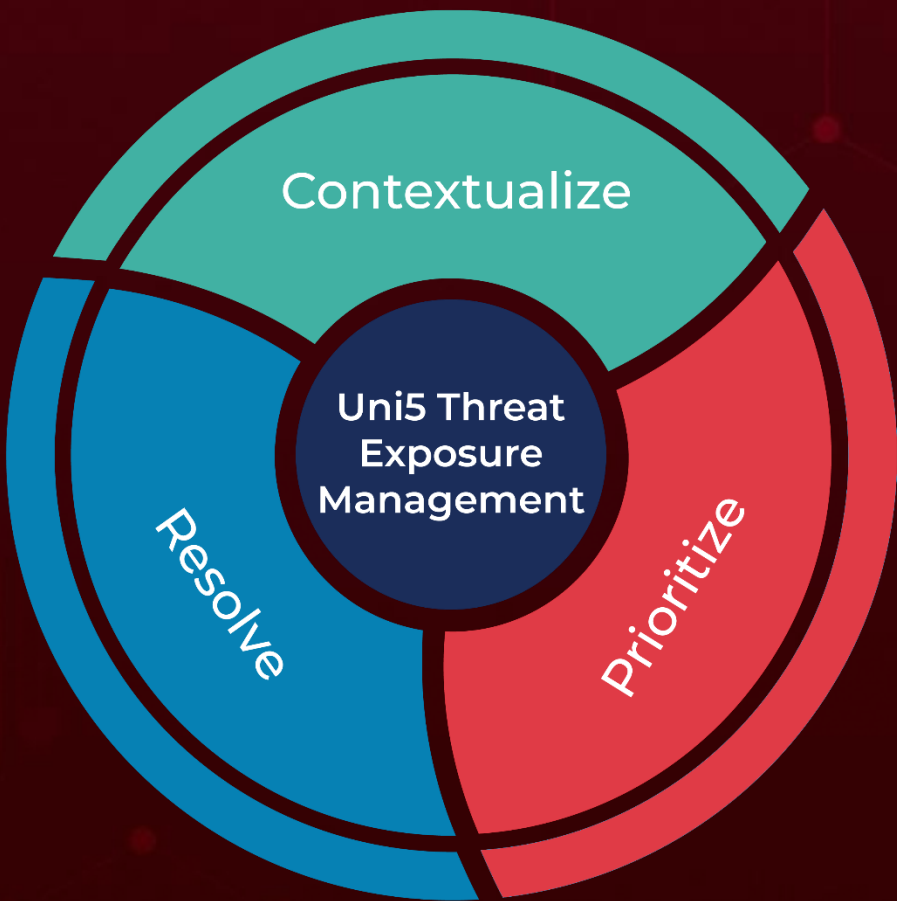
Attack Name	TYPE	VALUE
<u>Plague</u>	SHA256	5e6041374f5b1e6c05393ea28468a91c41c38dc6b5a5230795a61c2b60ed14bc,6d2d30d5295ad99018146c8e67ea12f4aaa2ca1a170ad287a579876bf03c2950,e594bca43ade76bbaab2592e9eabeb8dca8a72ed27afd5e26d857659ec173261,14b0c90a2eff6b94b9c5160875fcf29aff15dcfdfd3402d953441d9b0dca8b39
<u>SafePay</u>	SHA256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526,4fe8c6ccdfbcbf6714472e805447fd727d3e46525bd44baf08e5887f890ffb88,22df7d07369d206f8d5d02cf6d365e39dd9f3b5c454a8833d0017f4cf9c35177,0f23a313f79d54ae2102f193d3de1a6a98791c27921f28a4fab1092bcb43e5ee,327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917,f0127e786c9fb7bf2c8c999202d95c977af4c26cc27302a6ee352cfd62869e7b,94244ec2480addeaebb43aebbe48cee94f7f429231aa054f4c26f671653163b0,b3045308a07e46c9f7dd98d352e964f242307ce30df8087dc751488118b5b959,ba1b89023581a0bc7a75f8ede9ec6115d5dda98c0145634f1b98978fbc79c956,7f33c939f7aaf46945d58ed7fd0d1f5c7e3de1ff6a1a591ecc1992dab2a65078,fa74ac0e05b6209b7691511572386f97464ff5728732de99ddd6b5449ffae386,2f49bff45cc091a7bf52dcd061d24f9a7f2cf0ca9b3c12123bd3cf2fac56b481
	TOR Address	safepaypfxntwixwjrlcscft433ggemlhgkkdupi2ynhtcmvdgubmoyd[.]onion
<u>Qdoor</u>	SHA256	0cc25cf9f5d4f02c1a2ed014e2d4acb0d383f01c9bb1852a10b933eec17c1f20,5d2e7ed8f77bc95302e693312f9a154f0afb698a05796561e277c037deb15a9d,6d208e99cfac9b2a32df042889636db6217cd12de1980aca7d9678160bf58d4d,87db51984bfcadf9ee96183f0fe0fb5129b4cfe5a23a68c272b94299267779ea,

Attack Name	TYPE	VALUE
<u>MedusaLocker</u>	SHA256	c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7

# 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  
**August 11, 2025 • 7:30 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)