

Date of Publication
August 3, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

27 JULY to 02 AUGUST 2026

Table Of Contents

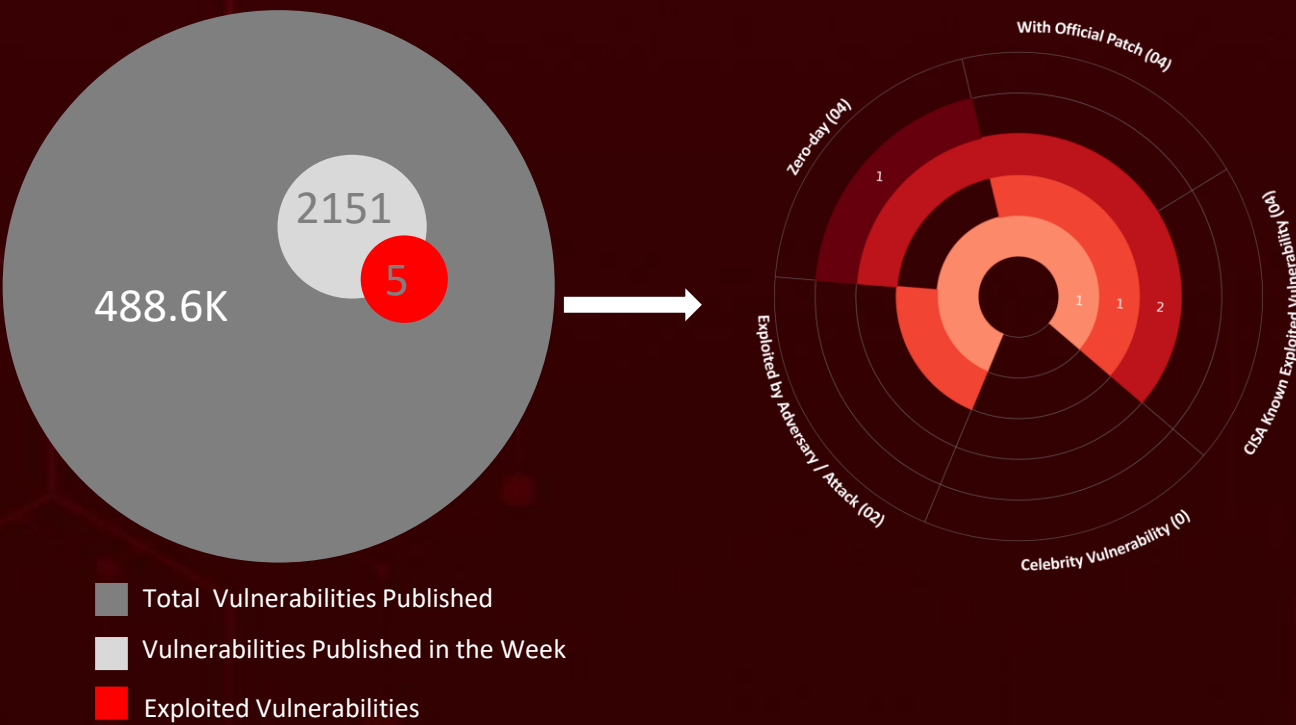
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	10
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	18

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **two** major attacks were detected, **five** vulnerabilities were actively exploited, and **one** threat actor group was closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, Arista has patched a maximum-severity flaw in the on-premises version of its VeloCloud Orchestrator (VCO), the platform organizations rely on to manage VeloCloud SD-WAN deployments and edge devices centrally. Tracked as [CVE-2026-16812](#), the flaw is an unauthenticated OS command injection vulnerability that allows a remote attacker to reach privileged internal functionality never intended for external exposure, without requiring any tenant or operator credentials. Cisco has similarly disclosed [CVE-2026-20316](#), an actively exploited zero-day vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software, rooted in a set of static, built-in credentials tied to a low-privilege account shipped with the software.

Elsewhere, [TA488](#) conducted a widespread email campaign exploiting CVE-2026-42897, a cross-site scripting flaw in Outlook Web Access, in which simply opening a malicious email triggers attacker-controlled JavaScript that deploys OWAReaper, a browser-based backdoor that leaves no trace on the host. Meanwhile, operators suspected of CIOp affiliation have been targeting internet-exposed PTC Windchill and FlexPLM deployments, chaining a pre-authentication FlexPLM WSDL disclosure with a Windchill login servlet flaw ([CVE-2026-12569](#)) to achieve unauthenticated remote code execution. Together, these incidents reflect a growing trend of hybrid cyber operations that blend technical exploitation with social engineering, underscoring the continued need for timely patching, vigilant monitoring, and layered security defenses.



High Level Statistics

2

Attacks
Executed

- OWAReaper
- Tengu

5

Vulnerabilities
Exploited

- CVE-2026-16812
- CVE-2026-12569
- CVE-2026-16723
- CVE-2026-42897
- CVE-2026-20316

1

Adversaries in
Action

- TA488



Insights

Cisco's own firewall manager had a skeleton key baked in; **CVE-2026-20316** turns static, built-in credentials into an actively exploited zero-day.

A maximum-severity bug, zero credentials required, **CVE-2026-16812** opened privileged internal functions of Arista's VCO to anyone remotely.

CVE-2026-16723 gets RCE straight out of FastJson's default settings, and it's already being used in the wild.

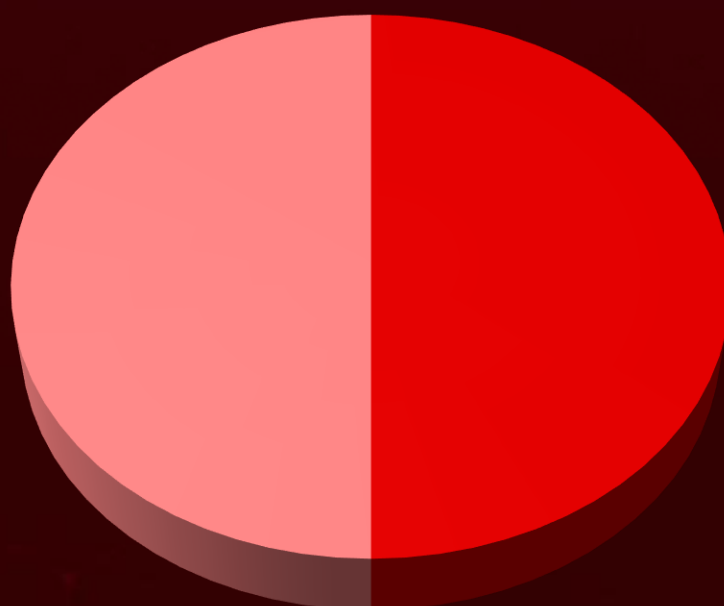
ClOp's playbook again: pre-auth disclosure, one login servlet flaw, unauthenticated RCE, and your **PTC Windchill** data is up for extortion.

Just opening the email is the exploit; **TA488's CVE-2026-42897** turns a glance at Outlook Web Access into OWAReaper, a backdoor that never touches the disk.

Built on Mirai's bones but far craftier,

Tengu proves that weak default passwords are still all it takes to build a botnet.

Threat Distribution



■ Backdoor

■ Botnet

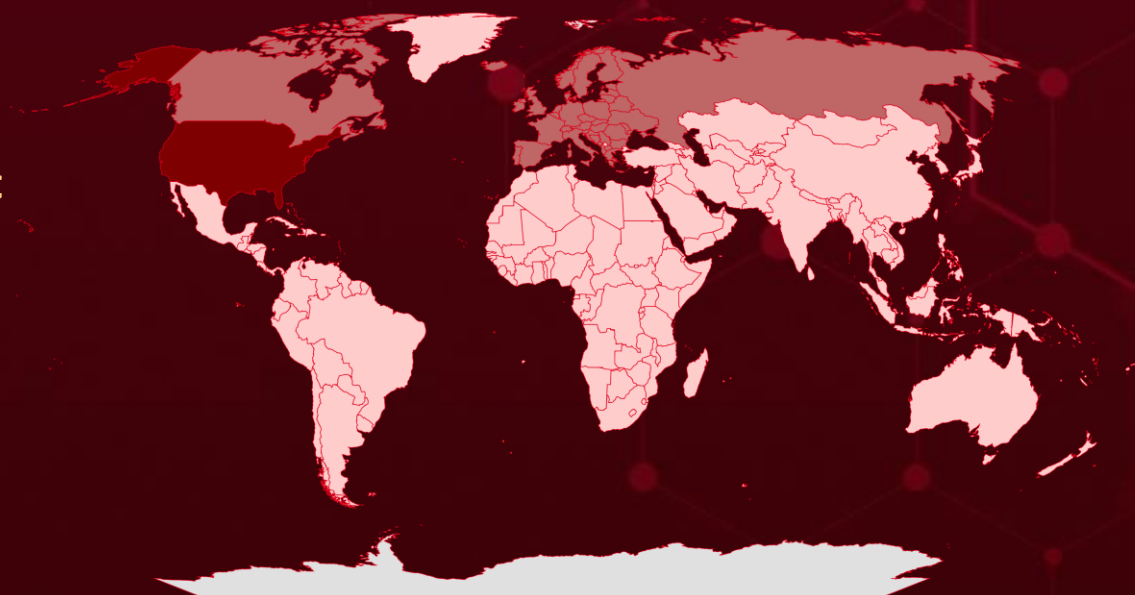


Targeted Countries

Most



Least

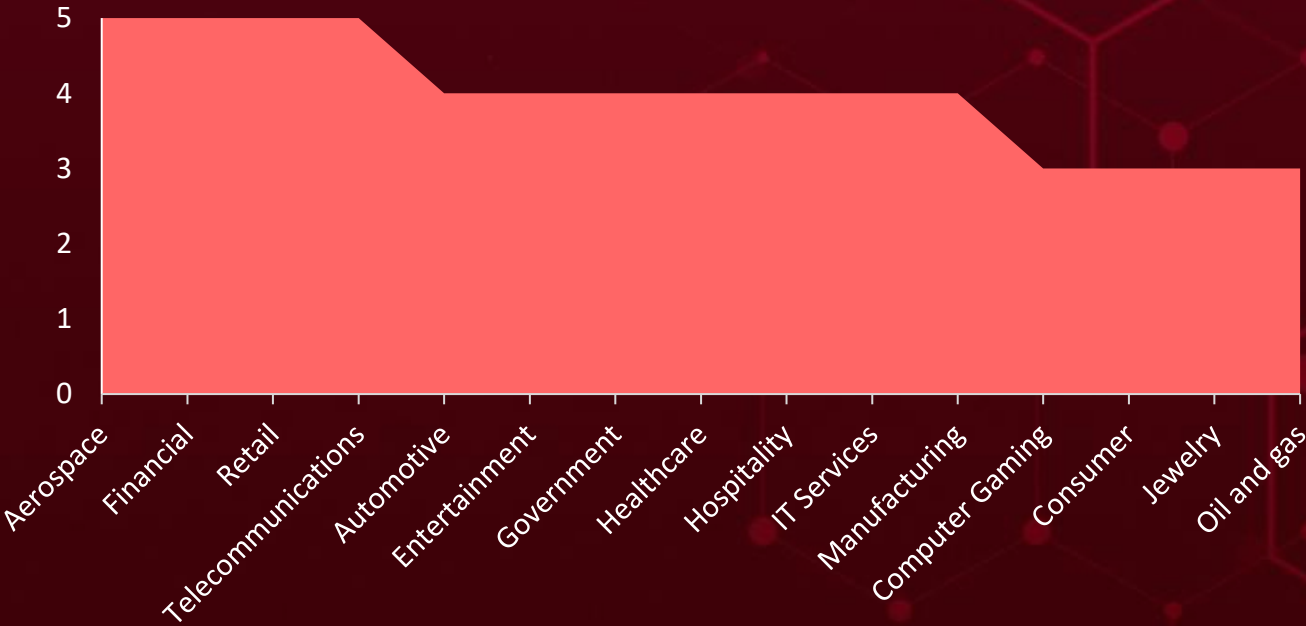


Powered by Bing

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

Countries	Countries	Countries	Countries
United States	Montenegro	Costa Rica	Egypt
Portugal	Finland	Peru	Saint Kitts and Nevis
Malta	North Macedonia	Argentina	El Salvador
Slovenia	France	Suriname	Senegal
Andorra	Poland	Cuba	Equatorial Guinea
Netherlands	Germany	Congo-Brazzaville	South Korea
Austria	Republic of Ireland	Curacao	Australia
San Marino	Greece	Northern Ireland	Syria
Belarus	Russia	Cyprus	Ethiopia
Ukraine	Holy See	Cambodia	Tokelau
Belgium	Serbia	Armenia	Faroe Islands
Monaco	Hungary	Canada Quebec	China
Bosnia and Herzegovina	Slovakia	Democratic Republic of Congo	Fiji
Norway	Iceland	Thailand	Venezuela
Bulgaria	Spain	Aruba	Algeria
Romania	Italy	United States	Mozambique
Canada	Switzerland	Virgin Islands	Azerbaijan
Singapore	Liechtenstein	Djibouti	Nepal
Croatia	Albania	Namibia	French Guiana
Sweden	United Kingdom	Dominica	Nicaragua
Czech Republic	Lithuania	Nigeria	Gabon
Luxembourg	Latvia	Dominican Republic	
Denmark	Samoa	Palestine	
Moldova	Botswana	Ecuador	
Estonia	Turkey	Puerto Rico	

Targeted Industries



TOP MITRE ATT&CK TTPs

<u>T1059</u> Command and Scripting Interpreter	<u>T1588</u> Obtain Capabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1041</u> Exfiltration Over C2 Channel	<u>T1027</u> Obfuscated Files or Information	<u>T1070</u> Indicator Removal	<u>T1586</u> Compromise Accounts	<u>T1505</u> Server Software Component
<u>T1586.002</u> Email Accounts	<u>T1505.003</u> Web Shell	<u>T1078</u> Valid Accounts	<u>T1005</u> Data from Local System	<u>T1485</u> Data Destruction
<u>T1546</u> Event Triggered Execution	<u>T1529</u> System Shutdown/Re boot	<u>T1573</u> Encrypted Channel	<u>T1105</u> Ingress Tool Transfer	<u>T1489</u> Service Stop

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>OWAReaper</u>	OWAReaper is a sophisticated backdoor delivered via half-click exploits, notable for its subtle persistence tricks. An evolution of the earlier ZimReaper payload, it shares much of the same code and behavior, including grabbing autofill passwords from the DOM with an invisible pop-up, but skips mass email exfiltration to stay quieter. It runs entirely inside the Outlook Web Access (OWA) reading pane, using Outlook APIs to rewrite the malicious email and strip out the exploit content while harvesting the victim's saved OWA credentials. For persistence, it hides an encrypted copy of itself in the browser's localStorage under a legitimate OWA settings key, so the backdoor executes automatically every time the user opens an OWA tab.	Exploiting Vulnerability	CVE-2026-42897
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise	Microsoft Exchange Server
ASSOCIATED ACTOR			PATCH LINK
TA488			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897
IOC TYPE	VALUE		
SHA256	6897b649f29e54d8910459963bbf94ed5c7a4fe66a56bc5962540b226b8e48c4		

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
Tengu	Tengu is a Linux botnet malware family derived from Mirai but substantially more advanced in stealth and self-preservation. It spreads by brute-forcing exposed Telnet services with weak or default credentials, exploiting no software vulnerability, and targets IoT and embedded Linux devices across a wide range of processor architectures.	Telnet credential brute force	-
TYPE		IMPACT	AFFECTED PLATFORM
Botnet		Persistent compromise	Linux (embedded and IoT), Android; samples compiled for i386, amd64, MIPS, ARM, PowerPC, and m68k
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	897226af37990fa60f25fea00b0509faa0e78d8bee10875c23b9b6ab0b8faed9		

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 PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-16812</u>		Arista VeloCloud Orchestrator (VCO) On- Prem (5.2.x before 5.2.3.14, 6.1.x before 6.1.3.4, 6.4.x before 6.4.2.4, 7.0.x before 7.0.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*	-
Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-12569</u>		PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030	ClOp
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ptc:windchill_pdmlink:*:*:*:*:*:*:*:*; cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*:*	-
PTC Windchill and FlexPLM Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502, CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.ptc.com/en/support/article/CS473270 , https://support.ptc.com/appserver/common/login/ssl/login.jsp?dest=%2Fappserver%2Fcss%2Fview%2Fsolution.jsp%3Fn%3DCS473270&msg=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-16723</u>		Alibaba FastJson 1.x (1.2.68 through 1.2.83)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:alibaba:fastjson:*:*:*:*:*:*:*	-
Alibaba FastJson Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502, CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42897</u>		Microsoft Exchange Server	TA488
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*	OWAReaper
Microsoft Exchange Server Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-20316</u>		Cisco Secure Firewall Management Center (FMC) Software (7.0.x through 7.7.x and 10.0.x releases prior to the fixed hot-fix builds)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:secure_firewall_management_center:*.~.*.*.*.*.*.*.*.*	-
Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability		CWE ID	ASSOCIATED TTPs
	CWE-259	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 TA488 (aka Void) Blizzard, Laundry Bear	Russia	Government, Telecommunications, Financial, Hospitality, Aerospace	United States and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026- 42897	OWAREaper	Microsoft Exchange Server
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0005: Defense Evasion, TA0003: Persistence, TA0006: Credential Access, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1586: Compromise Accounts, T1583: Acquire Infrastructure, T1566: Phishing, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1070: Indicator Removal, T1098: Account Manipulation, T1555: Credentials from Password Stores, T1528: Steal Application Access Token, T1114: Email Collection, T1102: Web Service, T1090: Proxy, T1041: Exfiltration Over C2 Channel, T1048: Exfiltration Over Alternative Protocol, T1586.002: Email Accounts, T1583.001: Domains, T1059.007: JavaScript, T1070.008: Clear Mailbox Data, T1098.002: Additional Email Delegate Permissions, T1555.003: Credentials from Web Browsers, T1102.002: Bidirectional Communication			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **TA488** and malware **OWAReaper, Tengu**.

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 **five exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TA488** and malware **OWAReaper, Tengu** in Breach and Attack Simulation(BAS).

Threat Advisories

[Critical Zero-Day Hits Arista VeloCloud Orchestrator](#)

[CI0p-Linked Actors Exploit PTC Windchill and FlexPLM in Data Theft Campaign](#)

[FastJson 1.x's Parting Gift: An Unpatched, Unauthenticated RCE](#)

[TA488 Unleashes OWAReaper: A Half-Click Backdoor for Outlook Web Access](#)

[Tengu The Mirai Fork With a Resurrection Clause](#)

[CVE-2026-20316: Cisco Secure FMC Skeleton Key Exploited as a Zero-Day](#)

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>OWAReaper</u>	SHA256	6897b649f29e54d8910459963bbf94ed5c7a4fe66a56bc5962540b226b8e48c4
	Domains	asecdns[.]com, acocdn[.]com, dnsrecursive[.]eu, tdndns[.]com
<u>Tengu</u>	SHA256	897226af37990fa60f25fea00b0509faa0e78d8bee10875c23b9b6ab0b8faed9

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 demo of HivePro.

REPORT GENERATED ON

August 03, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com