

Date of Publication
August 31, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors
24 to 30 AUGUST 2026

Table Of Contents

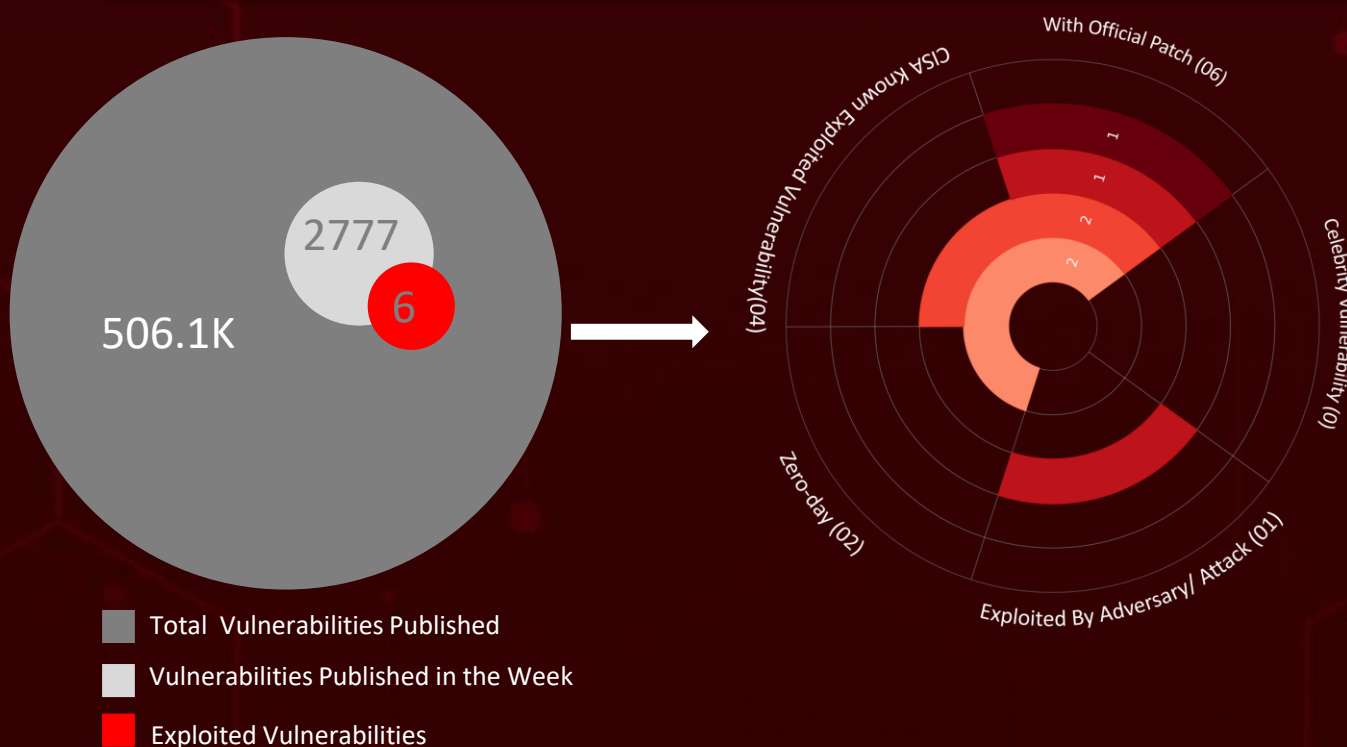
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	16
<u>Adversaries in Action</u>	22
<u>Recommendations</u>	23
<u>Threat Advisories</u>	24
<u>Appendix</u>	25
<u>What Next?</u>	27

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, **eight** major attacks were detected, **six** 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, **PaperCut** has confirmed active zero-day exploitation of two chained flaws affecting all versions of PaperCut NG and MF. CVE-2026-81578 (Authentication Bypass, CVSS 8.8) lets an unauthenticated attacker alter configuration, and CVE-2026-82078 (Unsafe Dynamic Class Loading, CVSS 9.4) turns that access into arbitrary code execution, yielding unauthenticated remote code execution against internet-exposed Application Servers. In parallel, **CVE-2026-21962**, a maximum-severity (CVSS 10.0) improper access-control flaw in Oracle HTTP Server and the WebLogic Server Proxy Plug-in, remains under active exploitation. Attackers were also confirmed exploiting CVE-2026-60004 in self-hosted Gitea servers to drop a cryptocurrency-miner-like payload, aided by Gitea's default open registration.

Elsewhere, **Dark Caracal**, a cyberespionage group linked to Lebanon's General Directorate of General Security, was observed deploying a previously undocumented Go framework tracked as GoCaracal alongside an updated Bandoock variant against a Venezuelan communications organization. A separate China-nexus campaign, Operation QUICSILVER, targeted Myanmar government and diplomatic personnel with the custom QUICAgent backdoor, tunnelling encrypted traffic over QUIC to evade conventional inspection. A Cambodia-focused cluster rounded out the espionage activity, chaining DLL sideloading and a Bring Your Own Vulnerable Driver routine (CVE-2026-36425) to disable endpoint defences in kernel mode before deploying **SparkRAT**. Together, these incidents reinforce a landscape in which rapidly weaponised edge-facing vulnerabilities and patient, evasion-heavy espionage operations advance side by side, underscoring the need for prompt patching of internet-facing systems and continuous monitoring for post-exploitation activity.



High Level Statistics

8

Attacks
Executed

6

Vulnerabilities
Exploited

1

Adversaries in
Action

- [C2Looper](#)
- [SynkLoader](#)
- [QUICAgent](#)
- [WeedHack](#)
- [GoCaracal](#)
- [Bandook](#)
- [Delphi loader](#)
- [SparkRAT](#)

- [CVE-2026-21962](#)
- [CVE-2026-60004](#)
- [CVE-2026-75604](#)
- [CVE-2026-36425](#)
- [CVE-2026-82078](#)
- [CVE-2026-81578](#)

- [Dark Caracal](#)



Insights

SynkLoader spreads via fake Microsoft Teams help-desk messages, using a pixel-perfect fake lock screen to steal users' real passwords.

CVE-2026-60004 is being exploited to hijack self-hosted Gitea servers and drop cryptocurrency miners, aided by default open registration.

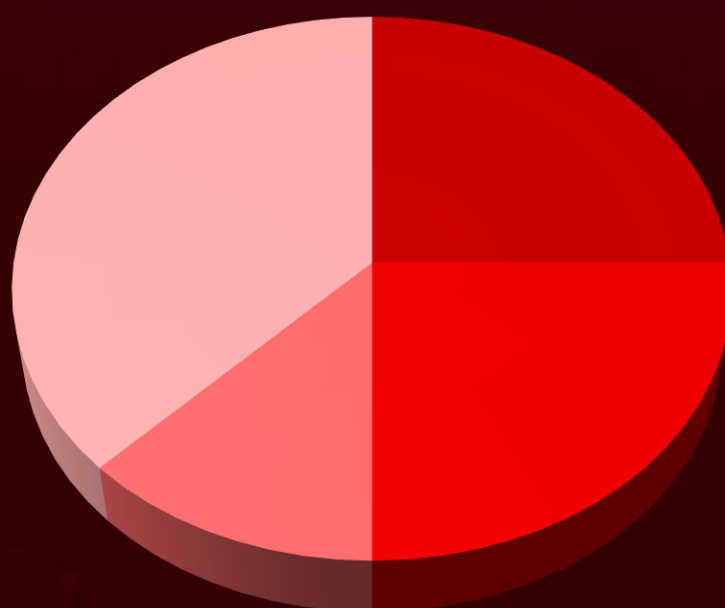
CVE-2026-82078 is an actively exploited PaperCut NG/MF zero-day, chaining with an auth-bypass flaw to give unauthenticated attackers remote code execution on all versions.

Dark Caracal, tied to Lebanese intelligence, deployed a new Go framework, GoCaracal, alongside Bandoos against targets across Latin America.

Operation QUICSILVER, a China-nexus campaign, hit Myanmar's government with the QUICAgent backdoor, tunnelling over QUIC to evade inspection.

CVE-2026-21962, a maximum-severity (CVSS 10.0) Oracle WebLogic Proxy flaw, is under active exploitation.

Threat Distribution



■ Backdoor

■ Loader

■ MaaS

■ RAT

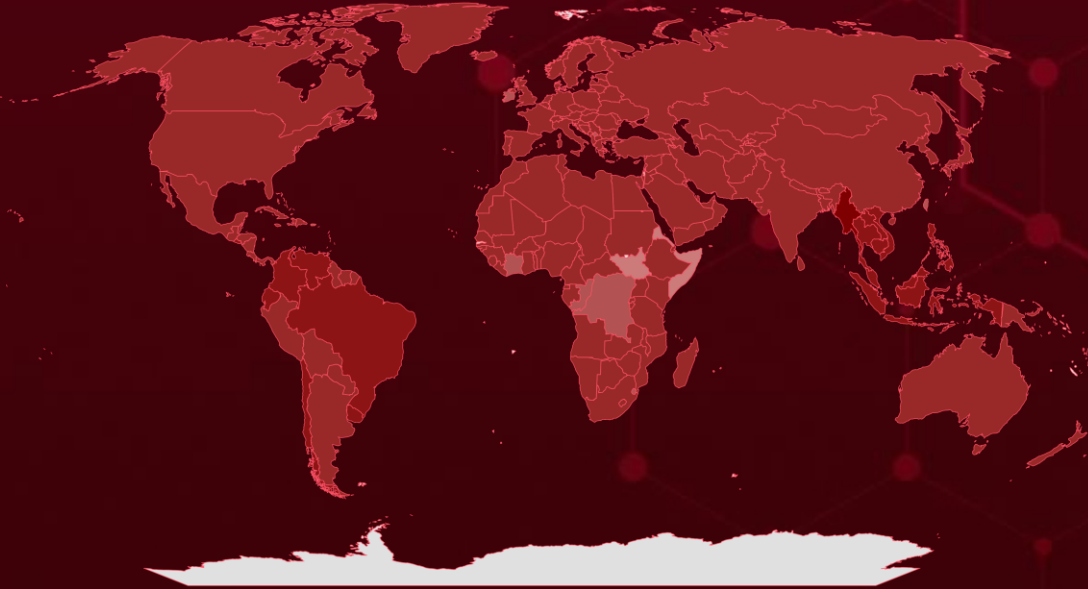


Targeted Countries

Most



Least

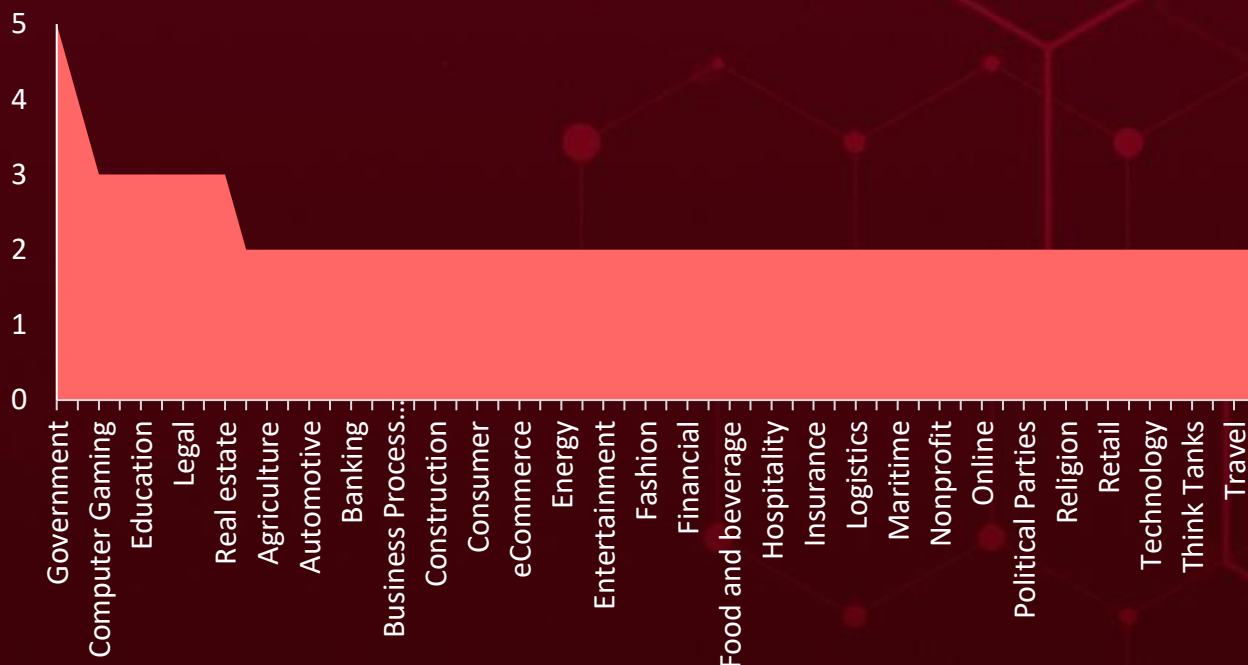


Powered by Bing

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

Countries	Countries	Countries	Countries
Myanmar	Tunisia	Belgium	Serbia
Uruguay	Bosnia and Herzegovina	China	Egypt
Philippines	Mongolia	Ukraine	Slovakia
Vietnam	Botswana	Antigua and Barbuda	Armenia
Brunei	Oman	Malawi	Spain
Thailand	Albania	Comoros	Equatorial Guinea
Cambodia	Saudi Arabia	Malta	Sweden
Venezuela	Algeria	Costa Rica	Estonia
Chile	Syria	Moldova	Tanzania
Brazil	Bulgaria	Croatia	Ethiopia
Malaysia	Belize	Morocco	Tonga
Colombia	Burkina Faso	Cuba	Fiji
Singapore	Mauritius	Nauru	Turkmenistan
Ecuador	Burundi	Cyprus	Finland
Timor-Leste	Bahrain	Nicaragua	United Kingdom
El Salvador	Andorra	Czech Republic	France
Indonesia	Nigeria	North Macedonia	Vanuatu
Laos	Cameroon	Denmark	French Guiana
South Africa	Paraguay	Panama	Bahamas
Netherlands	Canada	Djibouti	Gabon
Maldives	Rwanda	Bangladesh	Mali
Bhutan	Central African Republic	Dominica	Georgia
Portugal	Sierra Leone	Romania	Mauritania
Bolivia	Chad	Dominican Republic	Germany
	Sudan	Samoa	Mexico
	Angola	Argentina	Ghana

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1204

User Execution

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1082

System Information Discovery

T1204.002

Malicious File

T1566

Phishing

T1071.001

Web Protocols

T1588

Obtain Capabilities

T1070

Indicator Removal

T1140

Deobfuscate/Decode Files or Information

T1083

File and Directory Discovery

T1588.006

Vulnerabilities

T1573.001

Symmetric Cryptography

T1518

Software Discovery

T1053

Scheduled Task/Job

T1573

Encrypted Channel

T1547

Boot or Logon Autostart Execution

T1057

Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>C2Looper</u>	C2Looper is a Rust-based backdoor identified in July 2026, used to establish a foothold for lateral movement in ransomware intrusions. Its v2 build adds GitHub-based C2 and shellcode injection, and abuses OneDrive DLL sideloading for stealth.	ClickFix chain	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Foothold, recon, payload delivery	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	f96ff2f3abbff7f382ace509b90e54853b4b61c402ecde27d82f1c17b414867b		

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
SynkLoader	SynkLoader is a loader distributed through Microsoft Teams phishing campaigns to steal credentials via a fake lock screen. It got its name from its unusual mix of programming languages, Python, PowerShell, C#, and C++, sometimes blending up to three of them in a single module. The loader ships with a long chain of attack tools that bridge these different languages, with some modules using as many as three at once.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	d150c70d2732df17aa77991b9ebf4c896f044445e900978581d9598dfa5dc98c		

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
QUICAgent	QUICAgent is a custom 64-bit Go backdoor that performs sandbox evasion, then resolves its C2 via Cloudflare Workers and communicates over QUIC on UDP/443 with RC4 encryption. Deployed in Operation QUICSILVER.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote exec, espionage	Windows
ASSOCIATED ACTOR			PATCH LINK
China-nexus			-
IOC TYPE	VALUE		
SHA256	cd147efe37003399e174951927e5fe727a4481756b116f0204a14a64cc62b059		

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
<u>WeedHack</u>	WeedHack is a Minecraft-focused Malware-as-a-Service (MaaS) that shows how SEO poisoning can drop malicious downloads straight into gamers' paths. It has also become a major catalyst for cyberbullying: many of its customers appear to be teenagers and young adults who use its remote access capabilities to threaten, harass, and monitor victims around their own age.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
MaaS		remote-access	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	3951533d56803cd5d708014b4eed7e30349b4c4ba43f7d843133b3a5e2992ce6		

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
<u>GoCaracal</u>	GoCaracal is a modular Go-based RAT and post-exploitation framework with lightweight and extended profiles. Its extended variant uses Ethereum smart contracts as a fallback C2-resolution mechanism.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Data theft, keylogging, RDP, SOCKS5	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-
IOC TYPE	VALUE		
SHA256	1E499C815146124C4A6D2B48C99068B980AD74E1A2CFD16013F8D75A9425A0CA, 77F7AD29F4A8037EE5F38D3D87FB91CFD97CB8F7FA7883EDF3FCE506DF5200C0		

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
<u>Bandoock</u>	Bandoock is a long-running C++ remote access trojan and Dark Caracal's signature malware. Its June 2026 variant adds anti-analysis via randomized command IDs and obfuscated plugin export names.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		File theft, credential theft, keylogging	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-
IOC TYPE	VALUE		
SHA256	a2cdf2fe741de4b13ad2298b387a6c32da4a94da180ae75bf8547386aee7376b		

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
<u>Delphi loader</u>	Delphi loader is an intermediate stager in the Dark Caracal chain that carries Bandoon and the extended GoCaracal variant. It recurs across campaigns as an attribution artifact.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Payload delivery	Windows
ASSOCIATED ACTOR			PATCH LINK
Dark Caracal			-
IOC TYPE	VALUE		
SHA256	0A6DA70548F14834ACB8960689A589B48FF422F8385AE445A281AAB77045FE22		

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
<u>SparkRAT</u>	SparkRAT is an open-source, cross-platform remote access trojan written in Go and developed by XZB-1248. It runs on Windows, macOS, and Linux, and offers extensive remote access capabilities, including file and process management, file transfer, remote desktop monitoring, system information collection, and command execution through terminal access.	Phishing	CVE-2026-36425
TYPE		IMPACT	AFFECTED PLATFORM
RAT		System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			https://www.opswat.com/products/oesis-framework/application-removal
IOC TYPE	VALUE		
SHA256	c1a8556741564c3698b56419f66cc27ad50be9148ef483f92866d4edabc46624, f949d967355578cb6a34a678b6e8683b21e58e2ea6b6d5e0cdd4f59af2e37f19		

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-2026-21962</u>		Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for Microsoft IIS (12.2.1.4.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:oracle:http_server:*:*:*:*:* ; cpe:2.3:a:oracle:weblogic_server_proxy_plug-in:*:*:*:*:*	-
Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpujan2026.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-60004</u>		Gitea (1.17 through 1.27.0, before 1.27.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gitea:gitea:*:*:*:*:*:*:*	-
Gitea Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://blog.gitea.com/release-of-1.27.1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-75604</u>		Vercel Next.js (>= 13.4 and < 15.5.24; >= 16.0 and < 16.3.3) on Windows filesystem hosts using Pages Router and App Router without Cache Components	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vercel:next.js:*:*:*:*:*: node.js:*.*	-
Vercel Next.js Windows-Hosted Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://nextjs.org/blog/august-2026-security-release

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-36425</u>		OPSWAT AppRemover (ardrv.sys)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:opswat:appremoverdriver:*:*:*:*:*:*	SparkRAT
OPSWAT AppRemover Arbitrary Process Termination Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://www.opswat.com/products/oesis-framework/application-removal

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-82078</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng:*.~.*.*.*.*.*.*	-
PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability		cpe:2.3:a:papercut:papercut_mf:*.~.*.*.*.*.*.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-470	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter, T1070:Indicator Removal	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-81578</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:papercut:papercut_ng: *.*.*.*.*.*.*	-
PaperCut NG and PaperCut MF Authentication Bypass Vulnerability		cpe:2.3:a:papercut:papercut_mf: *.*.*.*.*.*.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190:Exploit Public-Facing Application, T1562:Impair Defenses	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Dark Caracal (aka ATK 27, TAG-CT3)	Lebanon	Communications, Government, Military, Businesses, Journalists, Activists, Legal, Healthcare, Education	Venezuela, Brazil, Ecuador, Chile, Colombia, El Salvador, Uruguay
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	GoCaracal, Bandoock, Delphi loader	Windows
TTPs			
TA0042:Resource Development, T1583:Acquire Infrastructure, T1583.001:Domains, T1583.003:Virtual Private Server, T1608:Stage Capabilities, T1608.001:Upload Malware, TA0001:Initial Access, T1566:Phishing, T1566.001:Spearphishing Attachment, TA0002:Execution, T1204:User Execution, T1204.002:Malicious File, T1059:Command and Scripting Interpreter, T1059.003:Windows Command Shell, TA0003:Persistence, T1547:Boot or Logon Autostart Execution, T1547.001:Registry Run Keys / Startup Folder, TA0005:Defense Evasion, T1112:Modify Registry, T1055:Process Injection, T1027:Obfuscated Files or Information, T1140:Deobfuscate/Decode Files or Information, T1564:Hide Artifacts, T1564.001:Hidden Files and Directories, T1070:Indicator Removal, T1070.004:File Deletion, T1036:Masquerading, T1036.005:Match Legitimate Name or Location, TA0006:Credential Access, T1555:Credentials from Password Stores, T1555.003:Credentials from Web Browsers, T1539:Steal Web Session Cookie, T1056:Input Capture, T1056.001:Keylogging, TA0007:Discovery, T1082:System Information Discovery, T1057:Process Discovery, T1083:File and Directory Discovery, T1518:Software Discovery, T1518.001:Security Software Discovery, T1010:Application Window Discovery, TA0009:Collection, T1005:Data from Local System, TA0011:Command and Control, T1105:Ingress Tool Transfer, T1573:Encrypted Channel, T1573.001:Symmetric Cryptography, T1071:Application Layer Protocol, T1071.001:Web Protocols, T1102:Web Service, T1102.001:Dead Drop Resolver, T1090:Proxy, T1090.001:Internal Proxy, T1219:Remote Access Tools, T1219.002:Remote Desktop Software, TA0010:Exfiltration, T1041:Exfiltration Over C2 Channel			

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 **Dark Caracal**, and malware **C2Looper**, **SynkLoader**, **QUICAgent**, **WeedHack**, **GoCaracal**, **Bandook**, **Delphi loader**, and **SparkRAT**.

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 **six exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Dark Caracal**, and malware **C2Looper**, **SynkLoader**, **QUICAgent**, **WeedHack**, and **SparkRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[August 2026 Linux Patch Roundup](#)

[C2Looper Builds Footholds for Ransomware](#)

[SynkLoader: When a Teams Message Fakes Your Lock Screen](#)

[CVE-2026-21962: Critical Oracle WebLogic Proxy Plug-in Flaw Exploited in the Wild](#)

[Operation QUICSILVER Drops a Go Backdoor on Myanmar Government](#)

[WeedHack Resurfaces via Fake Minecraft Clients and SEO Poisoning](#)

[Gitea RCE \(CVE-2026-60004\) Exploited to Hijack Servers for Crypto Mining](#)

[Dark Caracal Modernizes Its Espionage Toolkit](#)

[Critical Next.js Flaws Enable Unauthenticated Remote Code Execution](#)

[SparkRAT Ignites Cambodia via BYOVD Chain](#)

[PaperCut NG/MF Zero-Day Under Active Exploitation Across All Versions](#)

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
C2Looper	SHA256	f96ff2f3abbbff7f382ace509b90e54853b4b61c402ecde27d82f1c17b414867b
SynkLoader	SHA256	d150c70d2732df17aa77991b9ebf4c896f044445e900978581d9598dfa5dc98c
QUICAgent	SHA256	cd147efe37003399e174951927e5fe727a4481756b116f0204a14a64cc62b059
WeedHack	SHA256	3951533d56803cd5d708014b4eed7e30349b4c4ba43f7d843133b3a5e2992ce6
GoCaracal	IPv4	109[.]120[.]187[.]217, 109[.]172[.]95[.]121, 138[.]124[.]112[.]213, 138[.]124[.]14[.]130, 176[.]124[.]220[.]153, 185[.]125[.]101[.]181, 185[.]96[.]80[.]110, 185[.]96[.]80[.]54, 193[.]233[.]245[.]52, 193[.]233[.]245[.]45,

Attack Name	TYPE	VALUE
<u>GoCaracal</u>	IPv4	193[.]233[.]245[.]0, 62[.]60[.]237[.]22, 77[.]110[.]104[.]98, 77[.]110[.]105[.]244, 77[.]110[.]105[.]56, 77[.]110[.]105[.]59, 77[.]110[.]98[.]66, 80[.]71[.]224[.]30, 82[.]117[.]87[.]138, 82[.]117[.]87[.]192, 85[.]192[.]30[.]211, 79[.]137[.]192[.]38, 46[.]226[.]162[.]68, 45[.]152[.]198[.]108
	SHA256	1E499C815146124C4A6D2B48C99068B980AD74E1A2CFD16013F8D75A9425A0CA, 77F7AD29F4A8037EE5F38D3D87FB91CFD97CB8F7FA7883EDF3FCE506DF5200C0
<u>Bandook</u>	IPv4	91[.]208[.]197[.]80, 91[.]208[.]184[.]45, 91[.]208[.]206[.]88, 91[.]208[.]184[.]130, 176[.]123[.]1[.]174
	SHA256	a2cdf2fe741de4b13ad2298b387a6c32da4a94da180ae75bf8547386ae7376b
<u>Delphi loader</u>	SHA256	0A6DA70548F14834ACB8960689A589B48FF422F8385AE445A281AAB77045FE22
<u>SparkRAT</u>	SHA256	c1a8556741564c3698b56419f66cc27ad50be9148ef483f92866d4edabc46624, f949d967355578cb6a34a678b6e8683b21e58e2ea6b6d5e0cdd4f59af2e37f19, d56c6513a8b25b1883ef33a95d4ece591eabbe17a58f7e3d0fc77c6f29344148, a2c1b858c1d4788e87bb699e3775e851cda95488979b15f4d676f6e1915d8bc8,

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 31, 2026 • 11:40 PM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com