Date of Publication
July 27, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

20 to 26 JULY 2026

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 14

Adversaries in Action 19

Recommendations 20

Threat Advisories 21

Appendix 22

What Next? 24

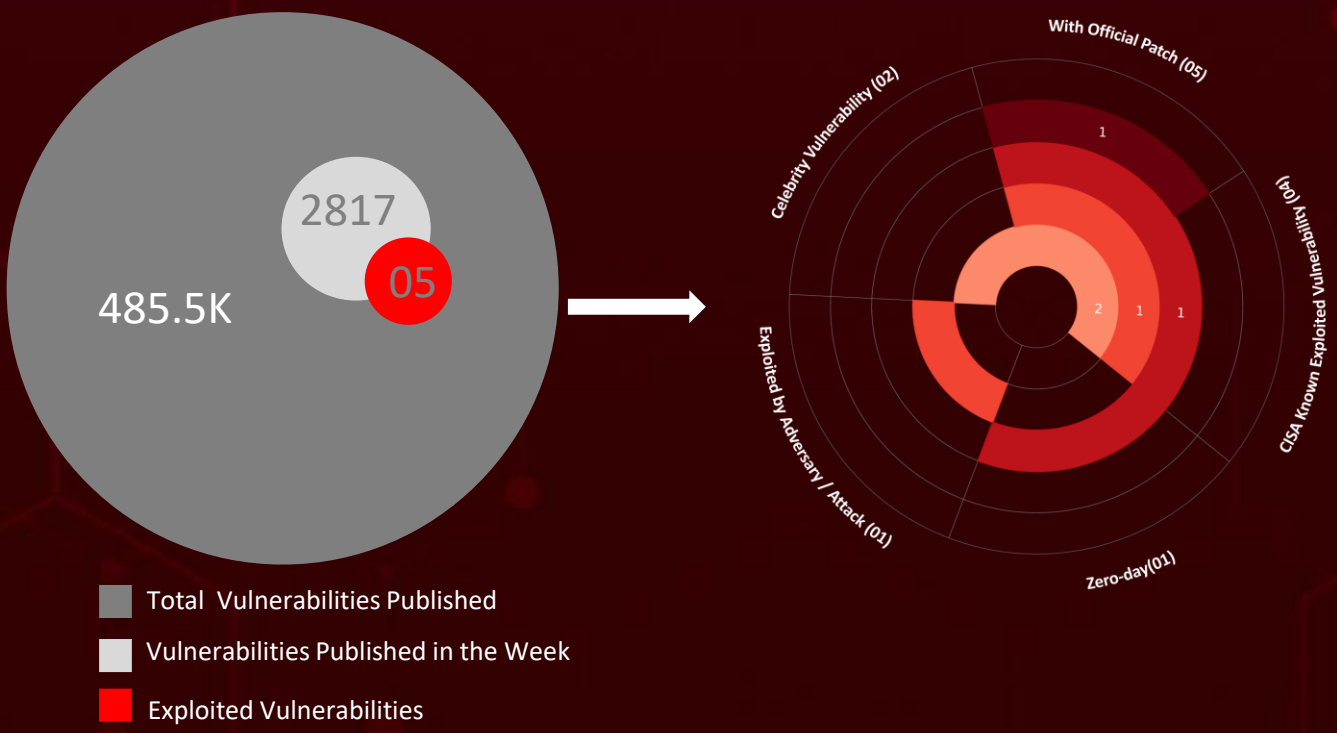
Summary

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

One of the biggest concerns is a flaw chain in WordPress Core, the platform behind more than 500 million websites. Dubbed **wp2shell**, it lets an attacker take over a site with just one web request, no login, no plugins, no user interaction required. The chain works by pairing two bugs together: a REST API mix-up introduced in WordPress 6.9 (CVE-2026-63030) and a SQL injection flaw in WP_Query's author parameter (CVE-2026-60137).

Check Point has also patched a critical issue in SmartConsole, the admin console used to manage its Security Management and Multi-Domain servers. Tracked as **CVE-2026-16232**, the bug is an authentication bypass that lets an attacker intercept a valid login token during the sign-in process and use it to gain full administrator access, no password needed.

Separately, researchers are tracking **HelloNet**, an espionage campaign active since at least May 2026 that targets Russian government and critical-infrastructure networks. The attackers abuse ViPNet's trusted software update mechanism to sideload a malicious DLL, quietly planting a multi-stage implant that blends in with legitimate update traffic. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

9
Attacks Executed

5
Vulnerabilities Exploited

0
Adversaries in Action

- HOLLOWGRAPH
- HelloInjector
- HelloProxy
- HelloExecutor
- HelloCleaner
- HelloBackdoor
- SmartLoader
- StealC
- Qilin Ransomware

- CVE-2026-63030
- CVE-2026-60137
- CVE-2026-6875
- CVE-2026-16232
- CVE-2026-0257

Insights

From dominant to more dominant, **Qilin's** latest chapter adds **CVE-2026-0257** to an already growing arsenal.

CVE-2026-16232 hit where it hurts most: the admin console managing Check Point's own Security Management and MDS servers.

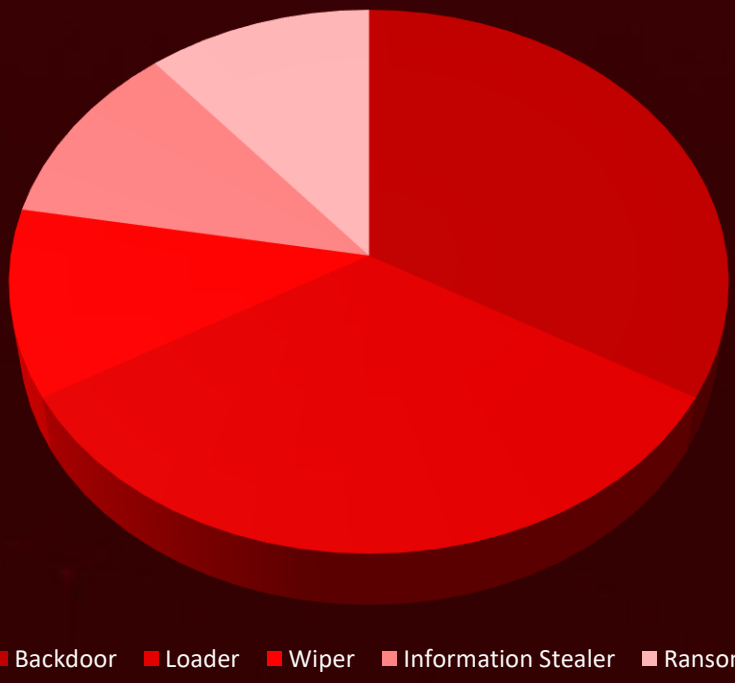
HOLLOWGRAPH's cover is genius: legitimate Microsoft Graph API calls, calendar invites for commands, and a 2050 timestamp so no one ever looks.

Signed, trusted, compromised: **HelloNet** rides ViPNet's legitimate update mechanism straight into government networks, then covers its tracks on the way out.

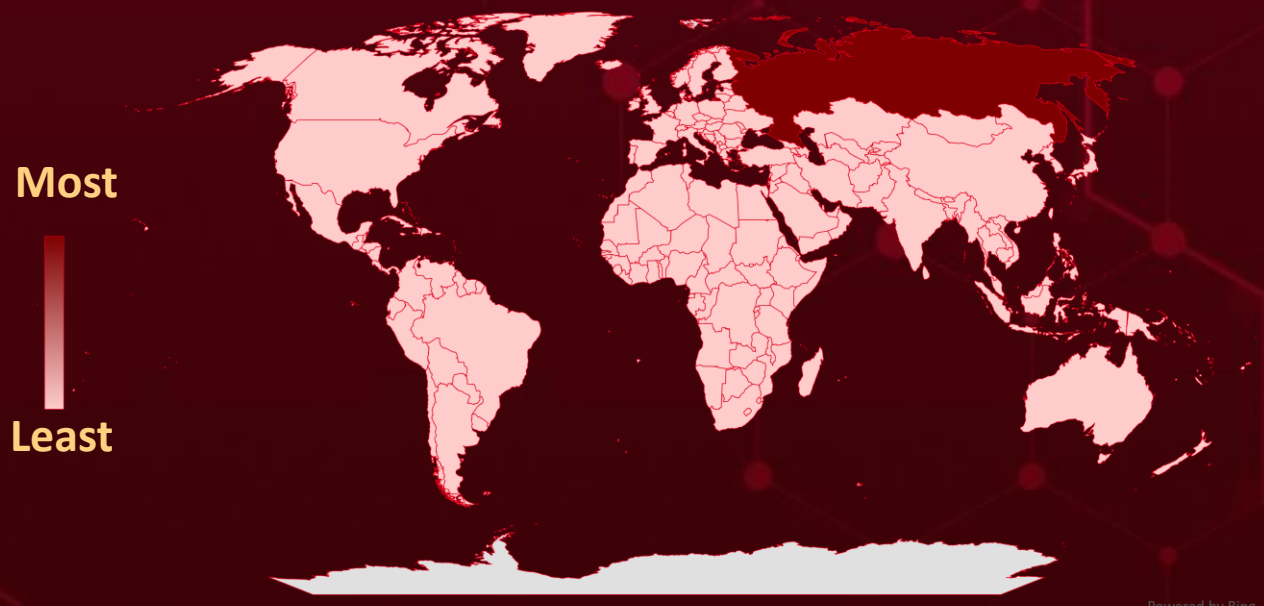
500 million WordPress sites, one flaw chain, zero authentication: **wp2shell** turns **CVE-2026-63030** and **CVE-2026-60137** into instant takeover.

FakeGit doesn't hack GitHub's trust; it borrows it, wrapping **SmartLoader** inside thousands of repos that look like the real thing.

Threat Distribution

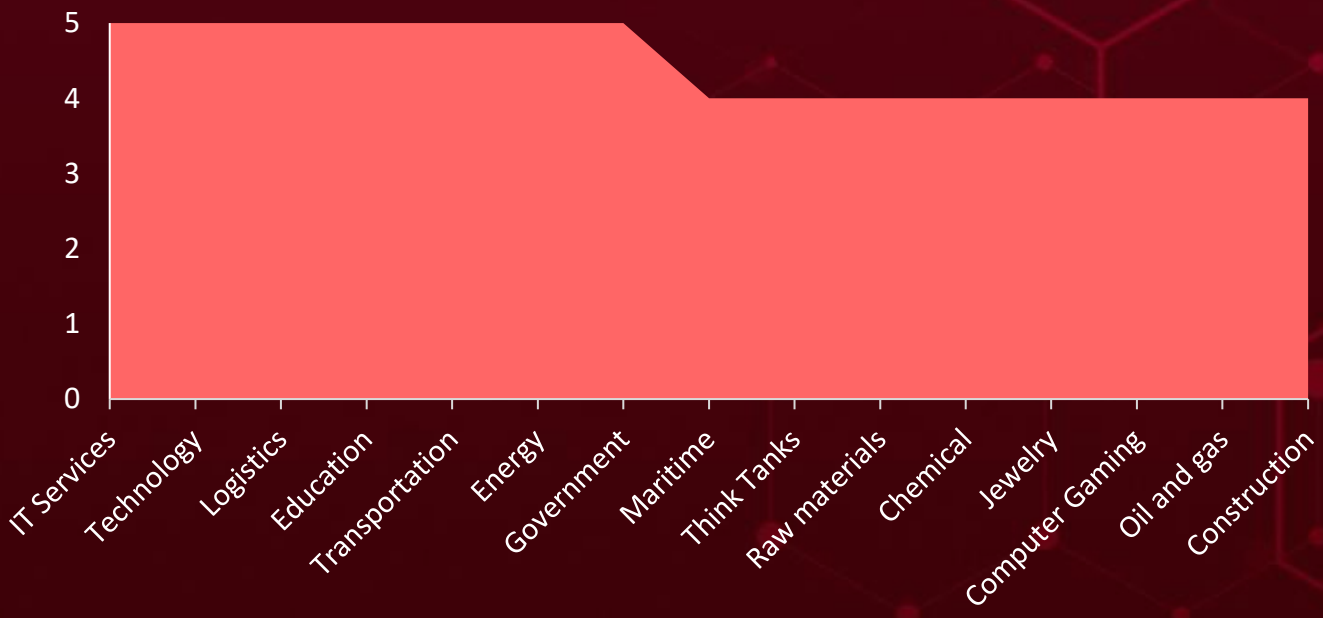


Targeted Countries



Countries	Countries	Countries	Countries
Russia	Austria	Turkmenistan	China
Israel	Vietnam	Bonaire	Serbia
Mexico	Azerbaijan	Uruguay	Colombia
Switzerland	Luxembourg	Bosnia and Herzegovina	Slovakia
Portugal	Bahamas	Afghanistan	Comoros
Algeria	Malta	Botswana	Spain
Liberia	Bahrain	Liechtenstein	Congo-Brazzaville
American Samoa	Montenegro	Brazil	Swaziland
Niger	Bangladesh	Macedonia	Costa Rica
Andorra	Netherland Antilles	British Virgin Islands	Tanzania
Scotland	Barbados	Maldives	Croatia
Angola	Northern Cyprus	Brunei	Togo
United Arab Emirates	Belarus	Mauritania	Cuba
Anguilla	Paraguay	Bulgaria	Tunisia
Malawi	Belgium	Monaco	Curacao
Antigua and Barbuda	Romania	Burkina Faso	Uganda
Myanmar	Belize	Morocco	Cyprus
Argentina	Saint Vincent and the Grenadines	Burundi	United States
Pakistan	Benin	Nauru	Czech Republic
Armenia	Sierra Leone	Cambodia	Vanuatu
Saint Eustatius	Bermuda	New Zealand	Democratic Republic of Congo
Aruba	Sudan	Cameroon	
South Africa	Bhutan	North Korea	
Australia	Tibet	Canada	
Tonga	Bolivia		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1005** Data from Local System	**T1036** Masquerading	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1562** Impair Defenses	**T1036.005** Match Legitimate Name or Location	**T1078** Valid Accounts	**T1572** Protocol Tunneling
T1102 Web Service	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1055** Process Injection	**T1059.003** Windows Command Shell
T1113 Screen Capture	**T1195** Supply Chain Compromise	**T1550** Use Alternate Authentication Material	**T1585** Establish Accounts	**T1068** Exploitation for Privilege Escalation

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HOLLOWGRAPH	HOLLOWGRAPH is a Windows backdoor that communicates exclusively through third-party services rather than attacker-controlled infrastructure. It uses the Microsoft Graph API to exchange commands and exfiltrate data through a compromised Microsoft 365 calendar, while DNS tunneling is used to retrieve and refresh Microsoft Entra ID credentials.	Microsoft 365 mailbox calendar	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509, F3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3

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
HelloInjector	HelloInjector is the initial loader in the HelloNet chain, deployed as a malicious wtsapi32.dll sideloaded by the signed ViPNet update binary at system startup. It decrypts an embedded payload and injects it into a netsvcs svchost.exe instance using native NT APIs, giving the operators a stealthy foothold inside a trusted, signed process.	DLL Sideloading	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		System Compromise, Defense Evasion	ViPNet Update System
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	ffdc194775b2904564bbbd1cf0eb01d1a01f83ef5197d1612b6e2d69de7a4732		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HelloProxy	HelloProxy is the main HelloNet payload, functioning as both a network proxy and an in-memory loader. It hooks network-related APIs via a legitimate hooking library and intercepts AFD IOCTLs to hinder user-mode security tools, listening on ports 5003 and 5060 behind a handshake-gated C2 to distinguish operator traffic before processing commands.	In-memory injection (via HelloInjector)	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Defense Evasion, C2 Communication, Payload Delivery	ViPNet Update System
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
HelloExecutor	HelloExecutor is a command-execution implant used for internal reconnaissance within compromised networks. It runs discovery commands for users, groups, and network configuration, and specifically harvests ViPNet Administrator and Client export paths to map the secure-networking environment.	In-memory execution (via HelloProxy)	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Discovery, Internal Reconnaissance	ViPNet Update System
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HelloCleaner	HelloCleaner is an anti-forensic module that scrubs ViPNet software log files to erase evidence of the operators' activity, supporting the campaign's emphasis on stealth and long-dwell persistence.	In-memory execution (via HelloProxy)	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Wiper		Defense Evasion, Indicator Removal	ViPNet Update System
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
HelloBackdoor	HelloBackdoor is a Rust-based backdoor that listens on port 443 and activates only on receipt of a specific trigger string derived from an MD5 hash. Once active it supports file upload, download, and arbitrary command execution via the command shell, providing a resilient secondary access channel.	In-memory execution (via HelloProxy)	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		Remote Access, Command Execution, Data Transfer	ViPNet Update System
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	16C211C96735F2FAE9361B89BD7A31BF		
SHA256	68b4c76a2280e3c31130d4de12b12dfd479a476f347f5b4a58cb2483d74aba7e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SmartLoader	SmartLoader sets up persistence and installs StealC, an information stealer that goes after credentials, active sessions, and other sensitive data. Attackers have used SmartLoader to target developers through convincing-looking GitHub projects, turning what feels like normal software discovery into malware delivery.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Establishes persistence and installs StealC	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	6f61812b300244df4921cc0eba252181bb2138f76cfe4e6848c73a46917daee1		

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
StealC	StealC is an information stealer that goes after credentials, active sessions, and other sensitive data, including browser passwords, cookies, browser extension data, email and remote-access credentials, screenshots, and host details. The malware chain itself is nothing new; what changes is the route that leads to it being run.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Information Stealer		Targeting credentials, active sessions, and other sensitive data	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	2fc8cabf074616e31880562c58c62874e5d9e3925d2c8603460ba26560b5ffa4, ff8ee64171af93214e844d098c40b2a12e3360a23ecdc7ae9f56a31ea4248c9d		

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
Qilin Ransomware	Qilin is a prolific Ransomware-as-a-Service operation whose affiliates use double extortion encrypting victims' files and stealing sensitive data to threaten public release unless a ransom is paid. In a notable evolution, affiliates now run a Linux ransomware variant on Windows hosts by abusing legitimate remote-management tools like AnyDesk, ScreenConnect, and Splashtop evading Windows-focused defenses and improving stealth in mixed-OS environments.	Social Engineering	CVE-2026-0257
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Ransomware		System Compromise, Encrypt Data, Financial Loss	Palo Alto Networks PAN-OS / Prisma Access
ASSOCIATED ACTOR			**PATCH LINK**
-			https://security.paloaltonetworks.com/CVE-2026-0257
IOC TYPE	**VALUE**		
SHA256	d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6		

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
CVE-2026-63030	wp2shell	WordPress WordPress Core (Version before 6.9.5 and 7.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	-
wp2shell (WordPress Core Interpretation Conflict Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-436	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-60137	wp2shell ZERO-DAY	WordPress WordPress Core (Version before 6.9.5 and 7.0.2)	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	-
wp2shell (WordPress Core SQL Injection Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-6875		ServiceNow AI Platform (before Australia Patch 2, Yokohama Patch 12 Hot Fix 1b, Yokohama Patch 13, Zurich Patch 7b, Zurich Patch 9, Brazil EA, and Brazil GA)	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:servicenow:ai_platform:*:*:*:*:*:*:*:*	-
ServiceNow AI Platform Remote Code Execution Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3137947

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-16232</td><td></td><td rowspan="2">Check Point Security Management Server/ Multi Domain Security Management (R77.30, R80, R80.10, R80.20, R80.30, R81 R81.10, R81.20, R82, R82.10)</td><td rowspan="2">-</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:a:checpoint:multi-domain_security_management:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Check Point SmartConsole Improper Authentication Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287</td><td>T1190: Exploit Public-Facing Application,T1550: Use Alternate Authentication Material, T1550.001: Application Access Token</td><td>https://support.checkpoint.com/results/sk/sk185169/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-0257		Palo Alto Networks PAN-OS / Prisma Access	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	Qilin
Palo Alto Networks PAN-OS Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-565	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2026-0257

Adversaries in Action

No threat actor activity was observed or reported during this week.

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 malware **HOLLOWGRAPH, HelloInjector, HelloProxy, HelloExecutor, HelloCleaner, HelloBackdoor, SmartLoader,** and **StealC.**

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 malware **HOLLOWGRAPH, HelloInjector, HelloBackdoor,** and **SmartLoader** in Breach and Attack Simulation(BAS).

Threat Advisories

wp2shell: One Request, No Login, Full Control of WordPress Core

CVE-2026-6875: ServiceNow AI Platform Pre-Auth RCE Exploited

HOLLOWGRAPH Hides Its C2 in Microsoft 365 Calendars

HelloNet Campaign Targets Russian Infrastructure via ViPNet Update Abuse

When Your AI Agent Hands You the Malware: Inside FakeGit's AgentBaiting Campaign

July 2026 Linux Patch Roundup

Check Point SmartConsole Authentication Bypass Exploited

Qilin Rising: Continued Global Dominance and Expanded Tradecraft

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
HOLLOWGRAPH	SHA256	75e51774b8f79e5f256eaae639635f911b3e744d4774fd6068dd980255621509, F3f3006f8304788251b153d53b305322b8acab0c66ec816b8d9f101bcc851da3, B3d0f6e4e3be395fd7cf9e8101c89963d77216578cbb117a6ac9bc3564485eff
HelloInjector	SHA256	ffdc194775b2904564bbbd1cf0eb01d1a01f83ef5197d1612b6e2d69de7a4732
HelloBackdoor	MD5	16C211C96735F2FAE9361B89BD7A31BF, 1BFE2B9493128574907A8279256A8BCC, f9eed2f0158dc98e7012fb809152209c
	SHA256	68b4c76a2280e3c31130d4de12b12dfd479a476f347f5b4a58cb2483d74aba7e
SmartLoader	SHA256	6f61812b300244df4921cc0eba252181bb2138f76cfe4e6848c73a46917daee1, 66afc7d87d10dbe392898c4e5c613e0442fabb396415c2bef3a5ef2ac752c5ad
StealC	SHA256	2fc8cabf074616e31880562c58c62874e5d9e3925d2c8603460ba26560b5ffa4, ff8ee64171af93214e844d098c40b2a12e3360a23ecdc7ae9f56a31ea4248c9d, 2335e3bee58734fa08dd2b54905e0ad3e25141521f2ac3e6c3622642de392041,

Attack Name	TYPE	VALUE
StealC	SHA256	398ad6a1f99275e87c34ca3ee2785e31b1d4959f4e97d2ce35bf2f61d222454e, 4f4bd485e8615f45401e0ba17c9f6543f185dea4df144a833c4cbdd17696903e, 71962aad3717cd520083309723df6dc7da4ae153a15ea1eed990c832c63db130, c825804d4c73e0264b6c169f59128479090e1854edb5344689c909340b283d32, 2db8be4701751d2cb69f3004939826181ca09faf04ecbe0511322e21cf5955a6, b65d87bdd8660a6dae6cd183964bdd27c521d94123c0f1ae6b490d5fb4963525, 3de02e03f9890e8b6707cfdcaabf5cc829d284209f54fb8496fb7ef2dd36dfcb, a0f34df9b0a19cccf41655ef4a69c28862515a4d8eb607b9ff8992f379471d12, 7f9e2dc8918ea3f90d35ff18dd92963b81e331651d234d6373e269e036606762, 65ba3988d38f83b9ee1f31cafa5bd37dc6b72279f5618aac94d71a904efa0cac, 049f644f98603e4c350f5a46e73f5b7091df869d3cb6f66d3e76ff7767ef2823, 74a37522f2b0ef1d1887d8b93bcd488365cdc675ecb715aa0d4095aa14de7454, b97a437a3058f45bae911a3b95aea1f78ae1b52da557fc67797e36dadee07592, f3eb200ac64568dbad840f6e13fe3c8651a072b1918a4e2eb28dfefaf48a2c03, 1e40fa9dd232593a6f918e0a00efcb542758768ff99afb48c8323fef0f357b55, c4dff48038c602d884dcdf18cdd9d39b332f5b0d76bbf7018360e786dd9320fb
Qilin Ransomware	Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
	SHA256	d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6

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

July 27, 2026 • 11:50 PM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com