Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

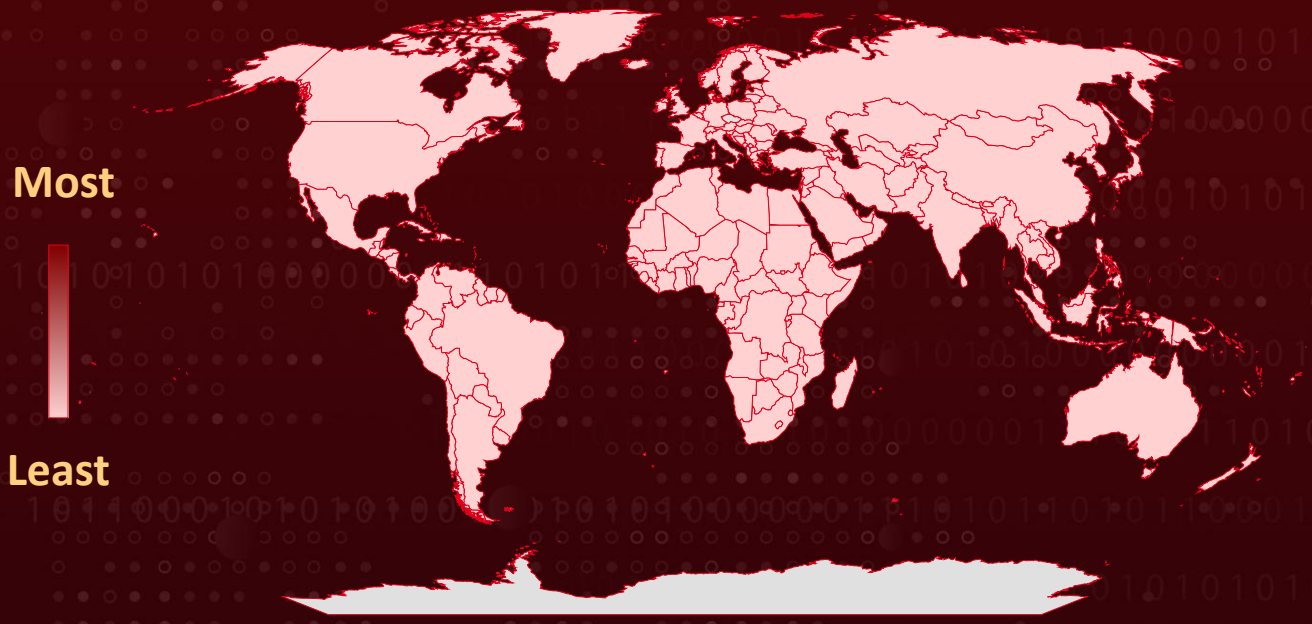
PhiliKit Implants and Wipers Hit Check Point Gateways via PHP2Shell

Date of Publication	Admiralty Code	TA Number
November 17, 2026	A1	TA2026340

Summary

First Seen: October 30, 2026
Targeted Regions: Israel (first wave, October 30); organizations across multiple countries worldwide (second wave, November 2)
Targeted Products: Check Point Security Gateway (Mobile Access portal), Check Point Security Management Server, Multi-Domain Security Management Server and Multi-Domain Log Server, Maestro Orchestrator, Check Point Force Firewalls, VMware ESXi
Malware: PhiliKit (consisting of TSGA, TSProxy)
Attack: An attacker scanned for and exploited unpatched Mobile Access portals on Check Point Security Gateways, using PHP2Shell exploitation for initial access and a local privilege-escalation flaw in the DynamicCLI interface to reach root. PHP webshells were planted in the portal's templates directory, followed by the TSGA backdoor and its embedded TSProxy networking component for persistent, encrypted access. The attacker then scanned the internal network, pivoted to a VMware ESXi host over SSH, and ran the destroy_v6 wiper, leaving a politically themed DREAM_ANNEXATION.txt note. A second, broader wave on November 2 showed no destructive activity.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-123039	Check Point Multiple Products Incorrect Permission Assignment for Critical Resource Vulnerability	Check Point Security Gateway, Security Management Server, Multi-Domain Security Management Server, Maestro Orchestrator	✓	✓	✓
CVE-2026-109618	PHP2Shell (PHP Memory Corruption Vulnerability)	PHP	✗	✓	✓
CVE-2026-109619	PHP2Shell (PHP Stale Internal Request-State Vulnerability)	PHP	✗	✓	✓

Attack Details

#1

The campaign began on October 30, 2026. An attacker scanned for Check Point Security Gateways that had not been patched and went after their internet-facing Mobile Access portals. The traffic came from 130[.]94[.]19[.]204 and hit Israeli organizations first, about a week after a fix was already available. The exploitation matched PHP2Shell and was tied to CVE-2026-109618 and CVE-2026-109619. The first signs on affected gateways were PHP session files carrying the upload_progress_pwn marker, along with hundreds of crashes in the portal's Apache and PHP workers. A second wave on November 2 went wider, hitting organizations in several countries with no clear industry focus.

#2

Once inside the portal, the attacker became root using CVE-2026-123039 in the DynamicCLI interface. A root process listens on the socket /tmp/dynamic_socket, which was left world-writable with no check on who was connecting, so any local user could send a command and have it run as root. With root access, the attacker dropped base64-decoded PHP webshells into the portal's templates folder as zz*.tpl files. The fuller webshell needed the key zz2026 and allowed system commands, PHP code, and file uploads to /tmp/.up.tpl, later copied in as challenge_render.tpl. The attacker then started the TSGA backdoor, which relaunched itself as slot_CPconfigdaemon in the boot folder and dropped its TSProxy library to /lib/libcpfwcommon.so, injecting it into appliance processes so it could answer marked attacker connections while normal traffic kept flowing.

#3

Next, the attacker ran the gogo scanner on the gateway to find internal systems and services, then moved over SSH to a VMware ESXi host using the vpxuser service account. TSGA provides encrypted remote access, configuration theft, persistence through backups and snapshots, process injection, and the ability to tamper with firewall logs. Both TSGA and TSProxy come from PhiliKit, a backdoor family seen earlier on Ivanti appliances. They share Tiny SHell roots, the same TCP port 11072 and socket, and TSProxy carries the same operator credentials, transport secrets, and TLS certificate as PhiliKit's own libdssafe.so.

#4

Through that encrypted channel, the operators could open shells, run commands and Python or Perl scripts, move files in and out, and pull part or all of the appliance configuration, while TSProxy added encrypted SOCKS-style proxying to reach deeper into the network. The destructive step came last. On the ESXi host, the attacker staged the destroy_v6 wiper to /tmp/des and ran it, deleting files recursively and overwriting them with zeros, then leaving a DREAM_ANNEXATION.txt note in every folder it touched. Attribution stays open: PhiliKit has previously been attributed to the China-nexus group UNC5221, and the gogo scanner, the LightNode hosting, and the scanning hours all point the same way, while the destruction, the focus on Israel, and the Hebrew note do not fit that picture, so the actor may have run the campaign, only sold the access, or taken part in a false-flag operation.

Recommendations

Patch the DynamicCLI Privilege Escalation Flaw: Apply the Jumbo Hotfix Accumulator that contains the fix for CVE-2026-123039, Take 14 or later for R82.20, Take 52 or later for R82.10, Take 132 or later for R82, and Take 174 or later for R81.20. The fix blocks and logs unauthenticated calls to the Dynamic CLI command instead of executing them as root.

Verify the Fix Actually Landed: After patching, run `ls -l /tmp/dynamic_socket` and confirm the output shows `srw-rw---- root config (0660)` rather than the vulnerable `srwxrwxrwx (0777)`. A patched appliance that still shows world-writable permissions has not taken the fix.

Apply the Mobile Access Portal Fix: Make sure every internet-facing Security Gateway is running the security fix that addresses the PHP2Shell exploitation path tied to CVE-2026-109618 and CVE-2026-109619. The first wave of this campaign hit organizations that were still unpatched about a week after that fix was published, so delay alone was the deciding factor.

Use the Interim Mitigation Where Patching Must Wait: If a gateway cannot be patched immediately, stop the `dynamic_server` process and keep it from restarting with `dbset process:dynamic_server` followed by `dbset :save`. Be aware this will cause the Dynamic CLI commands documented in sk144112 to fail, so plan for the operational impact.

Hunt Through the DynamicCLI Log: Search /var/log/dynamicCli.log for received commands that do not use the expected Clish wrapper, for the `#return_value#` system() sink that is rare or absent in legitimate traffic, and for exploitation-flavoured strings such as `id;`, `whoami`, `/etc/shadow`, `ncat`, `nc -`, `/dev/tcp`, `curl`, `wget`, `base64`, `useradd`, and `authorized_keys`. On patched appliances, also check for "Rejected connection from unauthorized uid" entries, since a non-zero or unexpected UID points to a blocked escalation attempt.

Look for the TSGA and TSProxy Artifacts: Check for /tmp/CPconfigdaemon, slot_CPconfigdaemon in the boot persistence directory, the hidden log /tmp/.bd.log, the dropped library /lib/libcpfwcommon.so, the staged upload path /tmp/.up.tpl, and the Unix socket /tmp/.p_sock. Also review PHP session files under /opt/CPcvpn-R81.20/tmp/ for the upload_progress_pwn marker and correlate any burst of Apache or PHP segmentation faults with portal access logs.

Block the Known Infrastructure and Watch Port 11072: Block and alert on traffic to and from 130[.]94[.]19[.]204 and 130[.]94[.]19[.]168, and monitor for TCP 11072 listening on or reachable from gateway interfaces, since that port carries the implant's authenticated, encrypted channel.

Rotate Credentials and Treat Configurations as Stolen: Assume any configuration held on a compromised gateway was collected over the encrypted channel. Rotate administrator passwords, API keys, certificates, pre-shared keys, and VPN credentials, and reissue anything the appliance configuration could have exposed.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1078: Valid Accounts	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1055: Process Injection	
	T1564: Hide Artifacts	
	T1070: Indicator Removal	
Discovery	T1046: Network Service Discovery	
Lateral Movement	T1021: Remote Services	T1021.004: SSH
Collection	T1602: Data from Configuration Repository	T1602.002: Network Device Configuration Dump
Command and Control	T1573: Encrypted Channel	
	T1571: Non-Standard Port	
	T1090: Proxy	T1090.001: Internal Proxy
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1485: Data Destruction	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	edb3e92eb7bda7413a09edcc4b1ba3cbed4bcdf42808a8abce63b6e4c3fda2b3, 4171b521fa6441382aa2fa014a08e18ff9a6e0ab6096c9144072bf46b37a2ec8, d7549671c7189979f0624ec52dad9ea6a707d23146e3585ab8f8c4720eca0c63, 3b51080a909023f7d484e2443740b572307ce0054eb9e32d98f0a06bfcd2db90, c7d9477309fac6c638a1128442056a242de086996add8cb49cd6496c36003237, 0522937c0c0337be54fe25493539e5f5f8ceb9742c980aaff1cfc9515f3a96f7, ee16e1695711b9d60c62925fcfb2fe1a29c18ae26565bc05410a14e16d2a39d7, fb1a6235eb6bce8c9ec8cd8bb85f17c9c2bde8ecb45b7a243a30ceadf26654da
IPv4	130[.]94[.]19[.]204, 130[.]94[.]19[.]168
Filename	slot_CPconfigdaemon, CPconfigdaemon, destory_v6, gogo, philistine, libdssafe.so, libcpfwcommon.so, DREAM_ANNEXATION.txt, challenge_render.tpl, zz*.tpl
File Path	/tmp/CPconfigdaemon, /tmp/.bd.log, /lib/libcpfwcommon.so, /tmp/.up.tpl, /tmp/.p_sock, /tmp/des, /opt/CPcvpn-R81.20/tmp/

Patch Links

CVE-2026-109618 and CVE-2026-109619: https://www.php.net/archive/2026.php#2026-10-21-5

CVE-2026-123039: https://support.checkpoint.com/results/sk/sk1000362

References

https://research.checkpoint.com/2026/php2shell-exploitation-on-check-point-gateway/

https://support.checkpoint.com/results/sk/sk1000362

http://www.hivepro.com/threat-advisory/php2shell-your-application-code-is-clean-but-the-engine-underneath-it-isnt

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

November 17, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com