INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:04 UTC

PCPJack Credential Stealer Chains Five CVEs for Worm-Like Cloud Propagation and Broad Credential Harvest

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0288
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cloud infrastructure (unspecified vendors), container environments, developer tooling, productivity services, financial services platforms
Published	2026-05-07T13:45:00
Discovery Source	Rss

Executive Summary

PCPJack is an active credential theft campaign targeting cloud-native infrastructure reported to exploit multiple unconfirmed vulnerabilities in order to propagate automatically across container environments, developer platforms, and financial service integrations. Organizations running modern cloud stacks face broad credential exposure across cloud provider keys, container registry tokens, and financial service access tokens. The self-propagating design means a single compromised entry point can cascade across interconnected systems before detection.

Technical Analysis

PCPJack is a credential harvesting framework with worm-like lateral movement capability, observed targeting exposed cloud infrastructure. As of this report date, specific CVE identifiers, patch advisories, and confirmed IOCs have not been published in authoritative sources (CISA, NVD, affected vendors). The following assessment is based on threat intelligence reporting and should be treated as indicators pending confirmation. Reporting indicates the toolset achieves propagation across cloud-native, container, developer tooling, and financial service environments. The toolset reportedly displaces TeamPCP artifacts on infected hosts, suggesting adversarial competition over compromised infrastructure. Credential targets span cloud provider API keys (T1552.005), container registry tokens, developer platform credentials, and financial service access tokens. Exfiltration is routed through attacker-controlled infrastructure (T1041, T1567). Based on the reported attack pattern and suspected vulnerabilities, likely CWE categories include insufficiently protected credentials

(CWE-522), improper access control (CWE-284), cleartext storage (CWE-312), and incorrect permission assignment (CWE-732). MITRE ATT&CK coverage includes T1190 (exploit public-facing application), T1210 (exploitation of remote services), T1619 (cloud storage object discovery), T1098 (account manipulation), T1078/T1078.004 (valid accounts, cloud accounts), T1534 (internal spearphishing), T1539 (steal web session cookie), and T1485 (data destruction). Attribution has not been established. Monitoring for vendor and threat intelligence updates is warranted to confirm CVE identifiers and IOCs. Primary reporting source: The Hacker News (T3, 2026-05-xx). Note: This assessment derives from vendor and security news outlets (T3 sources). No T1 authoritative sources (CISA, NVD, MITRE, law enforcement) have published independent confirmation as of this report date.

Action Checklist

1. Step 1: Containment (Patch Availability: Not Confirmed), As specific CVE identifiers have not been published, vendor patches are not yet available. Audit externally exposed cloud services, APIs, and container management interfaces immediately. Revoke and rotate any cloud provider keys, container registry tokens, and developer platform credentials that may have been accessible from internet-facing systems. Prioritize accounts with broad IAM permissions. Containment through credential rotation and access restriction is the primary lever at this time.
2. Step 2: Detection, Search cloud provider logs (AWS CloudTrail, Azure Activity Log, GCP Audit Logs) for anomalous API calls, unexpected credential enumeration, object storage discovery activity, and lateral access across accounts or projects. Review container runtime logs for unexpected process execution or outbound connections. Look for signs of TeamPCP artifact displacement as an infection indicator. Monitor for exfiltration patterns to unknown external endpoints on non-standard ports.
3. Step 3: Eradication, Specific CVE identifiers and vendor patch IDs are not confirmed in current reporting. Apply least-privilege IAM policies across all cloud environments. Disable unused service accounts and API keys. Remove any unrecognized tooling or scripts from container environments. Enforce secrets management through a dedicated vault (e.g., HashiCorp Vault, AWS Secrets Manager) rather than environment variables or config files.
4. Step 4: Recovery, After credential rotation, validate that revoked keys are no longer functional. Monitor for re-access attempts using previously compromised credentials. Review cloud provider access logs for 30 days prior to detection to establish a baseline infection timeline. Confirm no persistent backdoor accounts were created (T1098) before restoring normal operations.
5. Step 5: Post-Incident, This campaign exposes gaps in secrets hygiene, over-permissioned service accounts, and insufficient monitoring of lateral cloud-to-cloud access. Conduct a secrets inventory and eliminate hardcoded or improperly stored credentials (CWE-522, CWE-312). Implement CSPM tooling to continuously flag misconfigured permissions (CWE-732, CWE-284). Establish alerting on bulk credential enumeration and anomalous cross-service API activity.

Detection Guidance

Detection should focus on behavioral indicators given the absence of confirmed CVE identifiers or published IOCs. Key signals: (1) Cloud API calls for credential enumeration or secrets listing outside normal service patterns, AWS GetSecretValue, Azure KeyVault reads, GCP Secret Manager access from unexpected principals; (2) Container runtime anomalies, unexpected process spawning, outbound connections to unfamiliar

IPs, or file writes to locations consistent with tool staging; (3) TeamPCP artifact removal or replacement activity on hosts as a displacement indicator; (4) Exfiltration signals, large or frequent outbound data transfers to external IPs, particularly on non-standard ports, mapped to T1041 and T1567; (5) New or modified IAM roles, service account bindings, or SSH keys added without change management records (T1098); (6) Lateral movement between cloud accounts or projects via shared credentials or federation tokens (T1078.004). SIEM correlation: chain authentication events with subsequent resource discovery and outbound transfer within short time windows. No confirmed IOC hashes, domains, or IPs are available in current reporting. Treat all detections as requiring manual triage until CISA, the affected vendors, or MITRE publish official confirmation of CVE identifiers and IOCs.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not confirmed in available reporting]`	Attacker-controlled exfiltration infrastructure referenced in campaign description; specific domains not published in open-source sources as of this writing	LOW

Framework Mappings

MITRE-ATTACK

- **T1552** — Unsecured Credentials
- **T1552.001** — Credentials In Files
- **T1098** — Account Manipulation
- **T1078.004** — Cloud Accounts
- **T1485** — Data Destruction
- **T1619** — Cloud Storage Object Discovery
- **T1210** — Exploitation of Remote Services
- **T1078** — Valid Accounts
- **T1539** — Steal Web Session Cookie
- **T1552.005** — Cloud Instance Metadata API
- **T1190** — Exploit Public-Facing Application
- **T1041** — Exfiltration Over C2 Channel
- **T1534** — Internal Spearphishing
- **T1567** — Exfiltration Over Web Service

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **3.3** — Configure Data Access Control Lists
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552	Unsecured Credentials	Credential-Access
T1552.001	Credentials In Files	Credential-Access
T1098	Account Manipulation	Persistence

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1485	Data Destruction	Impact
T1619	Cloud Storage Object Discovery	Discovery
T1210	Exploitation of Remote Services	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1552.005	Cloud Instance Metadata API	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1534	Internal Spearphishing	Lateral-Movement
T1567	Exfiltration Over Web Service	Exfiltration

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/pcpjack-credential-stealer-exploi...	T3
Common Cloud Vulnerabilities & Security Risks Explained - OPSWAT	https://www.opswat.com/blog/common-cloud-vulnerabilities-security-r...	T3
Top 11 Cloud Security Vulnerabilities and How to Fix Them - Wiz	https://www.wiz.io/academy/cloud-security/common-cloud-vulnerabilities	T3
Cloud threat horizons report H2 2025 - Google Cloud	https://cloud.google.com/security/report/resources/cloud-threat-hor...	T3
Top 15 Cloud Security Vulnerabilities - SentinelOne	https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-...	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-07 19:04 UTC by TJS Security Command Center