FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
02 JULY 2026
FLASH-20260702-01

Cyber Criminal Group TeamPCP

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to highlight the tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with the cyber criminal group TeamPCP. TeamPCP actors have conducted large-scale software supply chain compromises by targeting widely used developers and security tools, gaining access to victim environments and extracting sensitive data, including but not limited to cloud access tokens, SSH keys, and Kubernetes secrets. The FBI encourages organizations to contact the FBI if they have been compromised, and to implement the actions in the Recommendations section to reduce the likelihood and impact of compromise by TeamPCP actors.

Threat

In 2026, TeamPCP compromised trusted software distribution channels by injecting malicious code into legitimate packages to modify software components and development dependencies. This allowed the threat actors to push trojanized updates that appeared normal but secretly installed credential-stealing malware and persistent backdoors, giving the threat actors persistent access to developer environments and downstream systems.

TeamPCP modified tools including, but not limited to, Trivy, KICS, LiteLLM, and the Telnyx Python SDK. These tools are commonly integrated into enterprise development continuous integration (CI)/continuous delivery (CD) pipelines, cloud infrastructure, and security workflows. By weaponizing these supply chain entry points, the threat actors were able to introduce malicious code into victim environments at scale. TeamPCP has also engaged in extortion and collaboration with cyber actors from other threat actor groups, including publishing victim names on a public leak site and threatening disclosure of stolen data. Organizations impacted by this campaign should treat exfiltrated data and credentials as a persistent risk, as affiliated threat actors are likely to weaponize them long after the initial compromise.

Malware Deployed by TeamPCP

- **CanisterWorm:** designed to harvest sensitive information, including cloud access tokens, credentials, API keys, and other authentication material associated with services such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

- **SANDCLOCK:** a credential stealing tool used by TeamPCP that extracts AWS credentials, Kubernetes ServiceAccount tokens, local environment variables, and cryptocurrency wallet data.

- **Mini Shai-Hulud**: a self-replicating, cross-ecosystem (npm/PyPI) software supply chain worm campaign.

- **Miasma**: a variant of Mini Shai-Hulud that self-propagates across open-source registries such as npm and PyPI, harvesting credentials and poisoning configuration files.

Indicators[1]

IP Addresses		
83.142.209.11	45.148.10.212	83.142.209.194
83.142.209.203	94.154.172.43	67.217.57.240

Domains		
scan.aquasecurtiy[.]org	checkmarx[.]zone	checkmarx[.]zone/vsx
checkmarx[.]zone/static/checkmarx-util-1.0.4.tgz	checkmarx[.]zone/raw	models.litellm[.]cloud
tdtqy-oyaaa-aaaae-af2dq-cai.raw.icp0[.]io	check.git-service[.]com	t.m-kosche[.]com
git-tanstack[.]com	recv.hackmoltrepeat[.]com	audit.checkmarx[.]cx/v1/telemetry

Hashes
18a24f83e807479438dcab7a1804c51a00dafc1d526698a66e0640d1e5dd671a
c37c0ae9641d2e5329fcdee847a756bf1140fdb7f0b7c78a40fdc39055e7d926
0c0d206d5e68c0cf64d57ffa8bc5b1dad54f2dda52f24e96e02e237498cb9c3a
61ff00a81b19624adaad425b9129ba2f312f4ab76fb5ddc2c628a5037d31a4ba
f398f06eefcd3558c38820a397e3193856e4e6e7c67f81ecc8e533275284b152
7df6cef7ab9aae2ea08f2f872f6456b5d51d896ddda907a238cd6668ccdc4bb7
5e2ba7c4c53fa6e0cef58011acdd50682cf83fb7b989712d2fcf1b5173bad956
e9b1e069efc778c1e77fb3f5fcc3bd3580bbc810604cbf4347897ddb4b8c163b
069ac1dc7f7649b76bc72a11ac700f373804bfd81dab7e561157b703999f44ce
7d80b3ef74ad7992b93c31966962612e4e2ceb93e7727cdbd1d2a9af47d44ba8
aeaf583e20347bf850e2fabdcd6f4982996ba023f8c2cd56bbd299cfd56516f5
877ff2531a63393c4cb9c3c86908b62d9c4fc3db971bc231c48537faae6cb3ec
4066781fa830224c8bbcc3aa005a396657f9c8f9016f9a64ad44a9d7f5f45e34

[1] Indicators derived from source: "Weaponizing the Protectors: TeamPCP's Multi-Stage Supply Chain Attack on Security Infrastructure" | https://unit42.paloaltonetworks.com/teampcp-supply-chain-attacks/

80a3d2877813968ef847ae73b5eeeb70b9435254e74d7f07d8cf4057f0a710ac
6f933d00b7d05678eb43c90963a80b8947c4ae6830182f89df31da9f568fea95
eb6eb4154b03ec73218727dc643d26f4e14dfda2438112926bb5daf37ae8bcdb
29ac906c8bd801dfe1cb39596197df49f80fff2270b3e7fbab52278c24e4f1a7
a68dd1e6a6e35ec3771e1f94fe796f55dfe65a2b94560516ff4ac189390dfa1c
71e35aef03099cd1f2d6446734273025a163597de93912df321ef118bf135238
a0d229be8efcb2f9135e2ad55ba275b76ddcfeb55fa4370e0a522a5bdee0120b
6cf223aea68b0e8031ff68251e30b6017a0513fe152e235c26f248ba1e15c92a
88896d478986d453f5da79b311de39d9b4b1bea95c21af1d8ef181b0f4e52fe9
21b6409a7b84446310daca5409ad6112ac60a1e4bef97736e53fff5f63bfdef4
0dc06ecdaa63fe24859cfd955053c23245c536e4733480239d14bebf12688e35
633c8410ee0413ca4b090a19c30b20c03f31598c25247c484846fa34c1df5b64
ef641e956f91d501b748085996303c96a64d67f63bfeef0dda175e5aa19cca90

Exfil-Repo
tpcp-docs
docs-tpcp

CVE	
CVE-2026-33634	CVE-2026-48027
CVE-2026-45321	CVE-2025-55182

Information Requested

The FBI encourages any suspected TeamPCP intrusions to be reported to their local FBI field office at www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324) or to the FBI Internet Crime Complaint Center at www.ic3.gov.

Retain all information regarding the incident, including affected package names and versions, CI/CD pipeline logs, network logs, credentials or secrets potentially exposed, and any extortion communications or ransom demands.

When available, include the date and time the compromise was discovered, estimated date of initial infection, type of activity observed, systems and environments affected, name of the submitting company or organization, and designated point of contact.

Recommendations

The FBI recommends organizations take the steps below to improve their security posture in response to the evolving entities targeted in this scheme. FBI recommends organizations also establish and maintain strong liaison relationships with the FBI Field Office in their region. Through these partnerships, the FBI can assist with identifying vulnerabilities and mitigating potential threat activity. The FBI further recommends organizations review, and if needed, update incident response and communication plan that list actions an organization will take if impacted by a cyber incident.

The FBI recommends network defenders apply the following actions to mitigate initial unauthorized access and harden security against future malicious attempts and compromises:

- Pin all GitHub Actions workflows to verified commit SHA hashes rather than floating version tags or branch references.
- Rotate all CI/CD secrets, publishing tokens, and cloud credentials accessible during exposure windows identified in the campaign timeline above.
- Search GitHub organization repositories for ‘tpcp-docs’ or ‘docs-tpcp’-named repositories, which are created by the worm using stolen credentials.
- Enforce least-privilege permissions on all CI/CD service accounts and registry publishing tokens; apply token scoping to prevent cross-repository propagation.
- Implement runtime behavioral monitoring (e.g., Harden-Runner or equivalent) for CI/CD pipelines to detect unexpected outbound network connections from runner processes.
- Audit all npm package maintainer accounts for stale or expired recovery email domains, which TeamPCP exploits to take over publishing credentials.
- Require phishing-resistant multi-factor authentication (MFA) for all accounts with code repository or package registry publishing access.
- Enforce a minimum package age threshold (e.g., 7 days) across all package installation environments to reduce exposure to newly published malicious versions before community detection occurs.
- Maintain offline, immutable backups of critical repositories and package release artifacts.

CI/CD Pipeline Mitigations

- Improve Credential Hygiene
    - Store credentials in dedicated, encrypted secrets management solutions; avoid hardcoding credentials in code or configuration files.

  - Prefer temporary credentials over static credentials; rotate all credentials regularly and immediately after any suspected compromise.
  - Scan repositories and logs for exposed secrets using automated tools and remove any found.
- Harden System and Pipeline Configurations
  - Change default credentials and enforce strong password policies on all systems.
  - Disable unnecessary services and remove unused software from CI/CD systems.
  - Regularly review and harden system configurations according to security best practices.
- Secure Artifact Integrity
  - Integrate automated integrity checks (hashes, signatures) into CI/CD pipelines before artifacts are published or deployed.
  - Maintain trusted, access-controlled artifact repositories and monitor for unauthorized changes.
- Govern Third-Party Service Usage
  - Maintain an inventory of all third-party services integrated into CI/CD pipelines.
  - Limit permissions and access for external services; isolate and sandbox integrations where possible.
  - Periodically review and update third-party integrations for security compliance.
- Enhance Logging and Visibility
  - Enable comprehensive logging across all CI/CD systems, including authentication events, configuration changes, and artifact handling.
  - Centralize log management and monitor logs for anomalies, suspicious activity, and failed login attempts.
  - Retain audit logs for incident investigations and compliance requirements.
- Monitor for Anomalous Pipeline Behavior
  - Continuously monitor pipeline activity for unexpected triggers, privilege escalations, or unauthorized artifact uploads.
  - Alert on deviations from normal pipeline execution patterns and respond promptly.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated considering your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistently with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the FBI.

This FLASH was coordinated with DHS/CISA and is marked **TLP: CLEAR**.