



An Lárionad Náisiúnta  
Cibearshlándála  
National Cyber  
Security Centre

NCSC 2603311404

# NCSC Advisory

## TeamPCP Supply-Chain Attack

31 March, 2026

**STATUS: TLP:CLEAR**

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



## Summary

The TeamPCP supply-chain attack involves the compromise of various development ecosystems, including GitHub repositories, container registries, and Kubernetes clusters. The attackers use stolen tokens to spread a worm called CanisterWorm. This advisory provides indicators of compromise (IoCs), affected software versions, and recommended defensive steps.

## Timeline

**Late February** a malicious actor was able to steal a privileged token.

**March 19** the malicious actor used the token to push changes which manipulated existing tags of previous releases, this would have caused anyone using these tags in their CI pipelines to download the compromised versions the next occasion the pipeline ran.

**March 19** the attack was discovered, and malicious artefacts removed from distribution.

**March 20** New safe versions were published.

**March 22**, a threat actor used compromised credentials to publish a malicious Trivy v0.69.5 and v0.69.6 DockerHub images.

## Products Affected

Product	Impacted Version or Tag
aquasecurity/trivy-action	75 of 76 tags affected
aquasecurity/setup-trivy	All 7 tags affected
checkmarx/kics-github-action	All 35 tags affected
checkmarx/ast-github-action	v2.3.28 affected
<b>OpenVSX Extensions:</b>	
ast-results	v2.53.0 affected
cx-dev-assist	v1.7.0 affected
<b>Python Packages:</b>	
litellm	v1.82.7 + v1.82.8 affected
<b>dockerhub/gchr.io registry images:</b>	dockerhub trivy images v0.69.5 and v0.69.6
Please see <a href="https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23">https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23</a> for full details of dockerhub exposure window and impacted images.	





## Indicators of Compromise:

Presence of the following C2 domains in network logs:

*aquasecurity[.]org*  
*scan.aquasecurity[.]org*  
*checkmarx[.]zone*  
*models.litellm[.]cloud*  
*tdtqy-oyaaa-aaaae-af2dq-cai.raw.icp0[.]jio*  
*plug-tab-protective-relay.trycloudflare[.]com*

Presence of the following IP addresses in network logs:

*209.159.147[.]239*  
*45.148.10[.]212*

Presence of files named *tcp.tar.gz* created on developer machines or in CI/CD pipelines and similar DevOps environments.

New Github repositories with names like *tcp-docs* or *docs-tcp*

## Recommended Defensive Steps:

Check for the presence of the GitHub repository used for data exfiltration, named 'tcp-docs'.

Consider all information that was accessible in environments where a malicious software version was executed or that was connected to the attacker's C2 servers as compromised and replace:

*Cloudreferences (AWS, Azure, GCP)*

*GitHub/Git-tokens*

*SSH-KEYS*

*References for containerregisters*

*Kubernetes-tokens*

*API-key, shell-environmentvariabels (env)*

*Remove malicious binary files and suspicious build artifacts.*

*Check whether persistence has been established on the system by checking for the presence of the following file:*

*~/.local/share/pgmon/service.py — Python implant*



## Additional Recommendations:

Hunt in network logs for connections to the domains and IP addresses used as C2 servers for exfiltration. Regularly review and update dependencies in development ecosystems.

## Impact

TeamPCP is known to be financially motivated and their known TTPs include:

- Initial Access: Exploiting public-facing applications (e.g., React2Shell) and exposed APIs(Docker, Kubernetes, Redis, Ray dashboards).
- Execution: Utilizing command and scripting interpreters (Shell, Python) and container administration commands.
- Persistence: Achieving persistence through scheduled tasks/cron (systemd services) and deploying containers.
- Privilege Escalation: Exploiting privileged Kubernetes workloads and escaping to the host.
- Credential Harvesting: Collecting credentials from files (.env, SSH keys, Git credentials, cloud secrets) and stealing application access tokens.
- Lateral Movement: Deploying containers and using remote services (container hopping).
- Command and Control: Establishing C2 via proxies (FRPS, GOST, P2P relays), application layer protocols, and encrypted channels (Sliver C2 framework).
- Exfiltration: Over C2 channels and to web services.
- Impact: Resource hijacking (XMRig cryptomining) and potential data encryption for impact(ransomware/extortion claims).

Be aware of the potential risks associated with TeamPCP's operations, which may include:

- Exfiltration of sensitive data, such as secrets, cloud credentials, SSH keys.
- Use of compromised tokens to spread malware in development environments.
- Deployment of ransomware and extortion attacks through infected systems.

TeamPCP's operations are fueled by the large volume of secrets already exfiltrated, and additional stages of exploitation should be expected in the coming weeks and months. Therefore, it is essential to maintain a vigilant approach to supply chain security and monitor for potential indicators of compromise.



## Recommendations

The NCSC strongly recommends moving to known safe releases and pin to these versions only moving to newer releases that are also known to be safe. SHA/Hash pinning and verification is preferred to simple version based pinning where supported. If during remediating and hunting in your environments you discover indicators associated with compromise, the NCSC CSIRT would appreciate if you could share this information with us so that the extent of this attack can be tracked.

This advisory is based on information provided by various sources, including:

<https://www.aikido.dev/blog/teampcp-stage-payload-canisterworm-iran>

<https://krebsonsecurity.com/2026/03/canisterworm-springs-wiper-attack-targeting-iran/>

<https://docs.litellm.ai/blog/security-update-march-2026>

<https://www.aquasec.com/blog/trivy-supply-chain-attack-what-you-need-to-know/>

<https://www.microsoft.com/en-us/security/blog/2026/03/24/detecting-investigating-defending-against-trivy-supply-chain-compromise/>

