TEAMPCP SUPPLY CHAIN

Checkmarx Attack Chain

47 days of persistent access. Incomplete rotation. Cascading compromise.

> *"This malware didn't do much. We're tired, and we have bigger targets. But if you're reading this, then hugs from TeamPCP."*
>
> — ~/hugs_from_teamPCP.txt left by malware

May 9	Jenkins AST Plugin compromised
Apr 22	Docker Hub poisoned → Bitwarden cascade
Mar 23	OpenVSX + GitHub Actions hijacked
Mar 19	Trivy attack harvests Checkmarx credentials

Rami McCarthy

`ramimac.me/teampcp`

MAY 9, 2026

Jenkins AST Plugin Compromised

Persistent access exploited after failed March eviction

IMPACT

~500 Jenkins plugin installs exposed to credential stealer. Encrypted exfil via 11 "Mini Shai-Hulud" dead-drop repos.

Malicious Plugin Published

checkmarx-ast-scanner v2026.5.09 pushed to plugins.jenkins.io via compromised identity

Bun Runtime Payload

cli.js credential stealer harvests Jenkins secrets, cloud tokens, SSH keys

Dead-Drop Exfiltration

Dune-themed repos (kralizec-navigator, fedaykin-laza, prescient-melange) receive encrypted data

ROOT CAUSE

Attacker credentials never fully revoked after March incident.

APRIL 22-25, 2026

Docker Hub + Bitwarden Cascade

KICS images poisoned, triggering downstream npm compromise

IMPACT

7 KICS Docker tags overwritten. Bitwarden Dependabot pulls malicious image → @bitwarden/cli hijacked. 334 npm downloads in 93 minutes.

Docker Hub Authentication

Attacker uses valid Checkmarx publisher credentials to overwrite :latest, :alpine, v2.1.20, v2.1.21

Bitwarden Token Leaked

Dependabot pulls poisoned KICS image → trusted-publisher npm token exfiltrated

LAPSUS$ Data Dump

April 25: Stolen Checkmarx data (from March 30 exfil) published on dark web

ROOT CAUSE

Docker Hub credentials remained valid 30 days after initial remediation

MARCH 23, 2026

OpenVSX + GitHub Actions Hijacked

126 tags force-pushed via compromised service accounts

IMPACT

35 KICS tags + 91 AST tags redirected to malicious commits. Memory dumping on GitHub runners. C2 at checkmarx.zone.

Service Account Takeover

cx-plugins-releases + ast-phoenix accounts compromised via harvested credentials

OpenVSX Extensions

ast-results v2.53.0, cx-dev-assist v1.7.0 published 12 seconds apart

Runner Memory Dump

Payload extracts Runner.Worker process memory, carves JSON objects flagged as secrets

ROOT CAUSE

Checkmarx service account credentials harvested via Trivy supply chain attack

MARCH 19, 2026

Trivy Supply Chain Attack

The upstream compromise that enabled everything

INITIAL ACCESS

❯ TeamPCP compromised Trivy via vulnerable pull_request_target workflow. Checkmarx used Trivy in CI/CD —> credentials harvested.

Pwn Request Exploit

Vulnerable workflow in aquasecurity/trivy exploited to steal aqua-bot PAT

Incomplete Rotation

"Wasn't atomic and attackers may have been privy to refreshed tokens"

47-Day Chain Reaction

March 19 → May 9: Jenkins, Docker Hub, OpenVSX, GitHub Actions, npm all compromised

LESSON

Credential rotation must be atomic and complete. Partial remediation = persistent access.