Tracking & Detecting GhostSocks Malware

By Isabel Evans

Published: 2026-03-26 · Archived: 2026-05-06 02:01:00 UTC

Software supply-chain attacks in 2026

Software supply-chain attacks now represent the primary threat shaping the 2026 security landscape. Rather than relying on exploits at the perimeter, attackers are targeting the connective tissue of modern engineering environments: package managers, CI/CD automation, developer systems, and even the security tools organizations inherently trust.

These incidents are not isolated cases of poisoned code. They reflect a structural shift toward abusing trusted automation and identity at ecosystem scale, where compromise propagates through systems designed for speed, not scrutiny. Ephemeral build runners, regardless of provider, represent high-trust, low-visibility execution zones.

The Axios compromise and the cascading Trivy campaign illustrate how quickly this abuse can move once attacker activity enters build and delivery workflows. This blog provides an overview of the latest supply chain and security tool incidents with Darktrace telemetry and defensive actions to improve organizations defensive cyber posture.

1. Why the Axios Compromise Scaled

On 31 March 2026, attackers hijacked the npm account of Axios's lead maintainer, publishing malicious versions 1.14.1 and 0.30.4 that silently pulled in a malicious dependency, plain-crypto-js@4.2.1. Axios is a popular HTTP client for node.js and processes 100 million weekly downloads and appears in around 80% of cloud and application environments, making this a high-leverage breach [1].

The attack chain was simple yet effective:

- A compromised maintainer account enabled legitimate-looking malicious releases.
- The poisoned dependency executed Remote Access Trojans (RATs) across Linux, macOS and Windows systems.
- The malware beaconed to a remote command-and-control (C2) server every 60 seconds in a loop, awaiting further instructions.
- The installer self-cleaned by deleting malicious artifacts.

All of this matters because a single maintainer compromise was enough to project attacker access into thousands of trusted production environments without exploiting a single vulnerability.

A view from Darktrace

Multiple cases linked with the Axios compromise were identified across Darktrace's customer base in March 2026, across both Darktrace / NETWORK and Darktrace / CLOUD deployments.

In one Darktrace / CLOUD deployment, an Azure Cloud Asset was observed establishing new external HTTP connectivity to the IP 142.11.206[.]73 on port 8000. Darktrace deemed this activity as highly anomalous for the device based on several factors, including the rarity of the endpoint across the network and the unusual combination of protocol and port for this asset. As a result, the triggering the "Anomalous Connection / Application Protocol on Uncommon Port" model was triggered in Darktrace / CLOUD. Detection was driven by environmental context rather than a known indicator at the time. Subsequent reporting later classified the destination as malicious in relation to the Axios supply-chain compromise, reinforcing the gap that often exists between initial attacker activity and the availability of actionable intelligence. [5]

Additionally, shortly before this C2 connection, the device was observed communicating with various endpoints associated with the NPM package manager, further reinforcing the association with this attack.

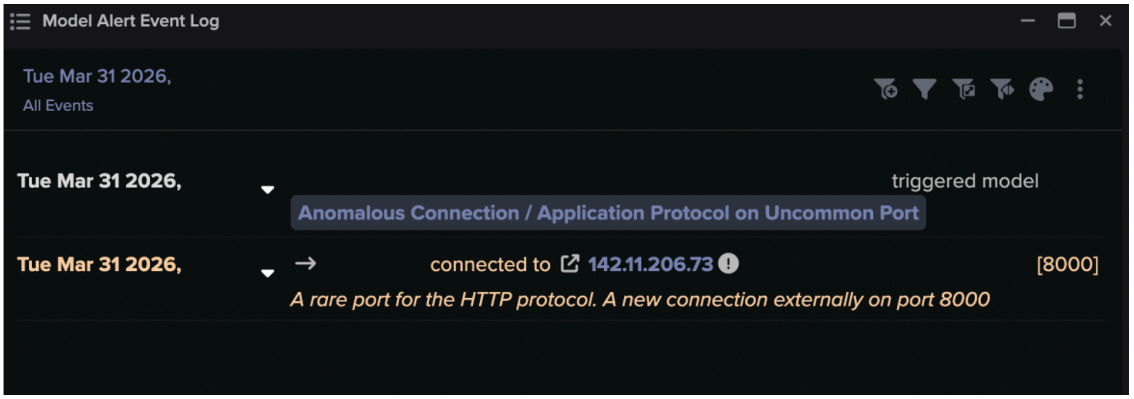

Figure 1: Darktrace's detection of the unusual external connection to 142.11[.]206[.]73 via port 8000.

Within Axios cases observed within Darktrace / NETWORK customer environments, activity generally focused on the use of newly observed cURL user agents in outbound connections to the C2 URL sfrclak[.]com/6202033, alongside the download of malicious files.

In other cases, Darktrace / NETWORK customers with Microsoft Defender for Endpoint integration received alerts flagging newly observed system executables and process launches associated with C2 communication.

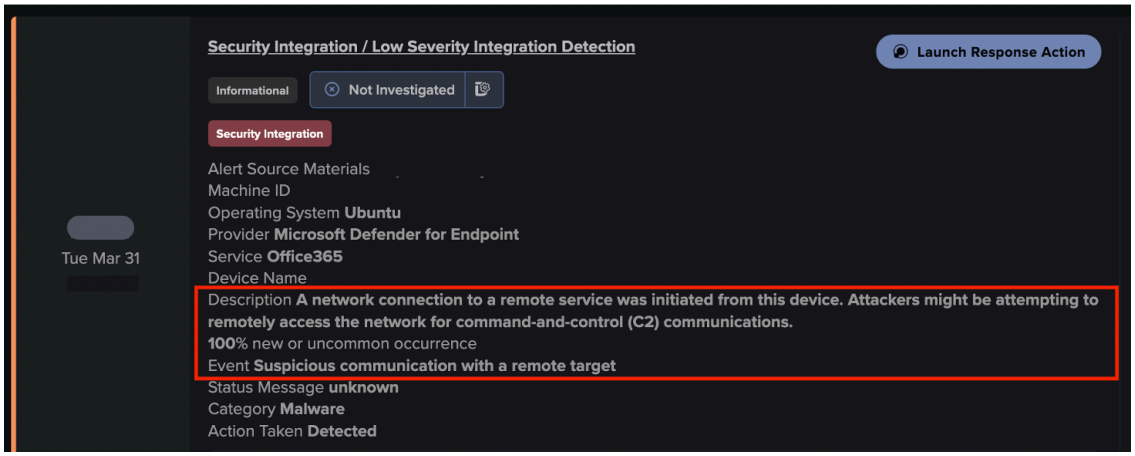

Figure 2: A Security Integration Alert from Microsoft Defender for Endpoint associated with the Axios supply chain attack.

2. Why Trivy bypassed security tooling trust

Between late February and March 22, 2026, the threat group TeamPCP leveraged credentials from a previous incident to insert malicious artifacts across Trivy's distribution ecosystem, including its CI automation, release binaries, Visual Studio Code extensions, and Docker container images [2].

While public reporting has emphasized GitHub Actions, Darktrace telemetry highlights attacker execution within CI/CD runner environments, including ephemeral build runners. These execution contexts are typically granted broad trust and limited visibility, allowing malicious activity within build automation to blend into expected operational workflows, regardless of provider.

This was a coordinated multi-phase attack:

- 75 of 76 of trivy-action tags and all setup-trivy tags were force-pushed to deliver a malicious payload.
- A malicious binary (v0.69.4) was distributed across all major distribution channels.
- Developer machines were compromised, receiving a persistent backdoor and a self-propagating worm.
- Secrets were exfiltrated at scale, including SSH keys, Kuberenetes tokens, database passwords, and cloud credentials across Amazon Web Service (AWS), Azure, and Google Cloud Platform (GCP).

Within Darktrace's customer base, an AWS EC2 instance monitored by Darktrace / CLOUD appeared to have been impacted by the Trivy attack. On March 19, the device was seen connecting to the attacker-controlled C2 server scan[.]aquasecurtiy[.]org (45.148.10[.]212), triggering the model 'Anomalous Server Activity / Outgoing from Server' in Darktrace / CLOUD.

Despite this limited historical context, Darktrace assessed this activity as suspicious due to the rarity of the destination endpoint across the wider deployment. This resulted in the triggering of a model alert and the generation of a Cyber AI Analyst incident to further analyze and correlate the attack activity.

TeamPCP's continued abused of GitHub Actions against security and IT tooling has also been observed more recently in Darktrace's customer base. On April 22, an AWS asset was seen connecting to the C2 endpoint audit.checkmarx[.]cx (94.154.172[.]43). The timing of this activity suggests a potential link to a malicious

Bitwarden package distributed by the threat actor, which was only available for a short timeframe on April 22. [4] [3]

Figure 3: A model alert flagging unusual external connectivity from the AWS asset, as seen in Darktrace / CLOUD .

While the Trivy activity originated within build automation, the underlying failure mode mirrors later intrusions observed via management tooling. In both cases, attackers leveraged platforms designed for scale and trust to execute actions that blended into normal operational noise until downstream effects became visible.

Quest KACE: Legacy Risk, Real Impact

The Quest KACE System Management Appliance (SMA) incident reinforces that software risk is not confined to development pipelines alone. High-trust infrastructure and management platforms are increasingly leveraged by adversaries when left unpatched or exposed to the internet.

Throughout March 2026, attackers exploited CVE 2025-32975 to authentication on outdated, internet-facing KACE appliances, gaining administrative control and pushing remote payloads into enterprise environments. Organizations still running pre-patch versions effectively handed adversaries a turnkey foothold, reaffirming a simple strategic truth: legacy management systems are now part of the supply-chain threat surface, and treating them as “low-risk utilities” is no longer defensible [3].

Within the Darktrace customer base, a potential case was identified in mid-March involving an internet-facing server that exhibited the use of a new user agent alongside unusual file downloads and unexpected external connectivity. Darktrace identified the device downloading file downloads from "216.126.225[.]156/x", "216.126.225[.]156/ct.py" and "216.126.225[.]156/n", using the user agents, "curl/8.5.0" & "Python-urllib/3.9".

The timeframe and IoCs observed point towards likely exploitation of CVE-2025-32975. As with earlier incidents, the activity became visible through deviations in expected system behavior rather than through advance knowledge of exploitation or attacker infrastructure. The delay between observed exploitation and its addition to the Known Exploited Vulnerabilities (KEV) catalogue underscores a recurring failure: retrospective validation cannot keep pace with adversaries operating at automation speed.

The strategic pattern: Ecosystem-scale adversaries

The Axios and Trivy compromises are not anomalies; they are signals of a structural shift in the threat landscape. In this post-trust era, the compromise of a single maintainer, repository token, or CI/CD tag can produce large-scale blast radiuses with downstream victims numbering in the thousands. Attackers are no longer just exploiting vulnerabilities; they are exploiting infrastructure privileges, developer trust relationships, and automated build systems that the industry has generally under secured.

Supply-chain compromise should now be treated as an assumed breach scenario, not a specialized threat class, particularly across build, integration, and management infrastructure. Organizations must operate under the assumption that compromise will occur within trusted software and automation layers, not solely at the network

edge or user endpoint. Defenders should therefore expect compromise to emerge from trusted automation layers before it is labelled, validated, or widely understood.

The future of supply-chain defense lies in continuous behavioral visibility, autonomous detection across developer and build environments, and real-time anomaly identification.

As AI increasingly shapes software development and security operations, defenders must assume adversaries will also operate with AI in the loop. The defensive edge will come not from predicting specific compromises, but from continuously interrogating behavior across environments humans can no longer feasibly monitor at scale.

Credit to Nathaniel Jones (VP, Security & AI Strategy, FCISCO), Emma Foulger (Global Threat Research Operations Lead), Justin Torres (Senior Cyber Analyst), Tara Gould (Malware Research Lead)

Edited by Ryan Traill (Content Manager)

Appendices

References:

1) https://www.infosecurity-magazine.com/news/hackers-hijack-axios-npm-package/

2) https://thehackernews.com/2026/03/trivy-hack-spreads-infostealer-via.html

3) https://thehackernews.com/2026/03/hackers-exploit-cve-2025-32975-cvss-100.html

4) https://www.endorlabs.com/learn/shai-hulud-the-third-coming----inside-the-bitwarden-cli-2026-4-0-supply-chain-attack

5) https://socket.dev/blog/axios-npm-package-compromised?trk=public_post_comment-text

IoCs

- 142.11.206[.]73 – IP Address – Axios supply chain C2

- sfrclak[.]com – Hostname – Axios supply chain C2

- hxxp://sfrclak[.]com:8000/6202033 - URI – Axios supply chain payload

- 45.148.10[.]212 – IP Address – Trivy supply chain C2

- scan.aquasecurtiy[.]org – Hostname - Trivy supply chain C2

- 94.154.172[.]43 – IP Address - Checkmarx/Bitwarden supply chain C2

- audit.checkmarx[.]cx – Hostname - Checkmarx/Bitwarder supply chain C2

- 216.126.225[.]156 – IP Address – Quest KACE exploitation C2

- 216.126.225[.]156/32 - URI – Possible Quest KACE exploitation payload

- 216.126.225[.]156/ct.py - URI - Possible Quest KACE exploitation payload

- 216.126.225[.]156/n - URI - Possible Quest KACE exploitation payload

- 216.126.225[.]156/x - URI - Possible Quest KACE exploitation payload

- e1ec76a0e1f48901566d53828c34b5dc – MD5 - Possible Quest KACE exploitation payload

- d3beab2e2252a13d5689e9911c2b2b2fc3a41086 – SHA1 - Possible Quest KACE exploitation payload

- ab6677fcbbb1ff4a22cc3e7355e1c36768ba30bbf5cce36f4ec7ae99f850e6c5 – SHA256 - Possible Quest KACE exploitation payload

- 83b7a106a5e810a1781e62b278909396 – MD5 - Possible Quest KACE exploitation payload

- deb4b5841eea43cb8c5777ee33ee09bf294a670d – SHA1 - Possible Quest KACE exploitation payload

- b1b2f1e36dcaa36bc587fda1ddc3cbb8e04c3df5f1e3f1341c9d2ec0b0b0ffaf – SHA256 - Possible Quest KACE exploitation payload

Darktrace Model Detections

Anomalous Connection / Application Protocol on Uncommon Port

Anomalous Server Activity / Outgoing from Server

Anomalous Connection / New User Agent to IP Without Hostname

Anomalous File / EXE from Rare External Location

Anomalous File / Script from Rare External Location

Anomalous Server Activity / New User Agent from Internet Facing System

Anomalous Server Activity / Rare External from Server

Antigena / Network / External Threat / Antigena Suspicious File Block

Antigena / Network / External Threat / Antigena Suspicious File Pattern of Life Block

Device / New User Agent

Device / Internet Facing Device with High Priority Alert

Anomalous File / New User Agent Followed By Numeric File Download

---