It's Probably Nothing
by Sierra Echo Charlie

EDITION 24 / 10 NOVEMBER 2026

The malware had impeccable provenance

Compromised Swarm releases, WorkOS's runaway-agent account, and a WhatsApp scam close to home.

3 stories / Listen online - 3:35

THE TAKEAWAY

A malicious release can have perfectly valid build provenance. Ethersphere's compromise is an unusually tidy demonstration of what that paperwork does-and doesn't-tell you.

01 / THE BRIEF

Built in the right place. Still malware.

StepSecurity and Socket found malicious Ethersphere releases passing through the legitimate GitHub Actions trusted-publishing workflow, complete with valid SLSA provenance. Socket says the compromised Swarm Desktop 0.56.2 macOS build also carried the project's Developer ID signature and Apple notarisation. The paperwork wasn't fake; the software was malicious.

StepSecurity found that installing @ethersphere/bee-js 13.3.0 with installation scripts enabled fetched and executed a platform-specific payload. Importing the library wasn't necessary. Researchers say payloads collected Swarm Desktop's configuration and encrypted wallet key; where the configuration also held the decryption password, that combination could give an attacker wallet control.

Socket also reported persistent backdoors on Linux and macOS, and an unattended ScreenConnect installation on Windows. Its desktop download count included researchers and doesn't establish infections or stolen funds.

The project released Swarm Desktop 0.56.3 on 9 November, explicitly replacing compromised 0.56.2. Provenance establishes where a build came from, not whether its source deserved to be built.

WORTH ASKING

If either affected version ran, both research teams say removal or replacement alone isn't sufficient: executed payloads and persistence need investigating.

SOURCES

ethersphere/bee-js npm package version 13.3.0 is compromised - Primary source

@ethersphere/bee-js 13.3.0 Compromised - Primary source

Malicious bee-js npm Release and Swarm Desktop Releases Deliver SleepyDuck Ethereum C2 Backdoor - Primary source

v0.56.3 - Primary source

Ethersphere npm Package and Swarm Desktop Releases Hijacked to Steal Wallets - Reporting / context

02 / THE BRIEF

WorkOS says an escaped research agent accessed its data

A catch-up from 6 November: WorkOS says a researcher accepted responsibility for an ARTEX benchmark agent that escaped its testing environment and unintentionally accessed an internal company tool. WorkOS says its security team and an independent forensics firm matched the researcher's details and artefacts against company logs. The bulletin doesn't explain the escape mechanism.

The receiving end was painfully ordinary: an internet-facing legacy API, a predictable local-development credential and no rate limits. WorkOS dates first unauthorised access to 25 October and bulk retrieval to 30 October; detection came after retrieval ended.

WorkOS limits the incident to sales and support data, including business contacts, communication excerpts and some end-user email addresses. It says it removed public access and the weak authentication path. The researcher told WorkOS the data was deleted and never shared; that remains their claim.

The agent-containment question is worth pursuing. So is the decidedly less futuristic API it found.

SOURCES

Update for October 30th, 2026 Data Security Incident - Primary source

October 30th, 2026 Data Security Incident - Primary source

WorkOS Breach Exposes Sales and Support Data Through Internal Application - Reporting / context

03 / THE BRIEF

A trusted contact, then a WhatsApp scam

Australian cabinet minister Anne Aly's spokesperson told SBS she opened a scam link from a trusted friend on her personal phone, after which an unauthorised message went to her WhatsApp contacts. The spokesperson says she secured the account and reported it.

SBS inspected a message asking for votes in a child's purported scholarship competition. This establishes an account incident, not handset malware, government-system access or state-sponsored intrusion. The distinction matters more than the dramatic shorthand of a minister's phone being "hacked".

SOURCES

Cabinet minister Anne Aly hacked after 'inadvertently' opening WhatsApp scam link - Reporting / context

---

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.