Protecting Digital Assets:

How a Crypto Exchange Prevented a Targeted Supply Chain Attack

Overview

A disguised PyPI “job scanner” tool attempted to steal credentials during onboarding, but Veracode intercepted it before it ever touched the environment.

Problem

- Crypto exchange exposed to risk by adopting open-source PyPI packages for rapid growth.
- Malicious “job scanner” tool targeted developers during hiring, aiming to steal credentials and wallets.

How We Solved It

- Veracode enforced registry-level blocking using policy rules mapped to APT threat indicators.
- Malicious package protection quarantined risk and flagged secure alternatives in real time.
- Veracode SCA mapped dependencies, surfaced transitive exposure, and enforced policy-aligned developer onboarding.

Result

- **Attack blocked pre-download; no credentials or assets lost.**
- **Protected hiring workflows and maintained safe developer toolchains.**

Background

A major cryptocurrency exchange, serving over one million users, sourced PyPI packages to build its analytics platforms. To support rapid growth and remote hiring, developers frequently adopted new and recommended open-source tools to accelerate their workflows, inadvertently increasing the company's exposure to software supply chain risks.

The Incident

In an attack mirroring trends associated with nation-state campaigns, threat actors published a malicious package on PyPI disguised as a "job scanner" tool. Designed to steal cryptocurrency wallets and credentials, the package used obfuscation to hide its true intent. A developer downloaded and installed the tool during the hiring process, unknowingly creating an entry point for attackers to gain an internal foothold.

The Impact

A successful breach would have resulted in multi-million-dollar crypto losses and the exposure of tens of thousands of user accounts. The reputational damage from such an incident could have triggered significant client churn and drawn intense regulatory scrutiny, delaying growth initiatives and eroding customer trust in the exchange's platform.

Resolution with Veracode

Veracode provided layered, preventative security at the source. The Veracode Package Firewall enforced registry-level blocking, using policy rules mapped to known Advanced Persistent Threat (APT) indicators and anomalous behavior patterns to stop the malicious package before it could be downloaded. In parallel, Veracode's malicious package protection capabilities correlated the package against real-time threat intelligence, automatically quarantining it and providing developers with vetted, secure alternatives, ensuring development workflows continued without disruption. Veracode SCA mapped the full landscape of developer tools and dependencies, surfaced APT-linked indicators across all transitive chains, and enforced policy guardrails during onboarding — standardizing safe alternatives and supporting secure growth.

Outcome

By blocking the threat pre-download and leveraging Veracode SCA to inventory dependencies and enforce policy-based upgrades, the exchange completely avoided compromise, protected hiring workflows, and standardized the use of verified, secure alternatives for ongoing development.

Key Takeaway

You can protect credentials and secure development workflows from sophisticated APT campaigns by applying threat intelligence–mapped policies at the registry-level enforcement to stop malicious indicators before they enter your environment.