Entwickler-Tools als neue Angriffsfläche

Sophos X-Ops ordnet aktuelle Supply-Chain-Angriffe ein und sieht auch KI-Tooling zunehmend im Fokus.

Aktuelle Angriffe auf den Infrastruktur-Scanner Checkmarx KICS und den Kommandozeilen-Client von Bitwarden zeigen eine neue Qualität von Supply-Chain-Attacken. Die Angreifer verteilten trojanisierte Versionen über offizielle Kanäle wie npm, Docker Hub und GitHub Actions. Sie unterwanderten damit das Vertrauen, das Entwickler in etablierte Distributionswege setzen. Neben klassischen Zugangsdaten wie GitHub-Tokens, SSH-Schlüsseln und Cloud-Credentials gerieten auch Konfigurationen von KI-Entwicklungsassistenten wie Claude, Cursor oder MCP-Setups (Model Context Protocol) ins Visier.

Entwickler-Tools als neues Angriffsziel
Sophos X-Ops, das Advanced-Threat-Research-Team des Unternehmens, sieht in dieser Aktivität einen Hinweis darauf, dass Angreifer zunehmend nicht nur Software-Abhängigkeiten, sondern auch das Vertrauen in Entwickler-Werkzeuge selbst ins Visier nehmen.

„Developer-Toolchains entwickeln sich immer stärker zu einem attraktiven Angriffsziel, weil dort privilegierte Zugriffe, Automatisierung und sensible Zugangsdaten zusammenlaufen", sagt Michael Veit, Cybersicherheits-Experte bei Sophos. „Bemerkenswert ist, dass nun offenbar auch Konfigurationen von KI-Assistenzsystemen gezielt mitgesammelt werden. Das deutet auf eine sich erweiternde Angriffsfläche hin."

Supply-Chain-Risiken mit größerer Reichweite
Aus Sicht von Sophos ist dabei entscheidend: Solche Angriffe enden häufig nicht beim Diebstahl von Zugangsdaten. Kompromittierte Tokens oder manipulierte Workflows können zum Ausgangspunkt für weiterreichende Angriffe auf Entwicklungs- und Produktionsumgebungen werden.

Hinzu kommt, dass beide Angriffe dieselbe Command-and-Control-Domain nutzten – ein Indiz, das auf einen koordinierten Akteur oder eine gemeinsam gesteuerte Kampagne hindeutet.

Die Vorfälle unterstreichen aus Sicht von Sophos vier zentrale Handlungsfelder:

- Entwickler-Tools und CI/CD-Pipelines als eigene Angriffsfläche absichern
- Tokens und Secrets konsequent rotieren und überwachen
- Software-Lieferketten auf Manipulationen prüfen
- KI-gestützte Entwicklerumgebungen in Sicherheitsmodelle einbeziehen
- Multi-Faktor-Authentifizierung (MFA) für Paket-Registries und Cloud-Konten aktivieren, wo dies noch nicht erfolgt ist.

Weitere Einzelheiten beschreibt Sophos auf seinem Blog (in englischer Sprache):
https://www.sophos.com/de-de/blog/supply-chain-attacks-hit-checkmarx-and-bitwarden-developer-tools

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de