Paket Python Terkait AI Dibobol

Penulis: Budi Rahardjo, ID-CERT/AI-CERT/PT INDOCISC

Pada akhir bulan Maret 2026 ditemukan masalah besar pada berbagai library (Python) yang digunakan untuk AI. Secara spesifik adalah LiteLLM dan PyPI.

Pada prinsipnya penyerang (attacker) memilih satu package yang tugasnya adalah untuk mengelola data pribadi (credential) yang digunakan untuk layanan AI. Misalnya data kunci OpenAI, kunci Anthropic, kunci Google, kunci Amazon, semuanya diarahkan melalui sebuah proxy (sebagai cara implementasi dari LiteLLM). Proxy ini berhasil disusupi malware sehingga semuanya dibobol secara bersamaan. (Jenis malware yang digunakan tidak jelas.)

Yang mengerikannya adalah paket yang sudah disusupi ini (sudah diracuni) ditanamkan di PyPI. Ini adalah berkas yang dijalankan oleh Python ketika dia mulai dijalankan. Jadi malware yang diinjeksikan ini langsung berjalan ketika paket tersebut ada di mesin / komputer Anda.

Awal Ketahuan

Serangan ini tedeteksi dikarenakan kode malwarenya dikembangkan kurang sempurna.s Ketika kode ini berjalan, komputer yang menjalankan kode ini *crash* dikarenakan kehabisan memori. Pengelola komputer melihat masalah ini dan melakukan investigasis. Ditemukan LiteLLM dipasang melalui Cursor MCP yang mana mereka tidak sadar sakan keberadaan LiteLLM ini.

Perjalanan Serangan

Ternyata serangan dimulai oleh TeamPCP (penyerang) dari Trivy, sebuah program untuk melakukan scanning keamanan. Pada tanggal 19 Maret 2026, LiteLLM menggunakan Trivy sebagai bagian dari pengembangannya (CI, Continuous Integration, pipeline).

LiteLLM sendiri merupakan sebuah produk yang digunakan di berbagai proyek AI untuk mempermudah pengembangan. Idenya mempermudah pemilihan model AI dari beberapa penyedia model melalui sebuah proxy. Di dalamnya kita bisa memasang akun OpenAI, Anthropic, Google, Amazon, dll. sehingga aplikasi AI kita bisa menggunakan model secara lebih transparan. Sayangnya dengan cara ini, akun kita tersebut jadi dibobol.

Setelah membobol Trivy - dan menemukan berbagai credential - TeamPCP membobol sistem yang menggunakan CI lainnya, seperti GitHub Actions, Docker Hub, npm, Open VSX. Dari sini mereka menemukan credential lainnya untuk membobol sistem lainnya. Bahkan TeamPCP mengatakan mereka akan membobol sistem-sistem lainnya.

Perlindungan

Untuk mengatasi masalah keamanan ini untuk sementara sebaiknya Anda mengganti password (credentials) yang digunakan di berbagai mesin AI. Pada saat yang sama cek apakah keberadaan LiteLLM ini ada tanpa kita sadari. Jika memang Anda menggunakan LiteLLM secara sadar, perbaharui segera dengan versi yang lebih bersih yang tidak ditanami oleh malware tesebut.

Penutup

Pengalaman ini menunjukkan bahwa kita harus berhati-hati dalam memasang aplikasi yang tidak kita ketahui sumbernya. Dalam kasus ini memang ada sedikit susah karena paket LiteLLM itu tidak kita pasang sendiri melainkan merupakan bagian dari *dependency* paket lainnya sehingga kita tidak sadar akan keberadaan paket yang sudah tersusupi tersebut. Adanya informasi yang cepat dapat membantu kita untuk mengurangi risiko tersebut.

Referensi

Tulisan ini disadur dari berbagai sumber.

https://x.com/karpathy/status/2036487306585268612 https://x.com/aakashgupta/status/2036653323978420322