

Google Tuntut Jaringan Siber Outsider Enterprise

Category: HUKUM, TEKNOLOGI

written by Redaksi | June 13, 2026



SEANTERONEWS.com – Google resmi mengajukan gugatan hukum untuk membongkar infrastruktur di balik jaringan kejahatan siber internasional berskala besar. Jaringan asal Tiongkok bernama “[Outsider Enterprise](#)” ini dituduh memanfaatkan teknologi kecerdasan buatan (AI) untuk melancarkan kampanye penipuan dan mencuri data sensitif pengguna.

Menurut laporan resmi Google, kelompok kriminal tersebut menggunakan AI untuk memproduksi SMS penipuan yang meniru identitas Google serta berbagai merek global lainnya. Modus penipuan ini dirancang untuk mencuri kata sandi (password) serta nomor kartu kredit para korban di berbagai belahan dunia.

Skala kerugian yang ditimbulkan oleh kelompok ini sangat masif. Biro Investigasi Federal AS (FBI) mengungkapkan bahwa sejak Juli 2023, platform penipuan milik Outsider Enterprise telah memfasilitasi pencurian sedikitnya 3,87 juta kartu kredit, dengan taksiran kerugian global mencapai 1,9 miliar dolar AS.

Modus Operandi Layanan Phishing Instan

Dalam berkas gugatannya, Google memaparkan bukti-bukti mengenai sistem kerja [Outsider Enterprise](#) yang dikelola oleh para pelaku kriminal di luar negeri. Kelompok ini membangun dan menyewakan perangkat lunak penipuan instan (phishing-for-dummies) bernama “Outsider” dengan tarif 88 dolar AS per minggu atau 200 dolar AS per bulan.

Layanan berbasis langganan ini memungkinkan pelaku kejahatan siber bahkan yang tidak memiliki keahlian teknis sekalipun untuk membuat replika situs web palsu dalam hitungan menit. Situs tiruan tersebut meniru tampilan penyedia telekomunikasi, lembaga keuangan, badan pemerintah, hingga platform belanja online terkemuka.

Secara ironis, pembuatan kode pemrograman jahat dan situs web palsu tersebut dibantu oleh teknologi AI generatif, termasuk model AI milik Google sendiri, Gemini.

Untuk memikat korban masuk ke dalam perangkap, para pelaku saling bekerja sama melalui saluran Telegram terbuka untuk menyebarkan tautan jahat lewat SMS penipuan massal. Data kartu kredit dan kode verifikasi (multi-factor authentication) yang dimasukkan korban pada situs palsu tersebut akan terkirim secara langsung (real time) ke dasbor penipu melalui platform Outsider.

Penggunaan Infrastruktur Google untuk

Kejahatan

Analisis internal Google menunjukkan bahwa sepanjang pertengahan November 2025 hingga April 2026 saja, sistem deteksi perusahaan mendeteksi lebih dari 1,59 juta tautan (URL) aktif yang terafiliasi dengan infrastruktur Outsider. Kelompok kriminal ini juga memanfaatkan infrastruktur penyimpanan komputasi awan seperti Google Drive dan Google Cloud secara ilegal untuk meng-host situs-situs phishing tersebut.

Guna menekan ruang gerak sindikat ini, Google menjalin kolaborasi erat dengan operator telekomunikasi besar di AS (seperti AT&T, T-Mobile, dan Verizon) untuk memblokir lalu lintas SMS penipuan. Google juga berkoordinasi dengan FBI dan Lumen's Black Lotus Labs untuk menyita domain web ilegal serta akun-akun toko daring yang digunakan untuk menguji layanan phishing tersebut.

Melalui gugatan hukum ini, Google menuntut ganti rugi kompensasi dan hukuman finansial bagi para pelaku, serta meminta pengadilan mengeluarkan perintah pemblokiran permanen terhadap aktivitas sindikat Outsider Enterprise. Langkah ini sejalan dengan strategi pertahanan siber Google yang mengandalkan teknologi "AI melawan AI" untuk mendeteksi dan memblokir lebih dari 10 miliar pesan penipuan setiap bulannya.