Peretas China Incar Microsoft

EXPOSEMEDIA - Microsoft melaporkan sebuah kelompok peretas yang didukung pemerintah China telah meretas kotak masuk email dari jarak jauh menggunakan kelemahan yang baru ditemukan dalam perangkat lunak server email Microsoft.

Melansir Reuters, kelompok peretas China itu bernama HAFNIUM. Microsoft menyatakan kelompok itu yang merupakan entitas yang disponsori negara yang beroperasi di luar China.

Dalam sebuah posting blog, Microsoft mengatakan aksi peretasan memanfaatkan empat kerentanan yang sebelumnya tidak terdeteksi dalam berbagai versi perangkat lunak.

Dalam posting blog terpisah, perusahaan keamanan dunia maya Volexity mengatakan bahwa Microsoft telah melihat para peretas menggunakan salah satu kerentanan untuk mencuri konten dari beberapa kotak surat pengguna dari jarak jauh pada bulan Januari.

Dalam aksi sebelumnya, HAFNIUM hanya mampu mengetahui detail server Exchange dan akun yang ingin mereka rampok.

Juru bicara kementerian luar negeri China Wang Wenbin membatan semua tudingan yang mengaitkan HAFNIUM dengan pemerintah China.

"China ingin media dan perusahaan yang relevan mengambil sikap profesional dan bertanggung jawab, dan mendasarkan karakterisasi serangan dunia maya pada banyak bukti, daripada dugaan dan tuduhan yang tidak berdasar," katanya.

Saat ini, langkah agresif para peretas telah menarik perhatian di seluruh komunitas keamanan siber. Mike McLellan, direktur intelijen untuk Dell Technologies Inc's Secureworks mengatakan telah melihat lonjakan tiba-tiba dalam aktivitas yang menyentuh server Exchange pada hari Minggu.

Rangkaian produk Microsoft diketahui telah diawasi sejak peretasan SolarWinds, perusahaan perangkat lunak yang menangani seluruh gangguan sistem di seluruh pemerintah dan sektor swasta.

Dalam kasus lain, peretas memanfaatkan cara pelanggan menyiapkan layanan Microsoft mereka untuk membahayakan target mereka atau menyelami lebih jauh ke dalam jaringan yang terpengaruh.

Peretas SolarWinds juga membobol Microsoft sendiri, mengakses dan mengunduh kode sumber, termasuk elemen Exchange, email perusahaan, dan produk kalender.

McLellan mengatakan aktivitas peretasan yang dia lihat saat ini tampak terfokus pada penyemaian perangkat lunak berbahaya dan menyiapkan panggung untuk gangguan yang berpotensi lebih dalam daripada langsung pindah ke jaringan secara agresif.

"Kami belum melihat ada kegiatan lanjutan. Kami akan menemukan banyak perusahaan yang terkena dampak tetapi sejumlah kecil perusahaan benar-benar dieksploitasi," ujar McLellan.

Microsoft mengatakan target peretasan adalah peneliti penyakit menular, firma hukum, lembaga pendidikan tinggi, kontraktor pertahanan, lembaga pemikir kebijakan, hingga kelompok non-pemerintah. **(cnni/*)**