Buletin Bulanan Keamanan Komputer

Penipuan Terfokus

Sekilas

Kriminalis siber selalu punya cara baru dan kreatif dalam melakukan operasinya. Salah satu jenis scam/penipuan yang mulai banyak dipakai adalah jenis penipuan terfokus. Kriminalis siber mencari atau membeli informasi ribuan orang dan menggunakannya untuk melakukan serangan secara individu. Dibawah ini, akan diterangkan bagaimana sebuah proses penipuan dilakukan beserta beberapa contoh. Semakin Anda tahu seluk beluk hal ini, akan lebih mudah bagi Anda untuk mengenalinya dan kemudian menghentikannya.

Bagaimana Caranya?

Penipuan menggunakan surel dan percakapan telepon sudah sering terjadi, cara ini dipakai selama bertahun-tahun. Apakah masih ingat surel "Anda Menang Undian" atau cerita seputar Pangeran Nigeria (dengan harta warisan). Cara penipuan tradisional ini, tidak memiliki sasaran terfokus. Kriminalis siber cuma membuat sebuah pesan dan menyebarkannya ke jutaan orang. Karena cara ini bersifat umum, tentu jadi mudah dikenali. Penipuan terfokus sedikit berbeda, kriminalis siber melakukan penelitian terlebih dahulu dan membuat pesan khusus bagi calon korban secara spesifik. Mereka mencari atau membeli basis data (database) nama orang, sandi, nomer telpon dan rincian lainnya. Semua informasi ini bisa bersumber dari situs web yang dibobol dll. Informasi itu umumnya juga ada di media sosial dan catatan publik pemerintahan. Berdasar semua informasi tersebut, pelaku memilih sasarannya.

Satu trik pelaku kriminal ini adalah menimbulkan rasa takut atau melakukan pemerasan supaya Anda memberikan uang. Berikut ini sekilas cara kerja penipuan itu. Pelaku penipuan mencari atau membeli informasi akun dan sandi dari web yang diretas. Mereka menemukan akun Anda (dan orang lain) dan mengirimkan surel berisi informasi pribadi, termasuk juga sandi yang Anda gunakan di situs web tersebut. Mereka mengatakan bahwa terungkapnya sandi Anda adalah "bukti" bahwa peralatan komputer atau gawai Anda sudah diretas, padahal ini tidak benar. Kemudian mereka akan bilang, selama proses peretasan, mereka mendapati bukti bahwa Anda mengakses situs pornografi daring (online). Selanjutnya, di bagian akhir surel, mereka mengancam mengungkap temuan itu ke keluarga dan rekan, bila Anda tidak membayar sejumlah uang.

Sebenarnya, dihampir semua kasus, kriminalis siber tidak pernah meretas sistem Anda. Mereka bahkan tidak mengenal Anda dan situs web apa saja yang dikunjungi. Mereka secara kreatif menggunakan secuplik informasi mengenai korbannya guna menciptakan rasa takut seputar peretasan komputer atau gawai dan mengecoh seseorang untuk menyetorkan sejumlah dana. Ingat, cara ini bisa digunakan via percakapan telepon.

Rencana Aksi

Kenali bahawa surel dan telepon seperti diatas adalah upaya penipuan. Tentu mengkhawatirkan juga bila data pribadi Anda diketahui orang lain, namun jangan lupa bahwa si pengirim hanya berpura-pura. Cara ini merupakan bagian dari proses penyebaran otomatis secara masif. Di jaman ini, semakin mudah bagi kriminalis siber mencari atau membeli informasi pribadi, jadi jangan heran kalau di masa depan akan lebih banyak model penipuan seperti itu. Beberapa hal untuk diperhatikan:

⚠

- **Waspada bila menerima surel, pesan atau telepon bernuansa terburu-buru. Manipulasi emosi seperti perasaan takut dan terburu-buru merupakan upaya agar Anda berlaku sembrono dan melakukan kesalahan.**
- **Bila seseorang menginginkan pembayaran lewat Bitcoin, voucher atau metode pembayaran unik dan sulit dilacak.**
- **Bila mendapatkan surel mencurigakan, coba gunakan Google untuk mencari tahu apakah ada orang lain juga mengalami hal yang sama.**

Pada akhirnya, akal sehat adalah perlindungan terbaik. Sangat disarankan menggunakan sandi cukup panjang dan unik di setiap akun daring. Tidak hafal semua sandi? Gunakan pengelola sandi. Bila mungkin, aktifkan metode verifikasi dua tahap.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Editor Tamu

Lenny Zeltser *berpengalaman dibidang keamanan siber. Mengembangkan solusi anti malware di Minerva Lab dan instruktur keamanan data di SANS Institute. Pengalamannya mencakup layanan dan konsultan keamanan data. Simak kiprahnya di zeltser.com/blog dan di Twitter @lennyzeltser.*

Sumber Pustaka

Rekayasa Sosial:	https://www.sans.org/u/MUU
Stop Pengelabuan:	https://www.sans.org/u/MUZ
Informasi Diri di Internet:	https://www.sans.org/u/MV4
Pengelola Sandi:	https://www.sans.org/u/MV9