SANS SECURITY AWARENESS

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

Menangkal Malware

Sekilas

Mungkin Anda tidak asing dengan istilah virus, Trojan, ransomware atau rootkit dalam perbincangan seputar keamanan siber. Semua itu adalah ragam program malware, yang digunakan kriminalis siber meretas komputer dan peralatan. Sekali terpasang, mereka bisa melakukan apa saja. Kenalilah malware, bahaya apa yang mungkin terjadi dan juga hal penting apa yang bisa dilakukan sebagai langkah perlindungan.

Mengenal Malware

Gampangnya, malware adalah perangkat lunak, sebuah program komputer, yang dipakai untuk melakukan tindak kejahatan. Istilah malware merupakan gabungan kata malicious (jahat/berbahaya) dan software (perangkat lunak). Kriminalis siber memasang malware di komputer atau peralatan Anda supaya dapat mengendalikannya. Sekali terpasang, malware memungkinkan orang lain mengintai aktifitas daring (online) Anda, mencuri sandi atau berkas, atau bahkan menggunakan sistem Anda untuk menyerang orang lain. Malware bahkan bisa merampas kontrol berkas Anda, meminta tebusan sebelum mengembalikannya. Sebagian orang beranggapan, malware hanya ada di komputer berbasis Windows. Padahal, malware bisa menular ke semua peralatan, dari komputer Mac, gawas, hingga perekam digital dan kamera sekuriti. Bagi pelaku kejahatan siber, semakin banyak komputer dan peralatan yang terinfeksi, semakin banyak uang bisa dipanen. Jadi setiap orang adalah sasaran, termasuk Anda.

Lindungi Diri – Hentikan Malware

Anda mungkin berpendapat bahwa ini hanyalah sekedar memasang program keamanan seperti perangkat lunak anti virus dan otomatis Anda terhindar dari hal tersebut. Kenyataannya, anti-virus tidak sanggup menangkal semua malware. Kriminalis siber selalu mengembangkan malware canggih baru yang bisa menghindar deteksi. Dilain pihak, pembuat anti-virus secara berkala juga meningkatkan kemampuan penelusuran malware. Jadi keduanya berlomba terus, namun pihak yang jahat biasanya setapak lebih maju. Oleh karena Anda tidak bisa hanya bergantung pada anti-virus saja, berikut ini adalah beberapa kiat langkah perlindungan:

Kriminalis siber sering menginfeksi komputer atau peralatan dengan cara memanfaatkan kelemahan perangkat lunak. Penggunaan perangkat lunak versi terbaru semakin sedikit titik lemahnya, ini mempersulit kriminalis siber mengutak-utiknya. Pastikan sistem operasi, aplikasi, browser & pelengkapnya dan peralatan selalu terperbarui dan menggunakan versi terakhir. Gunakan fitur pembaruan otomatis untuk mempermudah prosesnya.

Kriminalis siber umumnya meretas komputer atau alkom/gawas dengan cara menciptakan program komputer atau aplikasi palsu, mengunggahnya ke internet dan kemudian dengan segala upaya berusaha memperdaya Anda agar mengunduh dan menggunakannya. Oleh karena itu, unduh dan gunakan program atau aplikasi dari sumber daring terpercaya. Tambahan lagi, hindari penggunaan aplikasi baru, dengan sedikit ulasan positif, jarang diperbaharui atau jarang diunduh pengguna. Bila ada program komputer atau aplikasi yang tidak terpakai, hapus saja.

Pelaku kejahatan sering memperdaya orang supaya menggunakan malware bikinan mereka. Contohnya, mereka mengirimkan surel aspal (asli tapi palsu) dan berisi lampiran atau tautan (link). Bisa saja surel itu tampak berasal dari bank atau teman. Pada saat Anda membuka lampiran atau klik tautan, tindakan itu akan mengaktifkan proses instalasi malware ke dalam sistem Anda. Bila sebuah pesan menghadirkan suasana tergesa-gesa, terlalu berlebihan/ mengada-ada isinya, bisa jadi itu adalah sebuah upaya pengelabuan. Waspada, gunakan akal sehat Anda.

Secara berkala lakukan backup sistem dan file ke cloud. Atau simpan backup ke tempat lain yang terpisah dari sistem Anda. Ini akan memberikan perlindungan pada saat malware berupaya mengenkripsi atau menghapusnya. Backup adalah penting, terkadang ini hanya satu-satunya cara untuk bisa pulih dari serangan malware.

Mau tidak mau, cara paling ampuh menangkal malware adalah dengan memastikan semua perangkat lunak dan peralatan selalu terperbarui, menggunakan anti-virus dari sumber terpercaya dan waspada terhadap segala upaya pengelabuan. Bila semua itu gagal, backup adalah cara solusi terakhir.

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 *memerangi malware dengan cara menciptakan produk keamanan di Minerva Labs sekaligus mengajar di SANS Institute. Lenny aktif di Twitter sebagai @lennyzelter dan penulis blog keamanan di zeltser.com.*

Sumber Pustaka

Ransomware: https://www.sans.org/u/EdI

Backups: https://www.sans.org/u/EdN

Stop That Phish: https://www.sans.org/u/EdS