Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Mengenal Malware

Sekilas

Anda mungkin pernah mendengar istilah virus, trojan, ransomware dan rootkit dalam perbincangan keamanan dunia siber. Semua sebutan itu merujuk pada satu hal yaitu aneka program yang dipakai untuk meretas/membobol komputer dan peralatan lainnya. Istilah lain yang lazim dipakai adalah malware. Dalam edisi kali ini akan diterangkan apa itu malware, siapa penciptanya, apa tujuan membuat malware dan yang paling penting, bagaimana Anda bisa terhindar dari hal tersebut.

Editor Tamu

Lenny Zeltser berfokus pada perlindungan operasi IT pelanggan di NCR Corp serta pengajar penangkal malware di SANSInstitute. Lenny hadir di Twitter sebagai **@lennyzeltser** dan menerbitkan securityblog di **zeltser.com**.

Apa Itu Malware?

Gampangnya, malware adalah sebuah perangkat lunak, program komputer, yang digunakan untuk tujuan tidak baik/jahat. Perlu diketahui, istilah malware lahir dari kombinasi kata malicious (tidak baik/jahat) dan software (perangkat lunak). Kriminalis siber menanamkan malware ke sebuah komputer atau peralatan untuk mendapatkan kendali atau akses terhadap apa yang diinginkan. Sekali terpasang, malware tersebut bisa digunakan untuk memata-matai kegiatan online Anda, meretas sandi atau berkas dan juga memanfaatkan komputer Anda untuk menyerang komputer lain. Malware bahkan bisa memblokir akses ke berkas milik Anda sendiri dan meminta tebusan sebelum memberikan akses ke berkas tersebut..

Banyak orang beranggapan bahwa masalah malware hanya ada di komputer berbasis Windows. Memang Windows banyak digunakan sehingga menjadi sasaran utama, namun ternyata malware juga merambah beragam peralatan lain termasuk komputer Mac, alkom (smartphone) dan tablet. Semakin banyak komputer dan peralatan yang tertular malware, para pelaku akan semakin banyak mendapat keuntungan. Jadi ingat, setiap orang merupakan sasaran/target, termasuk Anda.

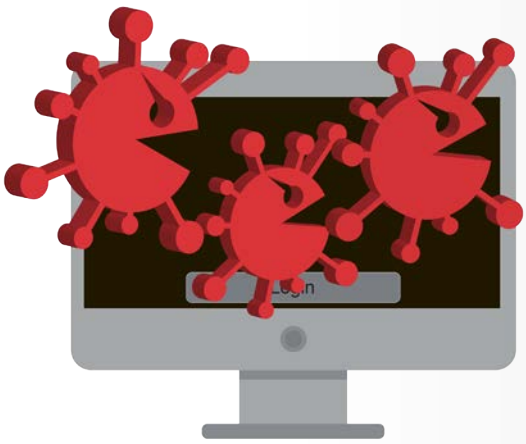
Siapa Pencipta Malware?

Malware tidak lagi dibuat ala kadarnya oleh orang iseng atau peretas amatir, namun dilakukan oleh kriminalis siber profesional. Tujuannya adalah meraup keuntungan dari komputer atau peralatan yang tertular, mungkin dengan cara menjual data yang dicuri, mengirimkan surel spam, melakukan serangan DOS (denial of service) atau melakukan pemerasan. Pihak yang

© SANS Institute 2016

Mengenal Malware

menciptakan, menyebarkan dan mendapatkan keuntungan dari malware bisa bervariasi, mulai dari perorangan hingga kelompok kriminal terorganisir bahkan bisa juga organisasi pemerintahan. Orang yang menciptakan malware canggih ini berkarya dengan sangat terarah, bekerja khusus untuk membuat malware. Selain itu, sekali berhasil menciptakan malware, mereka tidak jarang menjualnya ke individu atau organisasi dan malahan para 'pelanggannya' akan mendapatkan program pembaruan dan layanan purna jual.



Tangkal malware dengan waspada terhadap surel yang mencurigakan, upayakan selalu memperbarui peralatan dan menggunakan anti-virus terbaru.

Perlindungan Terhadap Malware

Tindakan yang sering dilakukan guna menangkal serangan malware adalah dengan memasang anti-virus dari penjual terpercaya. Perangkat lunak ini dikenal pula sebagai anti-malware, dirancang untuk mendeteksi sekaligus membungkam malware. Namun ingat, anti-virus tidak bisa menghadang dan memusnahkan semua malware. Kriminalis siber selalu berinovasi, terus melahirkan malware baru serta canggih yang semakin susah dilacak keberadaannya. Disisi lain, produsen anti-virus juga tidak mau kalah, selalu memperbarui produknya dengan berbagai kemampuan baru untuk mendeteksi malware. Terkadang ini seperti adu cepat, berlomba-lomba untuk lebih unggul dari lawannya. Sayangnya, pelaku kejahatan biasanya setapak lebih maju. Jadi, anti-virus tidak bisa diandalkan sepenuhnya, lakukan beberapa hal dibawah untuk memperkokoh perlindungan Anda.

- Penularan ke komputer atau peralatan sering memanfaatkan titik lemah perangkat lunak. Perangkat lunak versi terbaru akan semakin sedikit titik lemahnya dan bertambah susah untuk diretas. Jadi, pastikan sistem operasi, aplikasi dan peralatan melakukan pembaruan secara otomatis.
- Cara yang lazim dilakukan untuk meretas alkom adalah dengan menciptakan aplikasi alkom palsu, mengunggahnya ke internet dan memperdaya orang agar mengunduh sekaligus menggunakannya. Oleh karena itu, unduh dan pasang aplikasi dari sumber online terpercaya. Selain itu, gunakan aplikasi mobile yang telah diunggah cukup lama, diunduh banyak orang dan mendapatkan banyak ulasan positif.
- Di komputer, gunakan akun standar dengan hak yang terbatas (limited privilege) sebagai ganti akun "Administrator" atau "root". Ini merupakan proteksi tambahan agar malware tidak bisa dengan otomatis terpasang.
- Kriminalis Siber akan menggunakan segala tipu daya agar orang mau menginstall malware. Contohnya adalah dengan mengirim surel yang tampak asli dilengkapi dengan lampiran atau tautan (link). Bisa saja surel direkayasasehingga nampak berasal dari bank atau teman. Pada saat lampiran itu dibuka atau klik ke tautan

Mengenal Malware

yang ada, program tertentu akan dijalankan dan menanamkan malware ke dalam sistem. Bila sebuah pesan/surel menciptakan suasana tergesa-gesa, membingungkan atau isinya terlalu berlebihan/mengada-ada, bisa jadi itu merupakan sebuah upaya serangan. Waspadalah, gunakan akal sehat Anda.

- Lakukan backup sistem dan berkas secara rutin ke sistem cloud atau simpan backup di piranti yang tidak tersambung ke komputer seperti external drive. Ini akan melindungi backup tersebut saat malware berusaha mengenkripsi atau menghapusnya. Backup sangatlah penting, terkadang ini merupakan satu-satunya cara penyelamatan dari penularan malware.

Sudah barang tentu, cara terbaik menangkal malware ialah dengan memastikan perangkat lunak selalu diperbarui , menggunakan perangkat lunak anti-virus dari sumber terpercaya sekaligus waspada terhadap siapapun yang mencoba memperdaya Anda dalam upaya penularan malware.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi http://www.securingthehuman.org.

Versi Bahasa Indonesia

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

Sumber Pustaka

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Rekayasa Sosial:	https://securingthehuman.sans.org/ouch/2014#november2014
Aman menggunakan Aplikasi Alkom:	https://securingthehuman.sans.org/ouch/2015#january2015
Mengamankan Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup dan Recovery:	https://securingthehuman.sans.org/ouch/2015#august2015

OUCH! diterbitkan oleh SANS “Securing The Human” dan didistribusikan sesuai lisensi Creative Commons BY-NC-ND 4.0. Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan pengubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi ouch@securingthehuman.org.

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Diterjemahkan oleh: T. Gunawan