OUCH! | Februari 2014

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- Apa itu Malware
- Siapa dan Kenapa
- Pelindungan Anda

Mengenal Malware

Sekilas

Anda mungkin pernah mendengar istilah seperti virus, worm, trojan atau rootkit pada saat orang membicarakan keamanan siber. Berbagai istilah ini merupakan ragam program yang dipakai kriminalis siber (cyber criminal) untuk menginfeksi dan mengendalikan komputer & peralatan komunikasi. Sekarang, semua istilah ini disederhanakan menjadi malware. Di dalam buletin ini, akan dibahas apa itu malware, siapa pembuatnya, kenapa dibuat dan langkah pengamanan yang bisa dilakukan terhadap malware.

Editor Tamu

Lenny Zeltser fokus pada perlindungan kegiatan IT pelanggan di NCR Corp dan Pengajar pemberantasan malware di SANS Institute. Lenny aktif di Twitter **@lennyzeltser** dan menulis blog keamanan **blog.zeltzer.com**.

Apa Itu Malware

Gampangnya, malware adalah suatu perangkat lunak, sebuah program komputer yang digunakan untuk melakukan tindakan merugikan. Sebenarnya, sebutan malware itu sendiri berasal dari kombinasi kata “malicious” dan “software”. Tujuan akhir dari kriminalis siber adalah menanamkan malware ke dalam komputer atau piranti komunikasi. Sekali terpasang, para pelaku berpotensi mendapatkan kendali pada semua peralatan tersebut. Banyak orang berpikir keliru bahwa malware hanya merupakan persoalan pada komputer berbasis Windows. Karena Windows banyak dipakai, tentu menjadi sasaran utama, namun sebenarnya malware bisa menginfeksi semua jenis komputer, termasuk smartphone dan tablet. Bahkan, tingkat serangan perangkat lunak merugikan ini pada perangkat komunikasi justru meningkat pesat. Tambahan lagi, perlu diingat bahwa setiap orang adalah sasaran, termasuk Anda. Semakin banyak komputer dan piranti komunikasi terinfeksi, semakin banyak keuntungan yang bisa diraih oleh kriminalis siber. Mereka acap kali juga tidak peduli siapa yang terimbas karena tujuannya adalah menginfeksi sebanyak mungkin.

Siapa dan Kenapa

Malware tidak lagi digarap oleh sembarang orang atau peretas amatir, namun dilakukan oleh para kriminalis siber canggih dengan maksud tertentu. Tujuan ini diantaranya adalah mencuri data rahasia, mendapatkan data login dan sandi (password), mengirimkan surel spam, melakukan serangan DOS (Denial of Service), pemerasan dan pencurian data pribadi. Sebagai contoh, malware Cryptolocker digunakan untuk menginfeksi dan mengenkripsi berkas (file) didalam komputer Anda. Setelah komputer Anda terinfeksi dan semua berkas tidak bisa diakses, mereka akan meminta sejumlah tebusan untuk bisa “memulihkan” komputer Anda.

Pembuat, penyebar dan peraih keuntungan dari malware bisa saja seseorang bertindak atas nama pribadi,

Mengenal Malware

kelompok kriminalis atau organisasi pemerintahan. Tambahan lagi, pembuatan malware canggih dilakukan oleh seorang spesilis sebagai pekerjaan tetap (bukan iseng/sambilan). Saat sebuah malware selesai dibuat, sering kali dijual ke pihak atau organisasi lain, dilakukan penyempurnaan berkala dan dilengkapi layanan purna jual kepelanggannya. Sekali dibeli, kriminalis siber bisa meraup keuntungan dengan cara memasang malware ke dalam jutaan perangkat tanpa diketahui dan dicurigai pemiliknya, sehingga akhirnya terbentuk "Botnet" (jaringan komputer yang sudah terinfeksi malware). Botnet ini menjadi pasukan garis depan dengan kendali jarak jauh yang bisa digunakan untuk beragam keperluan atau diperjual-belikan ke kriminalis siber lain.

Cara terbaik perlindungan terhadap malware adalah dengan memastikan peralatan senantiasa diperbarui, bila mungkin gunakan anti-virus terbaru dan selalu waspada terhadap segala macam serangan.

Perlindungan Anda

Langkah umum dalam melindungi komputer dan piranti komunikasi terhadap malware adalah dengan menggunakan software anti-virus dari sumber terpercaya. Anti-virus atau sering pula disebut sebagai anti-malware, adalah sebuah perangkat lunak yang dirancang untuk menemukan dan menghentikan kerja perangkat lunak berbahaya. Namun, anti-virus tidak bisa menghentikan kerja atau menghilangkan semua malware. Penyerang siber selalu berinovasi dan mengembangkan serangan canggih baru yang sanggup menyiasati kerja anti-virus. Disisi lain, pengembang anti-virus juga senantiasa menyempurnakan produknya untuk menghadapi malware baru. Keduanya berlomba-lomba agar bisa setapak lebih maju dari yang lain. Namun dalam persaingan ini, kriminalis siber lebih sering unggul. Jadi, walaupun anti-virus bisa menemukan dan menghentikan kerja beragam malware, pasti akan selalu ada malware versi baru yang terlewatkan. Oleh sebab itu, Anda tidak bisa hanya bergantung pada anti-virus. Diperlukan upaya tambahan dalam langkah perlindungan Anda.

Pertama, pastikan semua operating system dan program aplikasi bisa menginstal pembaruan keamanan (security update) secara otomatis. Semakin baru versi perangkat lunak yang dipakai, akan semakin sulit bagi kriminalis siber untuk menembus komputer dan piranti komunikasi Anda.

Kedua, ingat bahwa Anda adalah perlindungan terbaik melawan malware. Infeksi malware acap kali menggunakan teknik rekayasa sosial (social engineering), yang pada dasarnya adalah jurus tipu daya agar Anda tergerak melakukan pemasangan malware. Salah satu cara adalah dengan melakukan "Phishing", sebuah surel yang tampak asli namun sebenarnya palsu, bertujuan untuk memperdaya Anda sehingga peralatan menjadi tertular. Sebagai contoh: seorang kriminal siber mengirimkan sebuah surel, seakan-akan berasal dari sebuah bank dan Anda diminta click sebuah tautan (link). Jika tautan tersebut diakses, Anda akan dibawa kesebuah website yang otomatis berusaha meretas

Mengenal Malware

dan menginfeksi komputer. Bisa pula mereka mengirimkan surel yang berisi pemberitahuan kegagalan pengiriman barang dan Anda diminta membuka lampiran dokumen yang isinya akan menginfeksi komputer pada saat dibuka.

Upaya Rekayasa sosial juga terjadi pada teknologi lain seperti telepon. Sebagai contoh, seorang peretas menelpon Anda, berpura-pura sebagai Dukungan Teknis Microsoft dan menyatakan bahwa komputer Anda terinfeksi. Itu hanyalah rekaan saja, komputer Anda bisa jadi baik baik saja. Tujuan upaya itu adalah membuat Anda yakin sudah terinfeksi dan akhirnya memperdaya Anda untuk memberikan akses jarak jauh (remote access) ke komputer atau membeli perangkat lunak keamanan komputer yang tidak lain adalah malware. Gunakan akal sehat. Jika telepon atau sebuah pesan terkesan mencurigakan, hindari atau abaikan saja.

Pada akhirnya, cara terbaik perlindungan terhadap malware adalah dengan memastikan selalu menggunakan perangkat lunak versi terbaru, menggunakan antivirus terpercaya dari sumber yang dikenal baik serta waspada terhadap beragam usaha untuk memperdaya Anda dalam upaya membuat komputer Anda terinfeksi.

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

OUCH Phishing:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH Securing Your Computer:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

You Are the Target Poster:
http://www.securingthehuman.org/resources/posters

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