Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Saya diretas, selanjutnya bagaimana?

Sekilas

Kami tahu Anda bermaksud untuk melindungi komputer dan informasi serta melakukan beragam tindakan untuk itu. Seperti halnya mengendarai mobil, bagaimanapun Anda berkendara dengan hati-hati, suatu saat bisa saja terjadi kecelakaan. Buletin ini akan menjelaskan apa yang perlu diperhatikan untuk mengetahui bahwa komputer Anda diretas serta tindakan apa yang bisa dikerjakan. Ketahuilah, semakin cepat dilakukan deteksi dan tindakan terhadap peretasan komputer, Anda akan lebih terhindar dari dampak merugikan.

Editor Tamu

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) adalah Pimpinan Peneliti di CSRgroup Computer Security Consultants. Jake merupakan salah satu penulis materi pelatihan Memory Forensics (FOR526) dan Malware Reverse Engineering (FOR610) di SANS.

Gejala Peretasan

Pertama, perlu diketahui bahwa seringkali tidaklah gampang untuk menentukan apakah sebuah komputer diretas. Biasanya melibatkan beberapa indikator. Jika Anda mengenali kombinasi beberapa gejala dibawah ini, berarti komputer Anda diretas. Simak beberapa contoh dibawah ini:

- Program anti-virus memberikan peringatan bahwa komputer Anda terinfeksi virus, khususnya bila muncul pesan yang menyatakan bahwa berkas (file) yang terinfeksi tidak bisa dihapus atau dikarantina.
- Browser Anda tiba-tiba berubah atau menampilkan website yang tidak pernah Anda inginkan.
- Tiba-tiba di komputer Anda muncul beberapa akun baru walaupun Anda tidak pernah menciptakan akun tersebut
- Program tidak dikenal mendadak aktif walaupun Anda tidak melakukan instalasi/pemasangan
- Komputer berkali-kali gagal fungsi (crash) atau bekerja dengan sangat lambat.
- Program di komputer meminta otorisasi Anda untuk melakukan perubahan ke dalam sistem walaupun Anda tidak melakukan instalasi atau perubahan pada program aplikasi.
- Firewall mengingatkan Anda akan adanya sebuah program tidak dikenal yang berusaha mengakses internet.

Saya diretas, selanjutnya bagaimana?

Tindakan

Jika komputer Anda diretas, cepat bertindak akan lebih baik. Seandainya Anda menggunakan komputer milik organisasi/perusahaan untuk bekerja, disarankan untuk tidak berupaya memperbaiki komputer tersebut secara mandiri dan juga jangan mematikan komputer tersebut. Hal ini bisa memperumit keadaan sekaligus merusak bukti-bukti yang bisa dipakai dalam proses penelusuran dan penyelidikan. Sebagai gantinya, laporkan secepatnya ke pihak management, melalui help desk, team keamanan atau atasan Anda. Jika pelaporan tersebut tidak bisa dilakukan, atau mungkin prosesnya tidak bisa cepat, putuskan sambungan ke jaringan komputer dan biarkan komputer tersebut dalam kondisi “sleep”, “suspend” atau “hybernate”. Bahkan jika Anda masih ragu apakah benar terjadi peretasan, melakukan pelaporan adalah hal terbaik. Organisasi/perusahaan biasanya memiliki prosedur dan tim khusus untuk menangani hal tersebut.

Cepat atau lambat, komputer Anda mungkin diretas, sedini mungkin lakukan deteksi dan tindakan.

Untuk komputer pribadi, berikut ini beberapa langkah yang bisa dilakukan:

- **Backup**. Langkah terpenting adalah selalu waspada dengan siap sedia dengan backup. Lakukan backup data secara berkala dan secara periodik periksa bahwa berkas (file) yang sudah dibackup bisa direstore kembali dengan benar. Sering kali jika sebuah komputer diretas, pilihan terbaik pemulihannya adalah dengan melakukan penghapusan total isi harddisk dilanjutkan dengan instalasi sistem operasi mulai dari awal. Pilihan lain adalah dengan membeli komputer baru. Apapun pilihannya, keduanya membutuhkan berkas backup agar Anda bisa mendapatkan kembali semua data.
- **Ganti Sandi**: Ganti total sandi Anda. Tidak hanya sandi di komputer dan peralatan komunikasi, namun juga semua sandi aplikasi online (di internet) . Lakukan penggantian sandi aplikasi online dengan menggunakan komputer yang aman dan terpercaya.
- **Anti-virus**. Saat program anti-virus menemukan berkas yang tertular virus, ada beberapa pilihan tindak lanjut yakni karantina berkas, pembersihan virus atau menghapus berkas tersebut. Kebanyakan program anti-virus memiliki informasi seluk beluk penularan virus untuk dipelajari. Bila ragu, lakukan karantina berkas yang tertular atau jika hal itu tidak bisa dilakukan, hapus saja berkas tersebut.
- **Instalasi ulang**: Jika program anti-virus gagal membersihkan komputer, cara teraman berikutnya

Saya diretas, selanjutnya bagaimana?

adalah dengan melakukan instalasi ulang dari awal. Lepaskan sambungan ke jaringan dan lakukan proses instalasi ulang sesuai petunjuk dari produsen komputer. Biasanya, instalasi sistem operasi dilakukan dengan menggunakan partisi recovery yang tersedia. Jika partisi ini hilang, rusak atau terinfeksi virus maka perlu digunakan DVD recovery. Jangan melakukan proses instalasi sistem operasi dari berkas backup. Backup tersebut boleh jadi rentan terhadap peretasan. Berkas backup hanya dipakai untuk mendapatkan kembali data milik Anda. Jika komputer tersebut sudah tua atau usang, mungkin lebih sederhana (dan mungkin lebih murah biayanya) jika membeli komputer baru dibanding melakukan proses bongkar pasang.

- **Jasa Profesional**: Bila Anda merasa diretas namun beranggapan tidak memiliki kemahiran dan pengetahuan untuk mengatasinya, mungkin Anda perlu bantuan jasa profesional. Sebagai contoh: setelah diretas, Anda melihat bahwa proses backup menjadi tidak tuntas atau tidak berjalan baik. Anda tergoda untuk memindahkan file penting seperti foto, dokumen dan video ke komputer lain. Namun dengan melakukan hal tersebut, justru akan menyebabkan komputer lain menjadi tertular. Cara paling aman adalah dengan menyerahkan komputer yang terinfeksi kepada teknisi khusus agar proses mendapatkan kembali file penting bisa dilakukan dengan benar dan aman.

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! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! What Is Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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