Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Ransomware

Mengenal Ransomware

Ransomeware adalah sejenis malware yang banyak tersebar di jagat internet, menebar ancaman untuk menghancurkan dokumen atau berbagai berkas milik korbannya. Malware adalah perangkat lunak, sebuah program komputer yang digunakan untuk melakukan aksi kejahatan. Walaupun ransomware hanya merupakan salah satu jenis malware, namun perkembangannya cukup pesat lantaran memberikan banyak keuntungan kepada pelakunya. Sekali ransomware bersemayam di dalam sebuah komputer, berkas-berkas tertentu atau bahkan seluruh hard disk akan di enkripsi. Akibatnya, akses seluruh sistem atau beberapa berkas penting, seperti foto atau dokumen terhenti. Ujung-ujungnya, akan muncul penjelasan rincian tebusan yang harus dibayar bila ingin melakukan dekripsi berkas dan memulihkan seluruh sistem. Sering kali tebusan yang diminta harus dibayar dalam bentuk mata uang digital seperti Bitcoin. Ransomware menyebar seperti halnya malware lainnya. Cara paling umum adalah melalui surel dalam bentuk lampiran. Penerima surel akan diperdaya agar mengunduh lampiran atau mengklik sebuah pranala/tautan tertentu.

Editor Tamu

Lenny Zeltser fokus 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 Harus Dibayar?

Pertanyaan yang susah. Terkadang dengan semakin sering orang membayar tuntutan tebusan, malah memberikan motivasi pelaku untuk mengulang perbuatannya. Dilain pihak, mungkin tidak ada pilihan lain selain membayarnya. Perlu diketahui bahwa dengan membayar tebusanpun, tidak ada jaminan semua berkas akan dikembalikan seperti sedia kala. Dalam berurusan dengan pelaku kriminal, bisa saja berkas tidak di dekripsi atau kalaupun diberikan cara melakukan dekripsi, namun tidak tertutup terjadi kekeliruan dalam proses dekripsi atau malah tertular malware lain.

Siap Siaga

Mungkin cara terbaik terlepas dari ancaman ransomware dan tidak membayar tebusan adalah dengan mendapatkan kembali semua berkas dari backup. Dengan cara ini, bahkan saat terserang ransomware, ada solusi untuk mendapatkan

Ransomware

kembali semua berkas setelah komputer dibersihkan atau di setup ulang. Ingat, bila berkas backup bisa diakses dari sistem yang terinfeksi, ransomware bisa saja menghapus atau mengenkripsi berkas backup.Jadi sangatlah perlu melakukan backup semua berkas penting ke jasa penyimpanan berbasis teknologi cloud atau menyimpan backup di external drive yang tidak selalu tersambung ke sistem. Salah satu kesalahan yang sering terjadi adalah kegagalan membaca berkas yang sudah dibackup. Agar hal ini tidak terjadi, secara berkala pastikan bahwa proses backup berfungsi dengan baik serta berkas bisa dibaca lagi pada saat dibutuhkan. Backup juga sangat berguna untuk mendapatkan kembali berkas yang secara tidak sengaja terhapus atau karena kerusakan media simpan.

Ransomware adalah malware, bila menginfeksi komputer, akan melakukan enkripsi dan mencegah akses ke semua berkas di dalam komputer.

Perlindungan Tambahan

Ambil langkah perlindungan terhadap serangan ransomware seperti halnya menghadapi malware yang lain. Dimulai dengan memastikan anti-virus selalu terperbarui dan didapat dari sumber terpercaya. Perangkat yang biasa dikenal sebagai anti-malware dirancang untuk mengenal dan membungkam malware. Namun ingat, anti-virus tidak bisa menghadang dan memusnahkan semua program berbahaya. Kriminalis siber selalu berinovasi, terus melahirkan malware baru yang mampu berkelit dari segala macam deteksi. 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 sangatlah perlu untuk melakukan backup semua berkas dan memperhatikan hal-hal tambahan dibawah ini sebagai langkah perlindungan:

- Penularan ke komputer atau peralatan sering memanfaatkan kelemahan perangkat lunak. Semakin baru sebuah perangkat lunak, semakin sedikit kelemahannya dan lebih susah untuk diretas. Jadi pastikan sistem operasi, aplikasi dan semua peralatan melakukan proses pembaruan secara otomatis.
- Di komputer, gunakan akun standar dengan hak terbatas (limited privilege) sebagai ganti akun “Administrator” atau “root”. Ini merupakan proteksi tambahan agar malware tidak secara otomatis terpasang.
- Pelaku kejahatan menggunakan beragam tipu daya agar orang mau menginstall malware. Contohnya adalah

Ransomware

dengan mengirim surel yang tampak asli dilengkapi dengan lampiran atau pranala/tautan (link). Bisa saja surel itu direkayasa sehingga tampak berasal dari sebuah bank atau teman. Pada saat lampiran itu dibuka atau melakukan klik ke tautan yang ada, program tertentu akan bekerja secara diam-diam dan menancapkan malware ke dalam sistem. Bila sebuah pesan/surel menciptakan suasana tergesa-gesa, membingungkan, isinya terlalu berlebihan/ mengada-ada atau banyak memiliki kesalahan tata-bahasa, bisa jadi itu merupakan sebuah upaya serangan. Waspadalah, gunakan akal sehat Anda.

Lindungi diri Anda dari ransomware dengan selalu waspada saat membuka lampiran surel atau mengklik sebuah pranala/ tautan, pastikan menggunakan anti-virus versi terbaru, melakukan backup secara berkala serta memastikan berkas backup bisa dibaca ulang.

Selanjutnya

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

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

Mengenal Malware: https://securingthehuman.sans.org/ouch/2016#march2016

Enkripsi: https://securingthehuman.sans.org/ouch/2016#june2016

Backup: https://securingthehuman.sans.org/ouch/2015#august2015

Microsoft Article: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

SANS FOR610 Course - Reverse Engineering Malware: https://sans.org/for610

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