AWAS VIRUS LEWAT EMAIL !!!

Virus kategori **ransomware** sedang marak di dunia IT. Virus ini mengunci layar komputer atau file sampai tak bisa diakses sama sekali, kemudian meminta tebusan dalam bentuk uang kepada korban.

Varian terbaru ransomware adalah **CTB Locker** (Curve-Tor-Bitcoin Locker). Virus ini hanya perlu menginfeksi satu file untuk mengenkripsi ribuan file lain dalam drive komputer korban.

Menurut perusahaan antivirus Eset yang mendeteksi ransomware sejak 2013, **CTB Locker menyebar melalui email yang berisi tautan** ke halaman web atau lampiran bermuatan Trojan yang dikenal dengan nama **Win32/TrojanDownloader.Elenoocka.A.trojan**.

Email biasanya berisi subject yang sangat serius atau menggoda untuk dibuka.

Begitu link diklik, Win32/TrojanDownloader.Elenoocka.A.trojan akan mengunduh varian lain yaitu **Win32/FileCoder.DA**, yang dikenal sebagai CTB Locker tadi, dari server-nya yang ada di tempat lain.

CTB Locker prevalence level-nya mencapai 0,16 persen di antara pengguna komputer bersistem operasi Windows XP, Windows Vista, Windows 7, dan Windows 8 di Indonesia.

File sharing di jaringan LAN di kantor akan dienkrip, bukan terinfeksi

Begitu penguncian file selesai, virus itu akan mengeluarkan pengumuman di layar komputer berupa **screenlock**, yang menyatakan bahwa data di komputer sudah dikunci dan memberikan panduan bagaimana melakukan **pembayaran untuk mendapatkan kunci**.

Kami menyarankan untuk tidak membayar karena tidak ada jaminan setelah dibayar file akan selamat.

Bagaimana ciri file yang sudah terkunci?

Ada tambahan random extension pada extension file yang sebenarnya. Misalnya extension sebenarnya adalah **.jpg**, maka akan ada tambahan jadi **.jpg.gibgkjd**.

Berikut ini tip supaya terhindar atau cara mengantisipasi serangan virus itu:

1. Back-up seluruh folder atau file di komputer secara berkala
2. Pastikan selalu meng-update patch atau hotfix dari Windows
3. Gunakan konfigurasi yang paling optimal pada software antivirus.
4. Tidak mengklik link web atau attachment yang tidak dikenal atau mencurigakan.
5. Pada sistem jaringan, pisahkan komputer atau perangkat yang terkena serangan supaya tidak mem-broadcast serangan ke jaringan.
6. Lakukan indepth scan di komputer yang terserang.

4 tanda yang bisa membantu Anda mengidentifikasi email-email berbahaya.

1. Penggunaan sapaan umum
2. Berisi Tautan Yang Aneh, misal idmsa.apple.com-idmswebauth-classiclogin.htm.artXXia.es/XXXXXXX.
3. Berisi lampiran mencurigakan, berbentuk file bereksistensi htm dan zip
4. Muncul pemberitahuan dari Microsoft Outlook e-mail phising tersebut

Email Phising

Phising yang mempunyai arti dasar yaitu "Memancing" maka bisa di katakan Phising adalah tindakan memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank, nomor kartu kredit seseorang secara tidak sah.

Ciri-ciri email phising sebagian sebagai berikut :

Verify your Account

Kalau verify nya meminta username, password dan data lainnya, jangan memberikan reaksi balik. Namun kalau setelah kita mendaftar account di suatu situs dan harus memverifikasinya dengan mengklik suatu URL tertentu tanpa minta mengirimkan data macam-macam, ya lakukan saja.

If you don't respond within 48 hours, your account will be closed

Harap baca baik-baik dan tidak perlu terburu-buru. Tulisan di atas hanya "propaganda" agar pembaca panik dan tidak berpikir jernih.

Dear Valued Customer

Ini juga hati-hati. Karena e-mail phishing biasanya targetnya itu random, jadi e-mail tersebut bisa menggunakan kata-kata ini. Tapi suatu saat mungkin akan menggunakan nama kita langsung, ini juga harus waspada.

Click the Link Below to gain access to your account

Ada beberapa hacker yang iseng dengan menampilkan masked URL Address atau alamat yang palsu. Walaupun interface webnya nanti sama, tapi kalau diminta registrasi ulang atau mengisi informasi sensitif, itu patut dipertanyakan.

Apabila menemukan e-mail berciri seperti diatas diharap agar anda berhati hati, kalau tidak yakin sebaiknya tidak usah dihiraukan.

WEB DEFACING

Deface jika berdasarkan kamus UMUM mempunyai arti merusakkan, mencemarkan, menggoresi atau menghapuskan.

Tetapi arti kata deface sendiri dalam istilah cyber crime disini yang sangat lekat adalah sebagai salah satu kegiatan merubah tampilan suatu website baik halaman utama atau index filenya ataupun halaman lain yang masih terkait dalam satu url dengan website tersebut (bisa di folder atau di file).

Deface adalah teknik mengganti atau menyisipkan file pada server, teknik ini dapat dilakukan karena terdapat lubang pada security system yang ada di dalam sebuah aplikasi.

Ada beberapa alasan mengapa website mudah di deface:

1. **Penggunaan CMS yang free dan opensource** tanpa adanya modification. Sehingga keseluruhan konfigurasi menggunakan default konfigurasi, hal ini memudahkan para defacer untuk menemukan informasi file, directory, source, database, user, connection, dsb.
2. **Tidak updatenya source** atau tidak menggunakan versi terakhir dari CMS. Hal ini sangat rentan, karena security issue terus berkembang seiring masuknya laporan dan bugtrack terhadap source.
3. **Tidak pernah ada research yang mendalam** dan detail mengenai CMS sebelum digunakan dan diimplementasikan. Sehingga pemahaman dan pengetahuan dari webmaster hanya dari sisi administrasinya saja, tidak sampai ke level pemahaman sourcecode.
4. **Tidak adanya audit trail atau error-log** yang memberikan informasi lengkap mengenai penambahan, pengurangan,

perubahan yang terjadi di website baik source, file, directory, dsb. Sehingga kesulitan untuk menemukan, memperbaiki dan menghapus backdoor yang sudah masuk di website.

5. **Jarang melakukan pengecekan terhadap security update**, jarang mengunjungi dan mengikuti perkembangan yang ada di situs-situs security jagad maya.
6. **Kurangnya security awareness** dari masing-masing personel webmaster & administrator. Sehingga kewaspadaan terhadap celah-celah keamanan cukup minim, kadangkala setelah website terinstall dibiarkan begitu saja. Kurangnya training dan kesadaran akan keamanan website seperti ini akan menjadikan website layaknya sebuah istana yang tak punya benteng.

Disadur dari berbagai sumber yang terpercaya