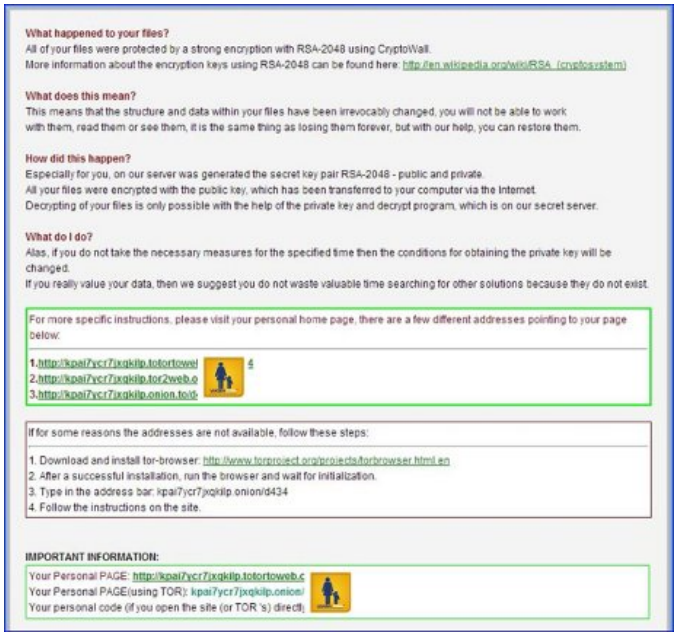
Melindungi Diri Dari Jeratan Cryptolocker cs

Sebenarnya secara teknis ransomware dengan nama Cryptolocker sudah tidak ada lagi karena pembuatnya sudah ditangkap oleh FBI bekerjasama dengan para penegak hukum internasional. Namun kabar buruknya, ibarat seperti bisnis kartel obat bius yang menggiurkan karena memberikan keuntungan sangat besar dimana setiap kali pimpinan kartel berhasil ditangkap oleh pihak yang berwajib.

Maka dalam waktu singkat posisinya akan digantikan oleh orang lain dan membentuk organisasi/kartel baru. Demikian pula dengan ransomware Cryptolocker yang rupanya memberikan keuntungan finansial cukup besar bagi pembuatnya. Tempatnya yang sekarang kosong dan langsung digantikan oleh ransomware lain.
Saat ini ancaman yang paling jelas dan nyata adalah ransomware dengan nama Cryptowall. Dari sisi korbannya bahkan Cryptowall berhasil menginfeksi sekitar 625.000 komputer di seluruh dunia, lebih tinggi 100.000-an komputer dari Cryptolocker dan tidak seperti Cryptolocker yang secara teknis sudah mati, cryptowall sampai saat ini masih aktif mencari korban baru. Cryptowall menyebarkan dirinya melalui lampiran spam email (drive by download) dan instalasi oleh malware lain yang telah menginfeksi komputer terlebih dahulu.



Menurut pantauan Vaksincom, Cryptowall juga sudah sampai di Indonesia dan memakan banyak sekali korban. Kabar buruknya, karena pembuat malwarenya masih belum tertangkap, maka dapat dikatakan tidak ada harapan untuk memecahkan kode enkripsi RSA 2048 yang digunakan untuk mengundi data penting komputer korban yang di infeksinya.

Jika Anda menjadi korban cryptowall dan tidak bersedia membayar tebusan yang memang sangat mahal, belajar dari kssus Cryptolocker, mungkin ada baiknya data yang dienkripsi oleh Cryptowall anda simpan baik-baik sambil berdoa semoga suatu hari nanti pembuatnya tertangkap dan private key untuk dekirpsi data diberikan secara gratis seperti yang terjadi pada cryptolocker. Namun sekali lagi tidak ada yang tahu kapan pembuatnya akan tertangkap dan tidak ada jaminan apakah database private key tersebut tersimpan dengan biak atau malah dimusnahkan oleh pembuatnya.

Menjawab pertanyaan Anda, bagaimana melindungi komputer dari ransomware, salah satunya adalah menggunakan program antivirus yang terpercaya dan mampu mendeteksi varian-varian ransomware yang sangat banyak. Jika anda belum memiliki program antivirus yang handal, Anda bisa mencoba menggunakan G Data Antivirus.

Namun, jika memiliki data penting yang berharga dan penting untuk dilindungi baik berupa data office, foto keluarga, database, pst (data MS Outlook) dan data lainnya yang berpotensi akan mengakibatkan kerugian finansial/kenangan pribadi jika disandera oleh ransomware maka Vaksincom menyarankan Anda untuk melakukan backup data anda secara teratur dan setelah backup jangan dihubungkan ke komputer/jaringan karena ransomware memiliki kemampuan mengunci semua data yang terhubung ke jaringan dan memberikan hak full sharing.

Jika Anda menggunakan cloud storage seperto dropbox, google drive atau Norman Secure Box untuk menyimpan data penting. Pastikan mengaktifkan fitur backup otomatis yang akan selalu menyimpan history/sejarah data yang anda simpan di cloud storage sehingga jika dienkripsi oleh ransomware anda tinggal melakukan restore ke data versi sebelumnya.

source: http://inet.detik.com/read/2014/09/01/141538/2677946/1440/melindungi-diri-dari-jeratan-cryptolocker-cs