MEMULIHKAN FILE YANG DIENKRIPSI VIRUS RANSOMWARE GLOBE (.globe)

PENGANTAR

Alhamdulillah puji syukur kehadirat Allah SWT pemilik segala ilmu yang dengan izin dan ridhoNya.

Terimakasih kepada bang anton hilman atas sudut pandang yang tidak terfikirkan oleh penulis yang merupakan dasar solusi dalam artikel ini. Atas pesan beliau pulalah maka tulisan ini dibuat dengan harapan dapat bermanfaat bagi pengguna lainnya.

Terimakasih kepada tim pengembang emmisoft yang mengizinkan pemakaian softwarenya. Secara pribadi saya berharap dapat berdonasi ke perusahaan anda pada waktu berikutnya.

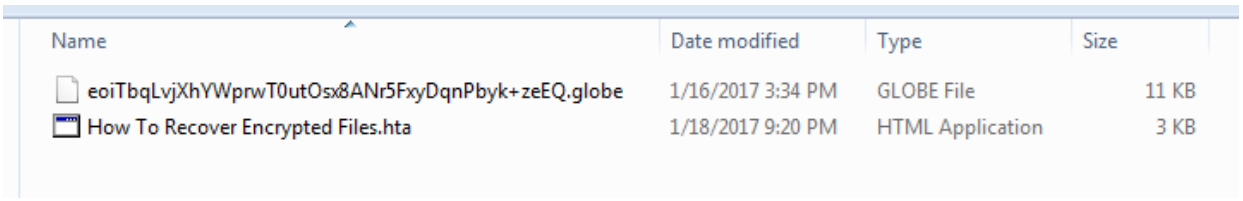
Terimakasih juga kepada senior dan rekan yang berkenan membalas pertanyaan penulis dalam upaya menemukan solusi dalam tulisan singkat ini.

Januari 2017
Penulis

PEMBAHASAN

Beberapa hari lalu, penulis didatangi seorang rekan kerja yang mengaku laptopnya terinfeksi virus. Pelapor mengakui laptopnya diserang virus sejak 2 hari dan seluruh file di drive D tidak bisa diakses.

Setelah pengecekan langsung, penulis melihat ternyata memang seluruh file yang ada di drive D berubah menjadi file type globe (.globe) dengan nama file yang cukup panjang berkarakter acak.



Gambar 1. Sebuah folder yang berisi file bertipe globe

Menurut pengakuan pelapor(rekan kerja penulis), seharusnya folder tersebut berisi sebuah file Microsoft excel dengan nama yang lazim pada berkas-berkas kerja (bukan karakter acak panjang seperti gambar).

Melihat ekstensinya penulis googling untuk mencari informasi tentang virus ini. Berdasarkan informasi yg diperoleh, virus ini dinamakan Ransomware dengan varian Globe, artinya virus Ransomware memiliki jenis atau varian yang lain selain Globe(.globe).

Virus ini berkerja dengan cara mengekripsi file original menjadi file bertipe baru yang tidak bisa diakses. Penyerang melalui suratnya(.hta file) meminta bayaran untuk 1 tools decryptor darinya(penyerang) sebesar **0.5 bitcoin** atau setara dengan sekitar **6 juta rupiah** dengan waktu pembayaran maksimal 1 minggu sebagai langkah solusi bagi korban. Jika dalam 1 minggu korban(pelapor) tidak membayar, penyerang mengancam akan menghapus key tools decryptor untuk memulihkan file laptop korban sehingga tidak bisa dipulihkan selamanya.

Pada titik ini, dari sisi biaya korban(rekan penulis) tidak memiliki biaya dan penulis juga menyarankan tidak tergesa-gesa mengabulkan permintaan penyerang terlebih dahulu karena dana tersebut bisa saja dipergunakan untuk mengembangkan kegiatan merusak lainnya. Hal ini sesuai dengan anjuran kebanyakan pengembang aplikasi keamanan komputer dari masing-masing situs resminya.

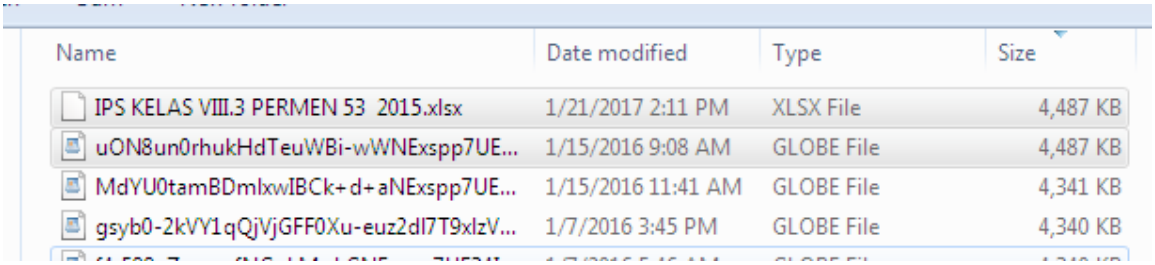
Lanjut…

Setelah virus teridentifikasi, langkah berikutnya adalah mencari solusi untuk memulihkan file. Penulis menemukan 2 tools yang mendukung yaitu emmisoft decryptor for globe dan avast decryptor for globe. Pada tulisan ini penulis memanfaatkan emmisoft decryptor yang diunduh dari situs resminya tanpa biaya (free).

Dan berikut langkah-langkah mendecrypt file yang terinfeksi:

1. Menyalin file original dan tools ke emmisoft decryptor ke satu folder dengan file yang terenkripsi.

   Penjelasan lebih lanjut:
   File original pada harddisk laptop victim memang tidak tersedia. Oleh sebab itu anda harus menyediakan file original dari salah satu file yang terenkripsi agar tools dapat menebak algoritma enkripsi yang digunakan virus dengan benar dan akhirnya dapat menentukan algoritma dekripsi yang nantinya akan digunakan untuk memulihkan file-file lain yang terinfeksi di laptop yang sama.
   Artinya, anda cukup mencari dan menyediakan 1 file original, dan memastikan bahwa file tersebut adalah file asli dari file yang terenkripsi(.globe). setelah 1 file original yang sesuai anda sediakan, maka tools dapat mendecrypt seluruh file terenkripsi yang lain tanpa memerlukan file originalnya.
   Cara sederhana menemukan file original adalah dengan mengingat apakah anda pernah menyalin atau mengunggah file dalam laptop anda (misalnya ke flashdisk atau ke email) sebelum terinfeksi virus. Selanjutnya anda bisa memastikannya berdasarkan kesamaan lokasi dan kesamaan ukuran antara file original dengan file terenkripsinya.
   Jika 1 file original dan file terenkripsi telah tersedia dengan benar (artinya memang itulah file original dari file terenkripsi), maka tools decryptor seharusnya berhasil menemukan algoritma yang tepat. Tapi jika file tidak cocok (itu bukan file original dari file terenkripsi), maka tools kemungkinan besar tidak akan berhasil mengdecrypt file lain karena algoritma yang salah.

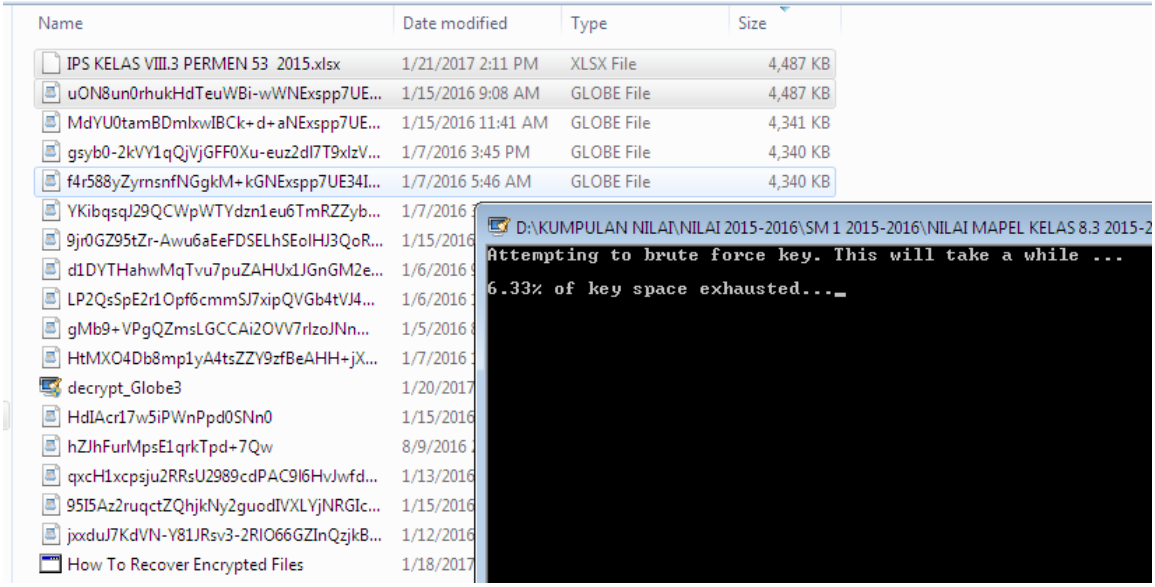


Gambar 2. File original (dari file yang terenkripsi) yang berasal dari laptop lain

Perhatikan pada gambar ukuran file sama (4,487 KB), yang berada pada folder yang sama sehingga disimpulkan file “IPS KELAS VII.3 PERMEN 53 2015.xlsx” merupakan file original dari file terenkripsi “uQNB……”.
File original ini diperoleh dari laptop lain yang dicopy sebelum terinfeksi virus.

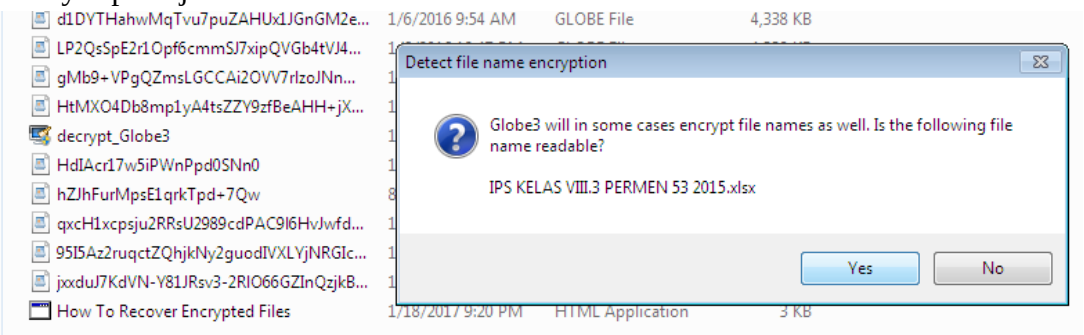
2. Copy juga tools decryptor ke dalam folder file terenkripsi tersebut.

3. Drag file original dan file yang dienkripsi virus bersama-sama ke dalam file emmisoft decryptor, maka akan terlihat progress brute force dari tools decryptor yang sedang berkerja



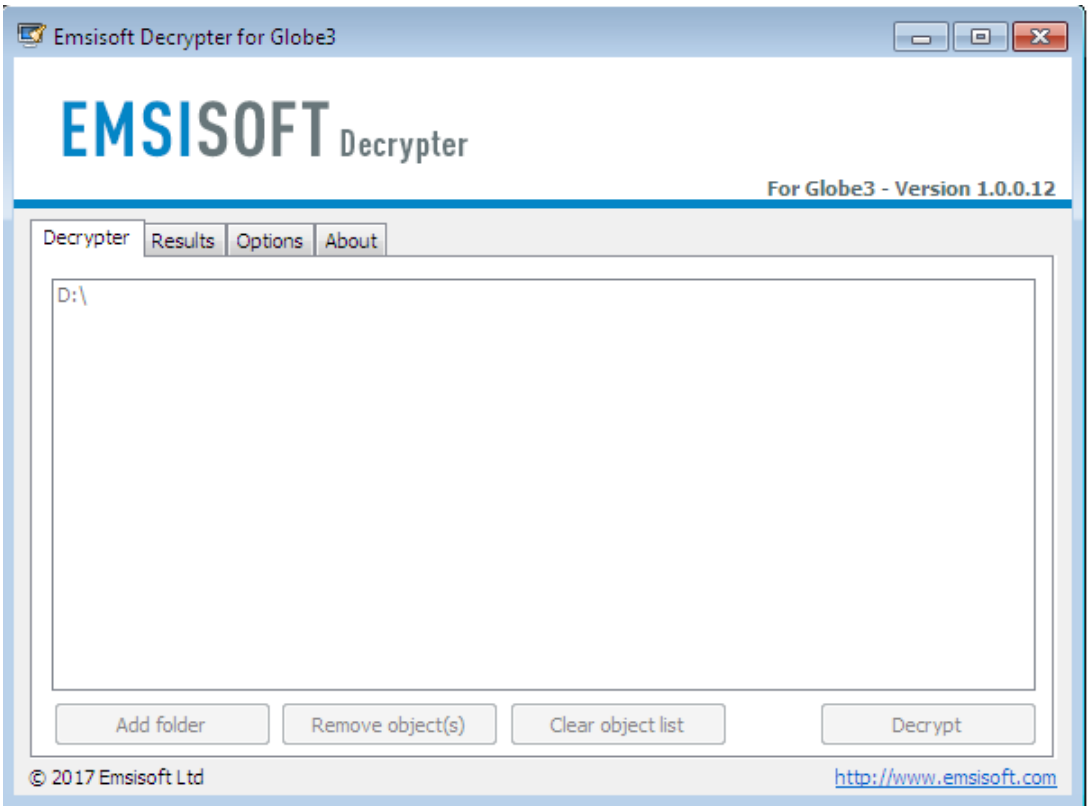
Gambar 3. Progress pencairan algoritma enkripsi

4. Klik yes pada jendela konfirmasi.



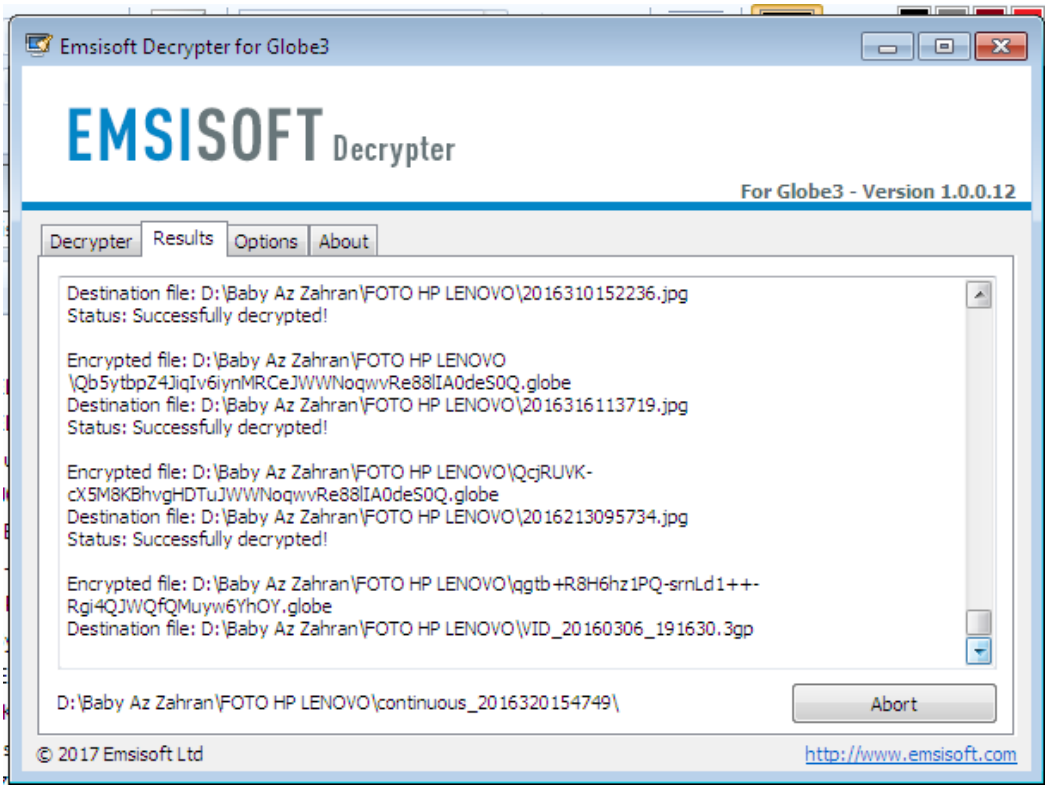
Gambar 4. Permintaan konfirmasi setelah pencarian algoritma selesai

5. Tentukan drive atau folder yang ingin dicek dan dipulihkan oleh tools dan klik **Decrypt**. (pada tahap ini, tools tidak memerlukan file original lagi)



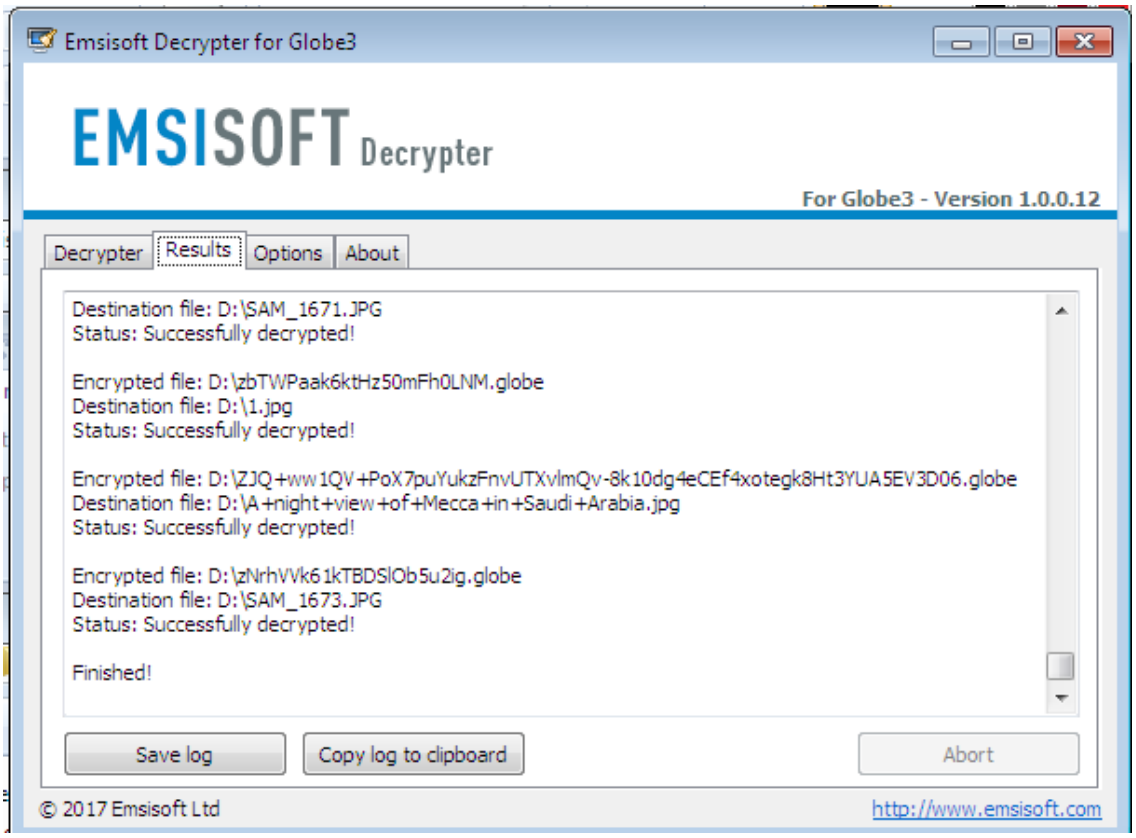
Gambar 5. Pemilihan drive D untuk di cek dan dipulihkan

6. Klik Tab Result untuk melihat progress proses pemulihan.

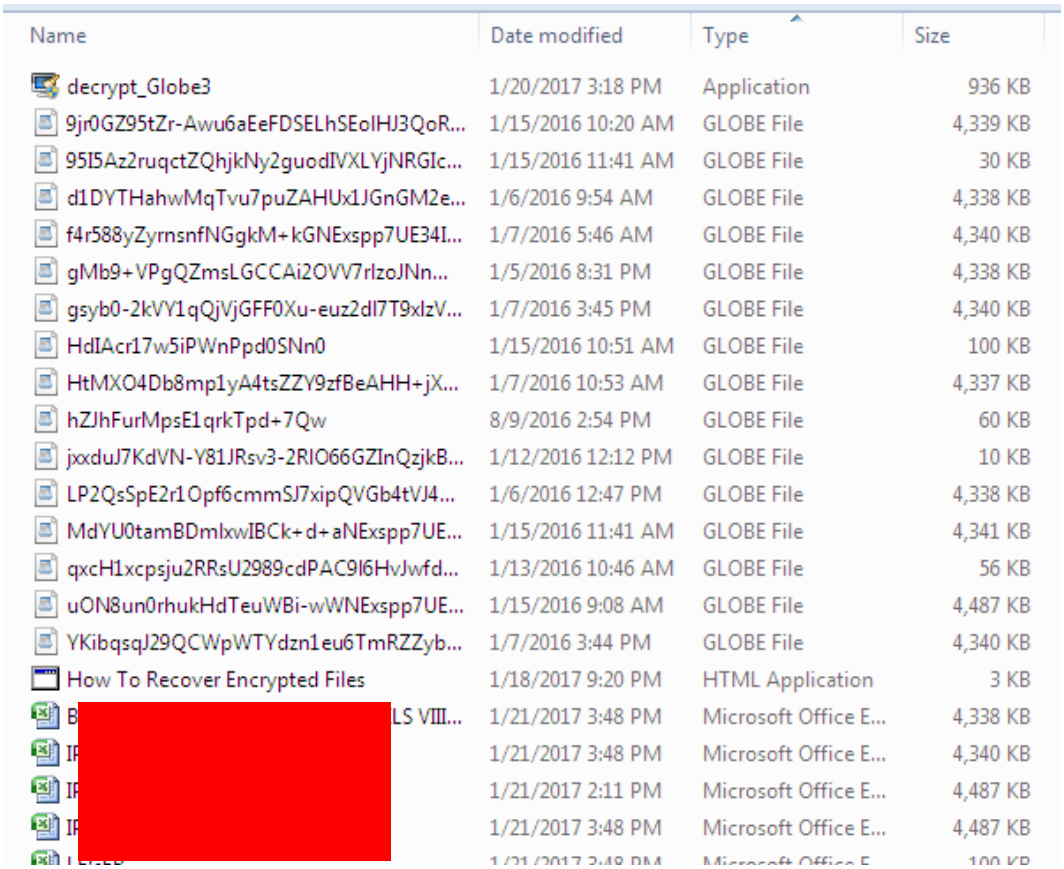


Gambar 6. Progress proses pemulihan(decrypt) seluruh file yang terinfeksi pada drive D

7. Akhirnya proses selesai dengan hasil seluruh file sukses dipulihkan.



Gambar 7. Informasi proses pemulihan selesai



Gambar 8. File-file original yang berhasil dipulihkan

PENUTUP

Tulisan ini penulis buat sebatas pemahaman penulis yang berdasarkan informasi terbatas yang penulis dapatkan. Tentu saja bisa terdapat pemahaman yang kurang tepat dan untuk itu penulis mengharapkan koreksi dari pembaca.

Akhir kata, semoga bermanfaat.

Kontak saya di **yuda89pratama@gmail.com**