**Ransomware WannaCry yang Mengguncang Dunia *Cyber***

Dunia *cyber* belum lama ini digemparkan oleh serangan ransomware berjenis WannaCry. Program jahat ini telah menyerang jaringan komputer milik rumah sakit dan perusahaan di berbagai belahan dunia mulai 12 Mei 2017 kemarin.

Ransomware WannaCry mengunci dokumen penting dari pihak yang diserang, membuatnya tak bisa diakses dan muncul pesan untuk membayar uang tebusan agar dokumennya bisa kembali. Jika tidak membayar uang tebusan, penyandera mengancam akan menghapus dokumen-dokumen milik korban.

**Apa itu RANSOMWARE?**

**Ransomware** adalah bentuk malware yang masuk ke dalam sistem dan mengunci pengguna dengan cara mengenkripsi seluruh file. Setiap dokumen yang terkunci oleh peranti lunak ini hanya bisa diakses dengan cara memasukkan kode unik yang hanya dimiliki si penyebarnya. Enkripsi ini bisa ‘ditebus’ dengan cara mengirimkan sejumlah uang kepada pemilik virus.



Tapi, ransomware sendiri tidak terbatas hanya pada mengunci dokumen saja, ada varian lain yang mengunci komputer sepenuhnya. Saat komputer dinyalakan, ransomware akan menampilkan pesan agar korban membayar tebusan untuk bisa mengoperasikan komputer.

Selain itu, ada juga varian ransomware yang memunculkan pesan pop-up yang sulit untuk ditutup dan membuat komputer sulit untuk digunakan.

**Bagaimana Ransomware Dapat Menginfeksi?**

Ransomware bisa menyerang komputer siapa saja, bisa datang dari kegiatan saat kita berselancar di dunia maya, seperti mengklik sebuah link yang ternyata 'jebakan', atau mengunduh dan membuka sebuah file.

**WannCry Hanya Menyerang Windows**

Para peneliti meyakini mengapa ransomware WannaCry hanya menyerang Windows dikarenakan para penjahat mengeksploitasi celah keamanan yang dinamakan EternalBlue pada OS Windows. Cikal bakal program ini dibikin dan dimiliki oleh Badan Intelijen Amerika Serikat (National Security Agency/NSA). Celah ini kemudian bocor dan dipakai para peretas untuk menerobos keamanan sistem operasi Windows dan menyebarkan ransomware WannaCry.

**Daftar Ransomware Indonesia**

Berikut ini adalah daftar sebagian ransomware yang pernah ada di Indonesia:

1. Cryptolocker

Cryptolocker sebenarnya sudah tidak menyebar lagi karena servernya sudah teridentifikasi dan dihentikan oleh pihak berwajib, namun karena ia merupakan ransomware pertama yang sukses dan banyak ransomware yang mengikuti metode dan cara penyebaran cryptolocker, maka cryptolocker tetap perlu diberikan sebagai acuan informasi supaya pembaca berhati-hati terhadap aksi ransomware.

Cryptolocker akan menyebar melalui email dengan lampiran yang di kompres (RAR/ZIP), file tersebut berisi sebuah file (nama file acak) dengan ekstensi ganda (pdf.exe).

1. CryptoDefense

CryptoDefense akan mengenkripsi file yang berada pada drive lokal pada komputer yang terinfeksi dan pada mapping drive. Setiap file yang di enkripsi akan menambahkan string !crypted! di awal isi file.

1. CryptoWall

Menyebar menggunakan email dan memanfaatkan celah keamanan software [oracle java remote | code execution vulnereability| abobe flash player] , emails, website (popup)

1. CryptoOrbit

Menyebar menggunakan email dan memanfaatkan celah keamanan software [oracle java remote | code execution vulneebility| abobe flash player] , website (popup). CryptOrbit tidak akan meng-enkripsi file, tetapi akan merusak file dengan menghapus string pada header file sehingga terjadi perbedaan ukuran sebesar 512 kb dari file asli yang mengakibatkan file tidak dapat dibuka.

1. Locker V.x.xx (varian)

Menyebar dengan menggunakan email (ZIP/RAR/Cab) dan internet dengan memanfaatkan celah keamanan aplikasi. Locker juga mematikan proses aplikasi VirtualBox/VmWare. Namun, pada akhirnya pembuat Locker akhirnya memutuskan untuk memberikan kunci dekripsi secara gratis

**Bagaimana Cara Mengatasi Ransomware WannaCry?**



Ada beberapa cara yang disarankan oleh ahli-ahli IT guna mengatasi penyebaran virus ini.

1. **Unduh update terbaru Microsoft**, terutama jika kamu saat ini menggunakan Windows XP. Microsoft telah menganalisis ancaman ini dan sudah menyediakan patch untuk menutup celah keamanan yang dieksploit malware ini melalui update terbaru.
2. **Install perangkat lunak anti-malware**. Pembuat perangkat lunak yang terlebih dahulu berhasil secara spesifik mengembangkan tool untuk menangkal ransomware wannacry adalah ESET. Software anti-malware ESET akan meningkatkan perlindungan dengan menambahkan deteksi terhadap ancaman spesifik seperti Win32/Filecoder.WannaCryptor.D.
3. **Waspadai tautan mencurigakan**! Jangan sembarangan mengklik tautan yang ada di email mencurigakan atau pesan aneh dari temanmu baik dari Skype, WA, Messenger, atau Instant message app lain.
4. **Aplikasi control berbasis whitelist** dapat digunakan karena WannaCry meninggalkan jejak jahat di sistem untuk menjalankan aksi enkripsi file yang terinfeksi.
5. **Penempatan patching** juga amat penting karena ransomware mengeksploitasi celah dari server SMB (Server Message Block). Sehingga, patching dapat melindungi serangan yang merasuki celah-celah keamanan tersebut.
6. **Block Ports : 139/445 & 3389**.