Bab I Pendahuluan

1.1. Latar Belakang Penelitian

Perkembangan teknologi yang semakin pesat tidak berarti akan menurunkan ancaman *cyber*, bahkan para penjahat *cyber* pun semakin berkembang dalam mengganggu pengguna komputer dan internet. Salah satu program jahat baru yang muncul beberapa tahun terakhir ini adalah *Ransomware*, *ransomware* ini mempunyai kemampuan melumpuhkan data komputer. Motif *ransomware* ini bertujuan untuk memeras pengguna komputer yang terinfeksi software melalui pemberitahuan permintaan pembayaran agar data komputer bisa kembali seperti semula (Suryadhi, 2012).

Sistem kerja *ransomware* mengenkripsi setiap data yang ada di dalam komputer korban, sehingga sulit untuk bisa dipulihkan oleh user pada umumnya. Penggunaan anti virus juga tidak terlalu berdampak, sebab *ransomware* ini diciptakan bukan untuk merusak tapi untuk menyandra data korban dengan enkripsi dan hanya bisa didekripsi oleh sang pembuat virus dengan membayar uang tebusan terlebih dahulu. Kejahatan *cyber* melalui *ransomware ransomware* diprediksi akan semakin merajalela. Perusahaan software keamanan komputasi Symantec mengatakan modus kejahatan ini semakin digemari penjahat dunia maya sejak setahun lalu (2012) dan diperkirakan terus meningkat (Putra, 2013).

Tim riset Dell SecureWorks Counter Threat Unit (TM) (CTU) menganalisis adanya *ransomware* file-encrrypting *ransomware* yang sedang aktif didistribusikan melalui Internet pada akhir Februari 2014, Jenis *ransomware* ini dikenal dengan nama Cryptolocker, meskipun mulai dikenal pada kuartal pertama 2014, tapi sebenarnya telah didistribusikan setidaknya sejak awal November 2013. Para peneliti CTU menganggap Cryptolocker akan menjadi *ransomware* yang terbesar dan paling merusak di internet, hal ini terbukti sampai saat ini tahun 2017 malware cryptolocker masih mengeluarkan varian terbarunya. (Intelligence, 2014)

Teknologi enkripsi yang digunakan Cryptolocker adalah enkripsi RSA 2048 yang digunakan oleh raksasa internet seperti Yahoo, Google, Facebook, industri keuangan dan e-commerce untuk melindungi lalu lintas data dari transaksi keuangan dan transaksi penting lainnya. Dimana kunci dekripsinya (Private Key) hanya dimiliki oleh pembuat *ransomware*

yang memiliki akses dan kontrol pada server yang digunakan untuk melakukan enkripsi. Namun, dalam banyak kasus, sekalipun uang tebusan (ransom) sudah dibayar, tidak ada jaminan bahwa dekripsi atas data yang dienkripsi akan berhasil

Sumber: https://www.secureworks.com/research/cryptolocker-*ransomware*

Country	Number of infected systems	Percentage of total
United States	22,360	70.2%
Great Britain	1,767	5.5%
India	818	2.6%
Thailand	691	2.2%
Peru	688	2.2%
Canada	658	2.1%
Philippines	645	2.0%
Indonesia	427	1.3%
Iran	333	1.0%
Ecuador	264	0.8%

Gambar 1.1 Rincian Geografis jumlah infeksi.

Penelitian tentang *Cryptolocker* masih sedikit dan hal yang harus diungkap adalah bagaimana cara kerja dari *ransomware* tersebut.hal ini disebabkan karena *ransomware* yang tidak biasa akan menyerang user tanpa diketahui gejala-gejala dalam penyerangannya. Oleh karena itu dibutuhkan penjelasan dan cara untuk mengantisipasi serangan *ransomware* tersebut pada sebuah komputer. Rincian geografis jumlah infeksi dapat dilihat pada gambar 1.1. Sedangkan tampilan cryptolocker pada komputer korban dapat dilihat pada gambar 1.2.

Gambar 1.2 Tampilan *Cryptolocker* di komputer korban

Penelitian tentang *Ransomware Cryptolocker* ini sangat penting karena perkembangan *ransomware* jenis *ransomware* ini sangat beragam, informasi yang dihasilkan dari analisa *ransomware* juga dapat dimanfaatkan oleh sub bidang lain, seperti digital *forensic examiner* dapat mengetahui bagaimana sebuah alur serangan terjadi serta hal-hal apa saja yang dilakukan oleh *ransomware* di dalam sistem termasuk karakteristik dan pola serangan

sehingga memungkinkan ditemukan hubungan dengan kasus yang sedang ditangani. Disamping itu penelitian ini dapat berkontribusi dalam dunia akademis untuk menambah acuan literatur dan informasi.

1.2. Identifikasi Masalah

Identifikasi masalah pada penelitian ini adalah

a. Salah satu program jahat baru yang muncul beberapa tahun terakhir ini adalah *Ransomware*,
b. Sistem kerja *ransomware* ini mengenkripsi setiap data yang ada di dalam komputer korban sehingga sulit untuk bisa dipulihkan oleh user pada umumnya
c. Masih sedikit penelitian yang dilakukan mengenai *ransomware Cryptolocker*
d. Korban tidak menyadari bahwa komputernya telah terinfeksi ransomware karena gejala-gejalanya tidak terlihat

1.3. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah :

a. Bagaimana mensimulasikan serangan *Cryptolocker* pada komputer?
b. Bagaimana karakteristik *Cryptolocker* dalam menyerang sistem data komputer?
c. Bagaimana metode Surface Analysis, Runtime Analysis dan Static Code Analysis mampu mendapatkan bukti digital untuk mendukung investigasi penyidikan dalam *malware forensics?*

1.4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini yaitu :

a. Membangun simulasi serangan *Cryptolocker* pada komputer.
b. Membuktikan sistem kerja *Cryptolocker* dalam menyerang sistem data komputer.
c. Mendapatkan bukti digital untuk mendukung investigasi penyidikan dalam *ransomware forensics*.

1.5. Batasan Masalah

Batasan masalah pada penelitian ini adalah :

a. Aplikasi yang akan di uji berjalan pada *platform* sistem operasi *Windows* 8 *enterprise*.
b. Simulasi *ransomware* dijalankan pada sebuah *real* komputer sebagai *environment* nya.

1.6. Manfaat Penelitian

Penelitian ini diharapkan dapat memberi kontribusi dalam kehidupan manusia dan dapat diterapkan dalam dunia nyata. Adapun manfaat penelitian ini antara lain :

a. Manfaat Bagi Peneliti

Dengan penelitian ini, diharapkan dapat menambah ilmu pengetahuan dan pemahaman mengenai analisa *ransomware* menggunakan metode *Surface Analysis, Runtime Analysis* dan *Static Code Analysis* sehingga nantinya dengan ilmu tersebut dapat dipergunakan dan bermanfaat bagi orang banyak.

b. Manfaat Bagi Instansi

Dengan adanya penelitian ini, diharapkan institusi / lembaga mendapatkan informasi mengenai hasil analisa *ransomware* dan implementasinya, serta sebagai acuan dalam metode analisa *ransomware* kedepannya.

c. Manfaat Bagi Pihak Lain

Dengan adanya penelitian ini diharapkan akan dapat membantu mengurangi serangan *ransomware*, serta mengamankaan data informasi strategis penting di lingkungannya.

1.7. Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini antara lain :

a. Studi Literatur

Studi Literatur digunakan untuk mendalami konsep dasar tentang *ransomware* dan perkembangannya

b. Sampel *Ransomware*

Proses mendapatkan sampel dan menguji sampel *ransomware*

c. Pembuatan Environment

Membangun sistem komputer untuk simulasi penyerangan *Ransomware* Cryptolocker, sistem laboratorium tidak diinstall antivirus supaya tidak mengganggu proses analisa.

d. Analisis *Ransomware*

Terdiri dari *Surface Analysis, Runtime Analysis* dan *Static Code Analysis. Surface Analysis Merupakan pendeteksian ransomware* dengan mengamati sekilas ciri-ciri khas sebuah file program tanpa harus mengeksekusinya. Untuk melihat ciri khas tersebut dapat dilakukan dengan menggunakan bantuan software atau perangkat aplikasi pendudukung.

Runtime Analisis, model analisa ini menghasilkan kajian yang lebih mendalam, dengan mengeksekusi *ransomware* dimaksud akan dapat dilihat perilaku dari program dalam

menjalankan skenario jahatnya sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.

Static Code Analysis, pada proses ini *ransomware* akan dibaca struktur kode aplikasi yang ada di dalamnya, baik dengan metode debugging, metode disassembling dan metode decompiling.

e. Laporan

Penulisan laporan kegiatan penelitian dari awal sampai akhir sesuai dengan sistematika penulisan yang disarankan.

1.8. Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian, maka dibuat sistematika penulisan pada penelitian ini:

a. Bab I Pendahuluan

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

b. Bab II Landasan Teori

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan *ransomware*.

c. Bab III Metodologi Penelitian

Bab ini membahas tentang langlah-langkah penelitian dan gambaran umum langkah penyelesaian.

d. Bab IV Pembahasan

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat yaitu dengan melakukan analisis dan uji coba.

e. Bab V Kesimpulan dan Saran

Kesimpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan serta asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.