BAB 2
Tinjauan Pustaka

2.1 Malware

Malware merupakan kependekan dari *malicious software,* dalam definisi tentang malware disebutkan bahwa malware merupakan program yang sengaja dibuat untuk membahayakan dan merugikan sistem operasi atau data pada komputer (Siddiqui, 2008). Definisi ini mencakup semua program yang dapat merugikan atau membahayakan data dan sistem operasi seperti virus, worm, trojan, spyware dan yang sejenisnya.

2.1.1 Sejarah malware

Sejarah kapan pertama kali malware ditemukan masih menjadi perdebatan, hasil penelitian ada yang menyebutkan pada awal tahun 1970-an malware telah ditemukan, Creeper merupakan contoh malware yang ditemukan pada tahun 1970-an awal di jaringan kompute ARPANET milik ARPA yang menyerbar hanya di jaringan milik perusahaan tersebut, malware ini dibuat oleh salah satu insiyur perusahaan teknologi *BBN Tecnology* yang bernama Robert "Bob" H. Thomas (Dalakov, 2012).

Namun (Milošević, 2013) menjelaskan bahwa sejarah munculnya malware dibagi berdasarkan kategori dan masing-masing kategori memiliki waktu kejadian munculnya malware, namun secara umum malware sudah ada sebelum tahun 1986, dan pada tahun 1986 muncul malware pertama kategori virus pada platform MsDos milik perusahaan Microsoft yang bernama Brain.A, malware ini dibuat di Pakistan oleh dua bersaudara Basit dan Amjad.

Sedangkan (Krebs, 2014) menjelaskan bahwa virus komputer merupakan satu dari sekian bayak tipe dari malware, dimana program yang dibuat dapat menggandakan diri dan didesain untuk menyebar dari satu komputer ke komputer lain. Masih menurut Krebs, sebenarnya teori tentang program yang dapat menggandakan dirinya sendiri sudah ada sejak tahun 1949 yaitu sebuah artikel berjudul "*Theory of Self-Reproducing Automata"* yang ditulis oleh John von Neumann dimana dalam artikel tersebut penulisnya menjelaskan tentang program komputer yang dapat menggandakan diri sendiri, namun artikel ini baru terkenal setelah di publis kembali pada tahun 1966.

Jika diurutkan berdasarkan waktu kejadian kapan pertama kali malware ditemukan, maka malware jenis virus merupakan malware yang pertama kali exis dari semua jenis

malware, hal ini dijelaskan oleh (Krebs, 2014) dalam mengurutkan kejadian munculnya virus dari pertama kali yang diawali dengan tahun 1949 dengan terbitnya artikel berjudul "*Theory of Self-Reproducing Automata"* yang ditulis oleh John von Neumann kemudian pada tahun 1959 virus CoreWars yang dibuat oleh Victor Vysottsky, H. Douglas Mcllroy dan Robert P Morris di Bell Laboratorium, selanjutnya tahun 1960 virus Rabbit dan tahun 1971 Creeper malware jenis worm pertama kali ditemukan di jaringan milik ARPANET.

2.1.2 Jenis-Jenis Malware

Terdapat banyak jenis malware, dalam penelitian ini disebutkan beberapa jenis-jenis malware tersebut dengan pengertiannya masing-masing.

A. Virus

Virus komputer merupakan program atau code yang dapat menggandakan dirinya dan meyerang file eksekusi (.exe). Virus biasanya membutuhkan canpur tangan manusia atau pengguna komputer untuk menempatkan dirinya dan menjalankannya.

B. Ransomware

Ransomware adalah malware yang dirancang untuk mencegah akses terhadap system atau data yang telah dikunci sampai dilakukannya pembayaran kepada penyerang (Microsoft, 2017). Terdapat dua jenis ransomware yaitu :

1. *Locker* Ransomware, atau disebut komputer *locker*, malware ini mengunci perangkat komputer milik korban dan hanya memberi akses terbatas pada keyboard seperti karakter dan nomor pada keyboard untuk korbah memasukkan kode pembayara. Hal lain yang dilakukan *locker* ransomware selain mencegah korban mengakses komputernya, malware ini juga meninggalkan pesan dan petunjuk ke korban hal-hal yang harus dilakukan korban.
2. *Crypto* Ransomware, atau disebut data *locker*, merupakan jenis ransamware yang melakukan pencarian dan enkripsi terhadap data pribadi yang menjadi korban dari malware ini. Penelitian ini akan mengambil salah satu type dari ransomware jenis *crypto* ransomware.

C. Worm

Worm mrupakan program *stand alone* yang dapat menggandakan dirinya dan menyebar di jaringan komputer. Worm biasanya tidak butuh bantuan manusia atau campur tangan pengguna komputer untuk memicunya berjalan dan menggandakan dirinya.

D. Trojan

Trojan atau dalam istilah lain disebut Trojan hourse merupakan program yang masuk dan melakukan beberapa aktivitas berbahaya dengan kedok sebagai program normal.

E. Spyware

Spyware adalah program yang diinstall secara diam-diam di komputer pribadi untuk menangkap atau mengambil informasi tentang interaksi pengguna dengan komputer tanpa sepengetahuan pengguna atau pemilik komputer.

F. Rootkit

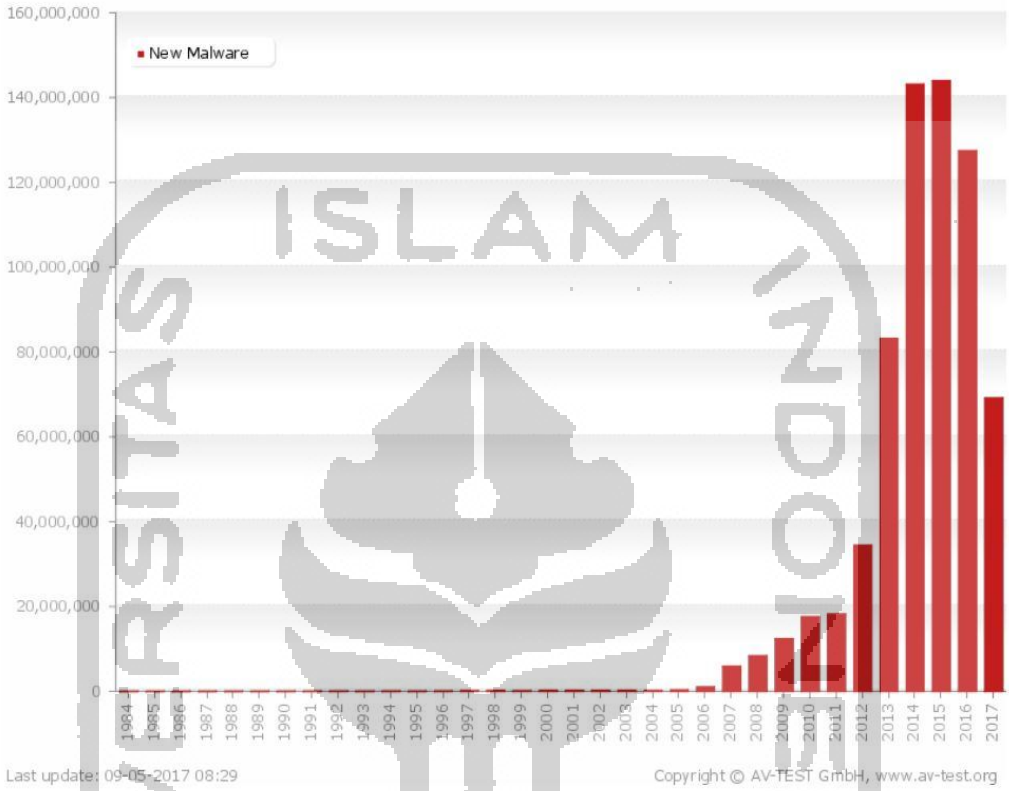
Rootkit pada awalnya merupakan program yang dipasang oleh penyerang pada sebuah sistem unix yang memungkinkan si penyerang mendapatkan hak akses sebagai administrator atau root. Saat ini rootkit digunakan lebih umum yaitu sebagai sebuah rutinitas dalam sebuah malware. Rootkit dapat mencegah agar prosesnya tidak terlihat dalam daftar proses yang berjalan pada sistem, atau mencegah agar filenya terbaca.

2.1.3 Perkembangan Malware

Perkembangan malware dari tahun ke tahun semakin meningkat terutama jika melihat grafik perkembangan malware untuk 10 (sepuluh) tahun terakhir, jika diawal-awal kemunculan malware jumlahnya tidak lebih dari 1 juta malware, maka untuk 5 (lima) tahun terakhir ditemukan 390.000 malware rata-rata setiap harinya, dalam laporannya (AV-TEST Institute, 2017) mulai merekam aktivitas perkembangan malware dimulai dari tahun 1984 sampain tahun 2017, peningkatan jumlah malware baru melebihi angka 1 (satu) juta dimulai dari tahun 2004 dan angka tertinggi malware baru yang ditemukan adalah di tahun 2014, 2015 dan 2016.

Tingginya jumlah peningkatan malware baru dihitung berdasarkan jumlah malware yang masuk ke database dan yang belum terekam dalam database sebelumnya, disamping metode pendeteksian malware yang masih menggunakan metode pendeteksian malware berbasis *signature based detection,* beberapa malware meskipun memiliki sekamaan *variant,* sistem, dan cara kerja namun pada kenyataannya anti virus dan program anti malware menganggapnya sebagai malware yang berbeda hal ini dikarenakan metode yang digunakan adalah metode deteksi yang masih menggunakan *signature based detection,* hal ini membuat beberapa malware yang dikembangkan menjadi malware baru meskipun dengan tingkat perubahan yang sangat sedikit akan dihitung sebagai malware baru, meskipun perubahan itu hanya berupa beberapa bari ataupun beberapa karakter hal ini cukup untuk dapat mengubah *signature* dari malware lama menjadi *signature* malware

baru. Berikut merupakan grafik perkembangan malware baru berdasarkan laporan yang diambil dari situs (www.av-test.org, 2017), grafik menunjukkan rekaman perkembangan malware baru sejak tahun 1984 sampai dengan tahun 2017.

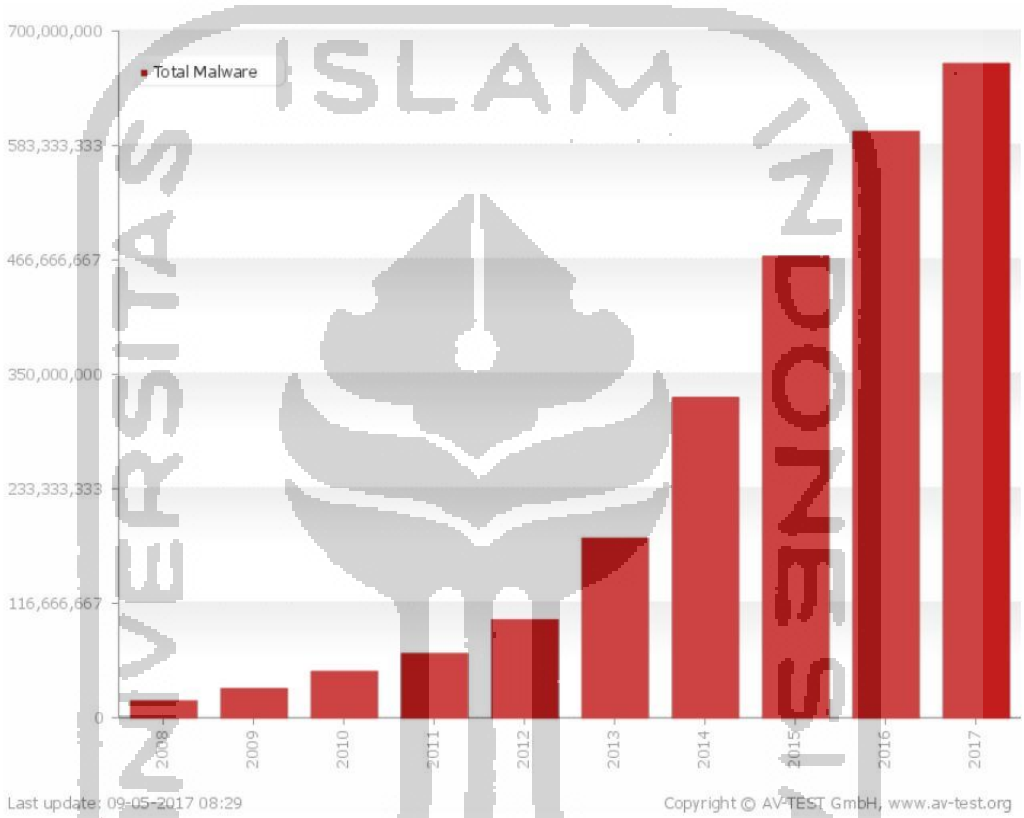


Gambar 2.1 Malware baru dalam angka sejak tahun 1984 – 2017

Sumber : (www.av-test.org, 2017).

Dari gambar 2.1 diatas menunjukkan peningkatan jumlah malware baru yang sangat signifikan terjadi sejak tahun 2007, dan terus mengalami peningkatan jumlah setiap tahunnya dan baru mengalami penurunan ditahun 2016, dan pada tahun 2017 mengalami penurunan sangat jauh berdasarkan data yang terdapat pada grafik, penurunan dari angka 120 (seratus dua puluh) juta malware turun menjadi 70 (tujuh puluh) juta malware untuk tahun 2017. Adapun total malware yang berhasil direkam untuk semua kategori yaitu malware baru dan malware lama dalam kurun waktu 10 (sepuluh) tahun terakhir terus mengalami peningkatan dari tahun 2008 sampai dengan tahun 2017, hal ini sebagaimana yang terdapat pada grafik dibawah yang diambil dari situs yang sama (www.av-test.org, 2017), menujukan peningkatan yang sangat tinggi terjadi pada kurun waktu tahun 2013 ke tahun 2014 yaitu dari angka 200 (dua ratus) malware ke angka 300 (tiga ratus) malware, terus mengalami peningkatan lagi pada kurun waktu tahun 2014 ke tahun 2015 yaitu dari

angka 300 (tiga ratus) juta malware ke 466 (empat ratus enam puluh enam) juta malware, dan masih mengalami perkembangan dari tahun 2015 ke tahun 2016 yaitu dari 466 (empat ratus enam puluh enam) juta malware menjadi 590 (lima ratus sembilan puluh) juta malware, selanjutnya perkembangan malware antara tahun 2016 ke tahun 2017 mengalami peningkatan namun tidak sebanyak tahun-tahun sebelumnya, hal ini dapat dilihat pada gambar 2.2 dibawah :



Gambar 2.2 Total Malware dalam kurun waktu 10 (sepuluh) tahun terakhir.

Sumber : (www.av-test.org, 2017).

Dari sekian banyak temuan malware yang paling banyak menarik perhatian dalam 5 (lima) tahun belakangan adalah malware jenis ransomware, bahkan tool anti virus McAfee (McAfee Labs, 2016) memberi judul laporannya dengan "Tahun 2016 akan diingat sebagai tahunnya Ransomware", ransomware mulai diketahui sejak tahun 2006 menurut (Vysottsky, 2014), namun jenis malware yang memiliki prinsip kerja dengan melakukan proses enkripsi sudah ada sejak tahun 1989 yaitu *AIDS Trojan* dimana malware ini malakukan enkripsi terhadap nama file (Lab Kapersky, 2016) dan pada tahun 2006

muncul malware *gpcode*, *TROJ.RANSOM.A* dan beberapa malware lainnya yang memiliki kesamaan system kerja yaitu melakukan enkripsi terhadap file (Deloitte, 2016).

2.1.4 Malware dan dampak hukum di Indonesia

Malware secara umum adalah program yang segaja dirancang untuk merusak atau merugikan pengguna komputer atau pemilik data, dan malware yang yang menjadi perhatian beberapa tahun terakhir adalah ransomware malware, malware ini sengaja dirancang untuk membajak data pengguna komputer, oleh karena itu butuh instrument hukum untuk menjamin dan melindungi hak-hak pemilik data, salah satunya adalah dalam bentuk undang-undang.

Terkait perlindungan data pribadi dalam bentuk Dokumen Elektronik atau Informasi Elektronik, Pasal 32 UU ITE mengatur tentang larangan bagi setiap Orang untuk melakukan interferensi (mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan) terhadap bentuk Dokumen Elektronik atau Informasi Elektronik tanpa hak dan dengan cara melawan hukum. Ancaman hukuman atas perbuatan tersebut diatur dalam Pasal 48 UU ITE.

Pasal 32 UU ITE selengkapnya berbunyi:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Sedangkan Pasal 48 UU ITE berbunyi:

(4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

(5) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(6) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). (www.hukumonline.com, 2013).

2.2 Metode-Metode Deteksi

Perkembangan Jumlah malware yang terus bertambah sangat pesat dan masih akan terus bertambah membuat para peneliti keamana komputer harus melakukan terobosan untuk menemukan metode baru untuk melindungi komputer dari serangan malware. Secara umum terdapat beberapa metode deteksi malware, namun dari semua metode jika dirangkum maka akan menjadi tiga metode deteksi malware yang paling populer, ketiga metode deteksi malware tersebut yaitu *Signature Based Detection, Behavior Based Detection dan Statistical Based Detection* (Damodaran, 2015).

2.2.1 *Signature Based Detection*

S*ignature based detection* adalah metode deteksi malware dengan cara mencocokkan dua pola atau *signature* dimana salahsatu pola menjadi model untuk pola yang akan dicocokkan, proses untuk mengukur kesamaan dua pola dilakukan dengan menggunakan salah satu atau kombinasi dari tiga bagian *signature* yaitu *file magic number* atau yang biasa disebut dengan file *signature*, kemudian file *checksum* atau biasa disebut file hash dan, *string signature* yaitu deretan *bytes* tertentu dalam tubuh file malware. Proses untuk memeriksa file *signature* dilakukan untuk menemukan setidaknya satu pola urutan byte dengan pola urutan byte yang ada di database *signature*, database ini merupakan database yang berisi daftar *signature* yang terdiri dari kombinasi pola urutan byte malware atau file hash yang telah didefinisikan sebelumnya oleh pakar keamana melalui ananlisis.

Signature based detection merupakan metode deteksi malware yang umum digunakan pada *tools* anti virus saat ini, pada metode ini terdapat beberapa cara yang biasa digunakan yaitu menggunakan file *checksum* atau kombinasi dari ketiga cara yaitu file *checksum, string signature* dan file *signature*. Dalam metode *signature based detection* penggunaan fungsi hash atau file *checksum* merupakan hal paling diutamakan, dan algoritma *hash* yang mula-mula digunakan adalah CRC32, terakhir algoritma ini sudah ditinggalkan karena memiliki keterbasan dan mulai beralih ke algoritma *hash* md5 atau sha1, kerena alasan keterbatasan dan mulai ditemukan kelemahan pada algoritma yang digunakan seperti md5 dan sha1 maka para penliti mengembangkan algoritma baru yang

sudah mulai diterapkan di lingkungan dunia malware dan keamanan computer seperti algoritma hash sha256.

2.2.2 *Behavior Based Detection*

Behavior based detection adalah metode deteksi malware berdasarkan pada perilaku malware. Perilaku malware di-*extract* melalui proses analisis saat malware dieksekusi menggunakan *tool* analisis, selain itu proses analisis dilakukan untuk memahami maksud dari malware. Dalam metode ini perilaku malware dan aplikasi normal dipelajari dan dilakukan pemantauan dalam masa waktu tertentu, setelah itu sebuah *executable* dikategorikan sebagai malware atau sebagai aplikasi normal.

Metode *behavior based detection* ini merupakan metode deteksi yang digunakan dalam penelitian ini, dalam metode ini penulis diharuskan untuk melakukan analisis terhadap sebuah malware, dipelajari dan dipantau perilaku dari malware tersebut desertai dengan beberapa aplikasi normal sebagai pembanding untuk mengetahui perilaku keduanya terhadap data, dari perilaku tersebut digunakan untuk deteksi malware.

2.2.3 *Statistic Based Detection*

Metode deteksi malware *Statistic Based Detection* adalah metode deteksi malware berdasarkan fitur-fitur yang tetdapat pada aplikasi atau malware. *Hidden Markov Model (HMM)* adalah salah satu metode untuk deteksi malware yang berbasis *statistic detection.* Metode ini biasa digunakan di sebagian besar pada sistem *speech recognition,* digunakan juga untuk *patern recognition, artificial intelligence* serta dalam hal *malware detection.*