ANALISA DAN PERANCANGAN KONSEP APLIKASI BIRDSHIELD

Nur Azis

Program Studi Sistem Informasi, Fakultas Teknik, Universitas Krisnadwipayana
Email : nuraziz@unkris.ac.id

Abstrak

Teknologi adalah salah satu unsur pokok dalam pembangunan yang terencana. Tanpa adanya perkembangan teknologi, maka perubahan zaman tidak akan secepat dan secanggih seperti sekarang. Adapun kecanggihan teknologi informasi yang kita nikmati saat ini merupakan buah hasil yang dimulai dari proses panjang puluhan atau bahkan ratusan tahun kebelakang. Terlepas dari dominasi yang terjadi, perkembangan teknologi seakan menjadi pisau bermata dua, dimana selain membawa manfaat juga sewaktu-waktu bisa melukai. Hal tersebut bisa dirasakan oleh para penguna personal *computer* (pc) atau laptop. Keamanan data menjadi isu penting dalam beberapa tahun terakhir. Jika ceroboh, informasi pribadi bisa jatuh ke tangan orang yang tidak bertanggung jawab. Hal tersebut terjadi karena pc yang digunakan terjangkit malware. Malware adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Berlatar belakang pemahaman diatas peneliti mencoba meneliti hal yang berkaitan dengan malware dengan mencoba membuat konsep aplikasi anti virus yang memiliki pandangan *cross-platform,* dan *cross-integrated engine.*

Kata Kunci : Teknologi, Personal Komputer, Malware, Konsep, Anti Virus

Abstrach

Technology is one of the main elements in planned development. Without the development of technology, the changing times will not be as fast and sophisticated as they are today. The sophistication of information technology that we enjoy today is the fruit of the results that began from a long process of tens or even hundreds of years back. Despite the dominance that occurs, the development of technology seems to be a double-edged knife, which in addition to bringing benefits can also hurt at any time. It can be felt by users of personal computer (pc) or laptop. Data security has become an important issue in recent years. If careless, personal information could fall into the hands of irresponsible people. This happens because the pc used is infected with malware. Malware is software created for the purpose of entering and sometimes damaging a computer system, network, or server without its owner knowing. Against the background of the above understanding researchers try to research things related to malware by trying to create the concept of anti-virus applications that have a cross-platform view, and cross-integrated engine.

Keywords : Technology, Personal Computer, Malware, Concept, Anti Virus

Pendahuluan

Dunia telah beralih dari era industrialisasi ke era informasi yang kemudian melahirkan masyarakat informasi (*information society*) (Ahmad 2012), perkembangan Teknologi Informasi (TI) terutama dengan teknologi internet sedang mengalami pertumbuhan yang sangat pesat. Seiring dengan kemajuan ini, muncul pula alternatif media baru yang berbasis pada TI(Syahri 2010). Begitu cepatnya perkembangan media internet menimbulkan pengaruh yang sangat signifikan bagi setiap negara. Indonesia merupakan salah satu negara yang mengalami dampak tersebut. Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), menyebutkan bahwa di Indonesia terdapat sekitar 25 juta pengguna internet. Setiap tahunnya pengguna internet terus meningkat sekitar 25%. Kenaikan tersebut salah satunya disebabkan oleh adanya kemudahan

dalam mendapatkan (mengakses) dan mengendalikan informasi serta mengoperasikannya(Setiawan 2018).

Dengan adanya kemudahan dalam mengakses informasi ada beberapa pihak yang coba mencuri data-data demi tujuan untuk kepentingan pribadi. Seperti dikutip dari jurnal yang ditulis oleh Vannyora Okditazeini dan Irwansyah (Okditazeini and Irwansyah 2018) bahwa Ketika sejumlah data pribadi dibagikan dalam SNS menjadikan pengguna target yang menggoda untuk diserang, seperti spam, malware, socialbots dan pencurian identitas. Bahkan penyerang dapat juga menemukan data signifikan lain, seperti informasi akun bank, yang kemudian digunakan untuk kejahatan seperti penipuan, kemudian identitas pribadi dan lokasi.

Dalam penelitian ini, peneliti coba membahas tentang malware dengan konsep birdshield, semoga dapat memberikan pengetahuan dasar tentang malware serta dapat melakukan pencegahan sebelum merusak pc atau laptop yang kita gunakan.

Tinjauan Studi

Teknologi

Kata teknologi secara harfiah berasal dari bahasa latin''texere''yang berarti Menyusun atau membangun. Sehingga istilah teknologi seharusnya tidak terbatas pada penggunaan mesin, meskipun dalam arti sempit hal tersebut sering digunakan dalam kehidupan sehari-hari(Ananda 2003)

Komputer

Komputer adalah sebuah mesin hitung elektronik yang secara cepat menerima informasi masukan digital dan mengolah informasi tersebut menurut seperangkat instruksi yang tersimpan dalam *computer* tersebut dan menghasilkan keluaran informasi yang dihasilkan setelah diolah(Kurniawan et al. 2015)

Malware

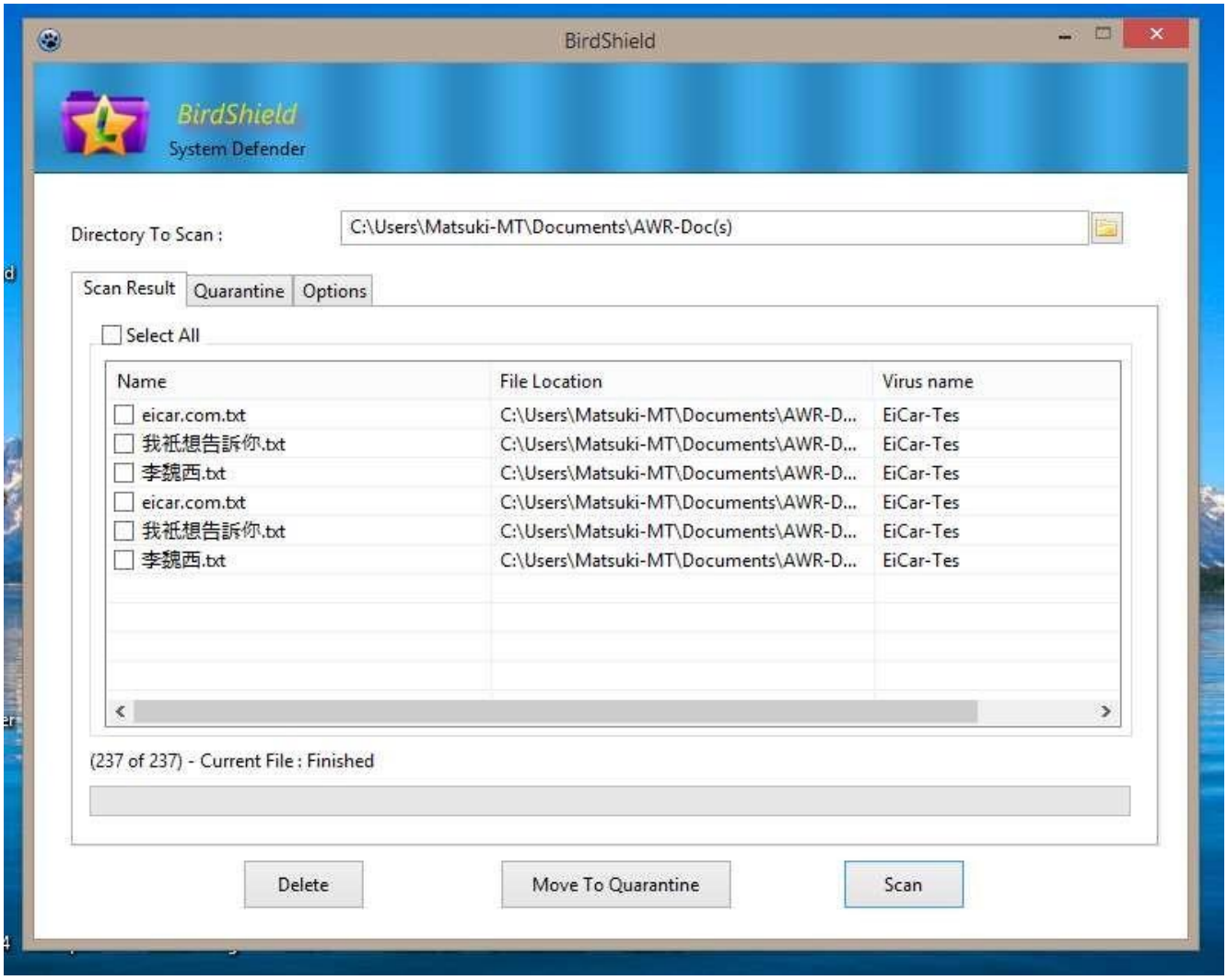
Malware didefinisikan sebagai semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat,seperti virus (komputer), trojans, spyware, dan worm. Virus komputer bekerja dengan cara menempel pada suatu file komputer yang biasanya berupa file executable, trojan bekerja dengan cara melakukan *social engineering files* berbahaya dengan menampilkannya seperti files yang terlihat tidak berbahaya(Septiani, Widiyasono, and Mubarok 2016)

Virus dan Antivirus Komputer

Istilah Komputer virus pertama kali digunakan oleh Fred Cohen dalam papernya yang berjudul 'computer viruses – Theory and Experiments' pada tahun 1983. Berikut kutipan definisi yang diberikan oleh Fred Cohen dalam paper tersebut : "we define a computer 'virus' as a program that can 'infect' other programs by modifying them to include a possibly evolved copy itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and this infection grows." Yang dikutip oleh Nazori Suhandi(Suhandi 2009)

Implementasi dan Pengujian

Tahap ini merupakan kegiatan pembuatan sistem atau aplikasi dengan menggunakan bantuan perangkat lunak maupun perangkat keras sesuai dengan analisis dan perancangan untuk menghasilkan suatu sistem yang bekerja



Gambar 1. Pengujian Virus dengan Aplikasi Birdshield

Pada pengujian diatas terlihat sejumlah virus atau malware di dalam *system computer* yang sedang di scaning, meskipun contoh virus tersebut telah di ubah namanya namun tetap di deteksi.

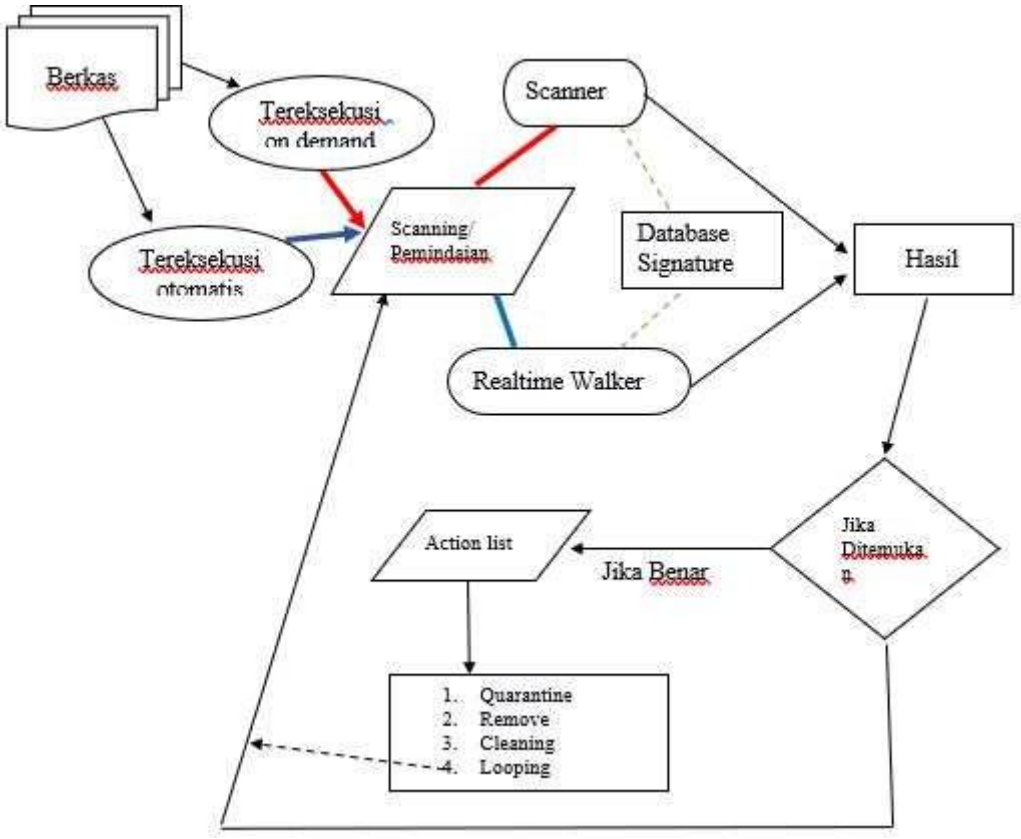
Paradigma dan Metode

Dalam implementasinya, sesungguhnya BirdShield menggunakan :

1. MD5 Checksum
2. SHA1 Checksum
3. SHA256 Checksum
4. SHA512 Checksum
5. Packer Mekanisme
6. UPX Mekanisme (Untuk PE Packing dan Unpacking)
7. 7Zip Compressing mekanisme

Semua disatukan didalam wadah proses multithreading dimana lingkungan atau sistem yang berorientasi multicore.

Adapun rancangan dasar awal sebagai berikut :



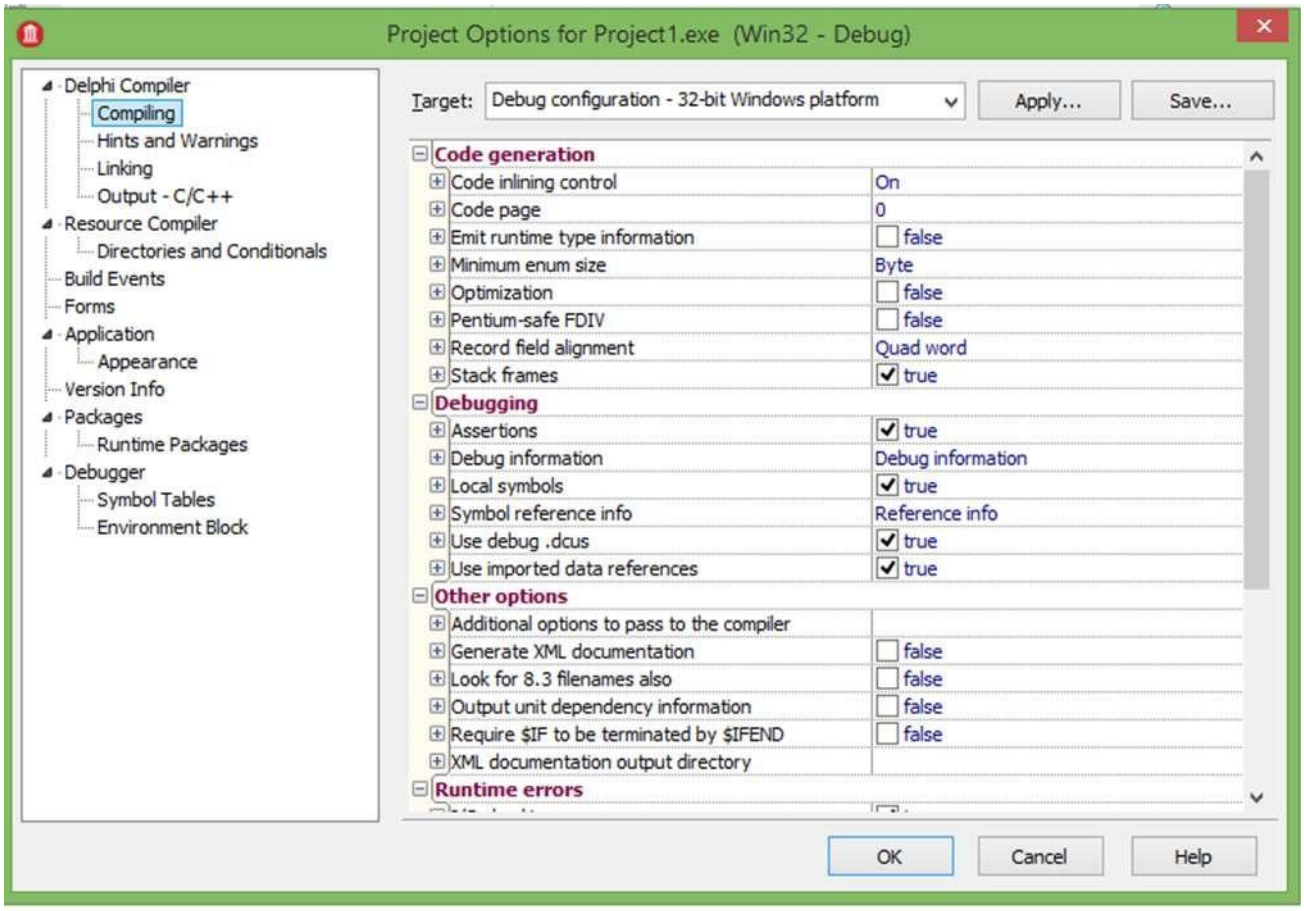
Gambar 2. Rancangan Konsep Dasar

Keterangan :

1. Scanning atau Pemindaian, merupakan sebuah proses melakukan cek terhadap suatu PE dengan beberapa mekasime atau standard checking yang telah ditetapkan sebelumnya untuk memutuskan apakah sebuah berkas itu memiliki indikasi dari sebuah malware atau tidak. Didalamnya terdapat penggunaan metode checking MD5, SHA1, SHA256, SHA512, checking setiap section, melihat penggunaan packer dan bagaimana cara unpackingnya.
2. Scanner, merupakan sebuah modul untuk melakukan scanning bersifat “on demand” (sesuai kebutuhan dan permintaan). Di operasikan oleh pengguna ketika dibutuhkan saja
3. Realtime Walker, merupakan sebuah mekanisme kerja serupa dengan scanner dari segi fungsi namun lebih kepada “automatisasi” scanner, dimana akan melakukan scanning terhadap semua tindakan baik yang dilakukan pengguna maupun sistem operasi itu sendiri. Disini, menggunakan teknik “hooking system processes”.
4. Database, menggunakan struktur terorganisir dari SQLite3 sebagai backend database sebuah signature malware, dimana tersimpan data identitas yang terindikasi sebagai sebuah malware.

Implementasi Pengujian

Meskipun terkesan kuno dan tidak terlalu bagus, namun dengan checksum terhadap beberapa section didalam sebuah berkas, maka akan dapat terdeteksi adanya “suatu injeksi” terhadap berkas atau tidak. Sebuah berkas, mungkin terinfeksi malware namun masih dapat berjalan seolah normal, namun ada script tersembunyi dimana malware menyisipkan perintah agar mengeksekusi dirinya terlebih dahulu sebelum berkas aseli tereksekusi. Seperti terlihat pada gambar 3.



Gambar 3. Implentasi Pengujian

Kesimpulan

Memang aplikasi ini perlu banyak perbaikan, pada aplikasi ini hanya sedikit menggambarkan :

1. Sesungguhnya virus merupakan sebuah program biasa, namun memiliki tujuan khusus dan biasanya merusak.
2. Salah satu cara termudah dalam mendeteksi virus adalah memperhatikan section pada berkas file. Virus biasa bersembunyi didalam salah satu section, ataupun dia membuat section tambahan.

Daftar Pustaka

[1] Ahmad, Amar. 2012. "Perkembangan Teknologi Komunikasi Dan Informasi." *Dakwah Tabligh* 13:137–49.

[2] Ananda, Erlisa Dwi. 2003. "Pemanfaatan Teknologi Informasi." *Jurnal Ilmiah Ilmu Dan Teknologi Lingkungan* 5(20):1–14.

[3] Kurniawan, Hendra, Dosen Manajemen Informatika, Jurusan Sistem Komputer, and Kendali Cahaya. 2015. "Jurnal TEKNOIF ISSN : 2338-2724 IMPLEMENTASI SISTEM KENDALI CAHAYA DAN SIRKULASI UDARA RUANGAN DENGAN MEMANFAATKAN PC DAN MIKROKONTROLER Pendahuluan Latar Belakang Maasalah Dalam Kehidupan Sehari-Hari , Manfaat Udara Dan Cahaya Sangat Diperlukan Bagi Tubu." *Jurnal TEKNOIF* 3(1):12–19.

[4] Okditazeini, Vannyora, and Irwansyah Irwansyah. 2018. "Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS)." *Jurnal Studi Komunikasi Dan Media* 22(2):109.

[5] Septiani, Devi Rizky, Nur Widiyasono, and Husni Mubarok. 2016. "Investigasi Serangan Malware Njrat Pada PC." *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)* 2(2):123–28.

[6] Setiawan, Daryanto. 2018. "Dampak Perkembangan Teknologi Informasi Dan

Komunikasi Terhadap Budaya." *JURNAL SIMBOLIKA: Research and Learning in Communication Study* 4(1):62.

[7] Suhandi, N. 2009. "Pengembangan Antivirus Songket Untuk Virus H1N1 Dengan Metode Behavior Blocking Detection." *Jurnal Generic* 4(2):79276.

[8] Syahri, Akhmad Syafrudin. 2010. "Bayang-Bayang Uu Informasi Dan Transaksi Elektronik (Ite)." (8).