Nama : Ridho Ilham Renaldo
NIM : 09011181520021
Keamanan Jaringan Komputer

Network Security : ***Malware Trojan***

1.1. Pengertian Trojan :

Trojan Horse merupakan jenis malware yang memiliki sifat seperti kuda Trojan. Trojan dapat berupa program apapun yang menyerupai program yang sah, namun didalamnya memiliki beberapa kode berbahaya. Jenis ini merupakan kode non-replikasi dan umumnya bersifat parasit karena membutuhkan sebuah program yang sah untuk menyembunyikan diri. Trojan merupakan sebuah perangkat lunak yang berdiri sendiri yang tidak menempelkan dirinya ke program lain atau menyebarkan dirinya melalui jaringan. Sebuah Trojan Backdoor, setelah diinstal dapat memungkinkan hacker untuk mengakses secara remote terhadap komputer yang telah terinfeksi. Penyerang setelah itu dapat melakukan berbagai tindakan pada komputer yang terkena, dari mulai mencuri informasi sampai menggunakan komputer untuk mengirimkan SPAM.

1.2.Fungsi Trojan

- Modifikasi file (merusak, menghapus file).
- Pencurian file (mengirim dan mengambil file).
- Menjalankan program aplikasi tersembunyi.
- Memanfaatkan penggunaan koneksi internet korban.
- Melakukan penyadapan komputer korban.
- Mengggunakan komputer korban untuk melancarkan serangan ke komputer lain.
- Merusak komputer korban

Nama : Ridho Ilham Renaldo
NIM : 09011181520021
Keamanan Jaringan Komputer

3.1.Cara Kerja Trojan

Memanfaat koneksi client – server melalui port tertentu.

4.1 Jenis – Jenis Trojan

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- Convert Channel Trojan
- Botnet Trojan
- Proxy Trojan
- Remote Access Trojan
- Malware Trojan
- FTP Trojan
- GUI Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-Banking Trojan
- Notification Trojan
- Mobile Trojan

Nama : Ridho Ilham Renaldo
NIM : 09011181520021
Keamanan Jaringan Komputer

5.1.Sumber Trojan

- ICQ.
- IRC (Internet Relay Chat).
- Email Attachment.
- Physiccal Access.
- Internet Browser.
- Software & Website Palsu.

2.1. Pembahasan

Adapun pembahasan ini terfokus pada ***Malware Trojan***. Dimana Malware adalah singkatan dari Malicious Ware yang berarti perangkat lunak yang dirancang untuk mengganggu kerja dari sebuah sistem komputer. Perangkat lunak ini diperintahkan untuk melakukan perubahan diluar kewajaran kerja dari sistem komputer. Malware biasanya menyusup pada sistem jaringan komputer tanpa diketahui oleh pemilik jaringan komputer, dari jaringan komputer ini malware tersebut akan memasuki sebuah sistem komputer. Pemilik komputer juga tidak mengetahui bahwa komputernya telah disusupi oleh malware. Tujuan seseorang untuk menyusupkan program jahat bermacam-macam, yaitu: mulai hanya sekedar iseng ingin mencoba kemampuan, merusak data, mencuri data, sampai menguasai computer orang lain dan mengendalikannya dari jarak jauh melalui jaringan komputer. Bentuk Malware ini dapat muncul dalam bentuk kode dieksekusi (exe), script, konten aktif, dan perangkat lunak lainnya.

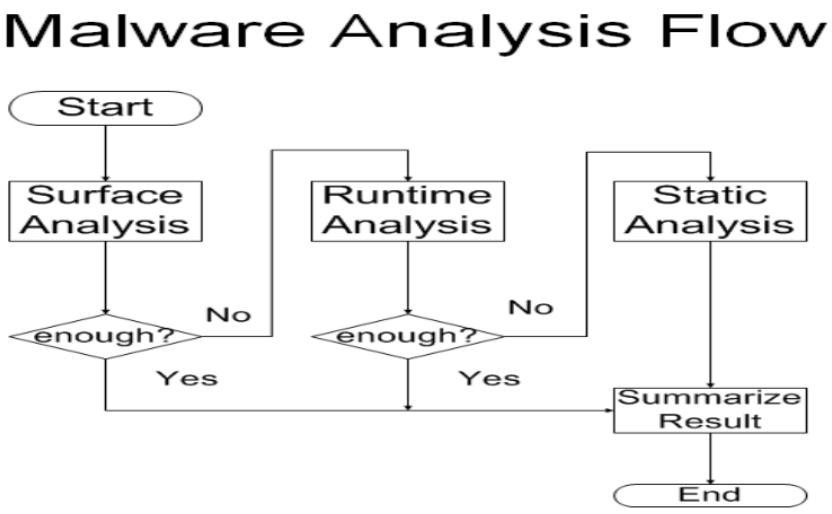
Untuk Analisis malware adalah proses yang biasa dilakukan seoran analis malware untuk menginvestigasi karak- teristik dan perilaku malware. Analisa atau kajian ini sangat penting untuk dilakukan karena :

- Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya-sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika.
- Malware sering diselipkan didalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu, sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan.

Nama : Ridho Ilham Renaldo
NIM : 09011181520021
Keamanan Jaringan Komputer

- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan. - Malware sering dikembangkan agar dapat menularkan dirinya ke tempat-tempat lain, dengan cara kerja seperti virus atau worms, sehingga komputer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya.
- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.

Berikut ini adalah Malware Analysis Flow :



Yang Menjelaskan mengenai ***'Metode surface* analysis'** yang artinyaSe memeriksa file dari luar, memiliki ciri bahwa pemeriksaan pada tahap ini tidak melakukan eksekusi terhadap file yang diperiksa sehingga file tidak diaktifkan. Sesuai dengan namanya "surface" maka pemeriksaan tahap ini hanya memeriksa file dari permukaan saja sehingga informasi yang didapatkan juga terbatas.

Pemeriksaan file melalui metode surface analysis mampu memberikan informasi seperti jenis file asli yang diperiksa, ukuran file sebenarnya, file lain pada file yang diperiksa. Surface analysis mampu memberikan informasi yang akurat untuk mengetahui malware yang menyamar dengan menjadi icon atau ekstensi lain. Dari pemeriksaan ini juga didapatkan hash function atau

fingerprint (MD5, SHA-1, dll) sebagai identitas unik dari file yang diperiksa, biasanya fingerprint inilah yang digunakan oleh antivirus untuk mendeteksi malware. Informasi yang didapatkan dari surface analysis sudah bisa memberikan gambaran bila file yang kita periksa termasuk malware atau file biasa. Meski demikian diperlukan informasi yang lebih detail untuk memberikan keterangan lebih lengkap mengenai file yang diperiksa. Beberapa tools yang digunakan pada metode surface analysis adalah HashTab dan digest.exe (Hash Analysis), TrID (File Analysis), BinText dan strings.exe (String Analysis), HxD (Binary Editor), CFF Explorer (Pack Analysis), dan 7zip (Archiver).

Selain metode Surface Analysis ada Pada **'Metode Runtime Analysi'** ini sebuah file yang diperiksa akan diaktifkan untuk selanjutnya mampu dikumpulkan informasi mengenai dampaknya terhadap komputer ketika file malware menjalankan prosesnya. Sehingga bisa diketahui kegiatan apa saja yang dilakukan oleh malware saat berhasil menginfeksi sebuah komputer. Tahapan runtime analysis akan memeriksa komputer dengan secara keseluruhan seperti proses yang berjalan di komputer, perubahan registry, aktivitas komunikasi internet dan peristiwa janggal lainnya yang biasa terjadi ketika sebuah komputer terinfeksi malware. Melakukan aktivitas malware di dalam komputer tergolong cukup sulit karena biasanya malware memiliki proses dengan nama yang sama seperti proses default yang ada di sistem operasi. Terlebih lagi malware kerap menyembunyikan dirinya di dalam komputer sehingga sulit untuk bisa menemukannya. Meski demikian biasanya malware memiliki ciri yang unik dengan menjalankan aktivitas yang tidak biasa dan berbeda dengan program lainnya. Berikut beberapa aktivitas khas yang dilakukan malware: 1. Modifikasi (mengubah, menghapus, merusak) file yang ada di komputer. 2. Mengubah registry. 3. Melakukan upaya untuk koneksi internet. 4. Mematikan proses antivirus dan firewall. Analisis pada metode runtime haruslah sangat peka dan disarankan agar kita mengetahui kondisi default pada komputer , sehingga bila ada perubahan sekecil apapun yang diakibatkan oleh malware maka dapat dengan mudah untuk langsung diketahui. Beberapa tools yang digunakan untuk Runtime Analysis : Process Explorer, Regshot, Wireshark, TCPView, Process Monitor, FUNdelete, Autoruns, Streams/ADSSpy. Tools pada server untuk membuat simulasi serangan malware secara lebih nyata menggunakan tools seperti: FakeDNS, netcat/ncat, tcpdump/tshark.

Selanjutnya malware akan dianalisa dengan menggunakan metode Static Analysis. Metode ini seperti kegiatan testing pada perangkat lunak secara white box. Pada Static Analysis kita akan melihat secara langsung source code yang dituliskan pada program malware tersebut. Sehingga informasi yang didapatkan sangatlah lengkap dan bisa memberikan gambaran yang sangat detail tentang mekanisme kerja malware tersebut secara keseluruhan. Meski demikian sebagai sebuah file yang sudah terkompilasi maka kita tidak bisa untuk melihat source code sebagai sebuah bahasa pemrograman yang utuh. Karena executable file akan berbentuk binary code sehingga yang bisa dilakukan adalah mengubahnya menjadi berbentuk assembly code (bahasa mesin)

Selanjutnya adalah Metode Static Analysis membutuhkan ahli yang mampu memahami bahasa mesin terutama arsitektur sebuah program. Lebih baik lagi seorang ahli yang sudah terbiasa memahami struktur malware sehingga bisa langsung membuat gambaran pasti cara kerja malware

dari bahasa mesin tersebut. Terapan dari Static Analysis mampu memberikan informasi detail untuk kegiatan tahap lanjut yaitu kegiatan reverse engineering. Contoh tools untuk Static Analysis : IDA Pro (Disassembler); Hex-Rays, .NET Reflector, and VB Decompiler (Decompiler); MSDN Library, Google (Library); OllyDbg, Immunity Debugger, WinDbg/Syser (Debugger); HxD, WinHex, 010editor (Hex Editor); Python, Linux Shell/Cygwin/MSYS (Others Programming

3.1 Daftar Pustaka

[1] P. Insiden and B. Csirt, “Panduan penanganan insiden,” pp. 1–39, 2014.

[2] P. Richardus and E. Indrajit, “Analisa Malware.”