Nama : Ratih Gustifa
NIM : 09011281320007
Tugas : Keamanan Jaringan Komputer

# MALWARE

*Malware* ini sebenarnya memiliki nama lengkap *malicious software*. Malware adalah istilah umum yang digunakan untuk software atau program yang dirancang bertujuan menyusup atau merusak sebuah sistem komputer secara diam-diam. Sekali lagi, istilah *malware* ini tidak begitu akrab di telinga sebagian pengguna internet.

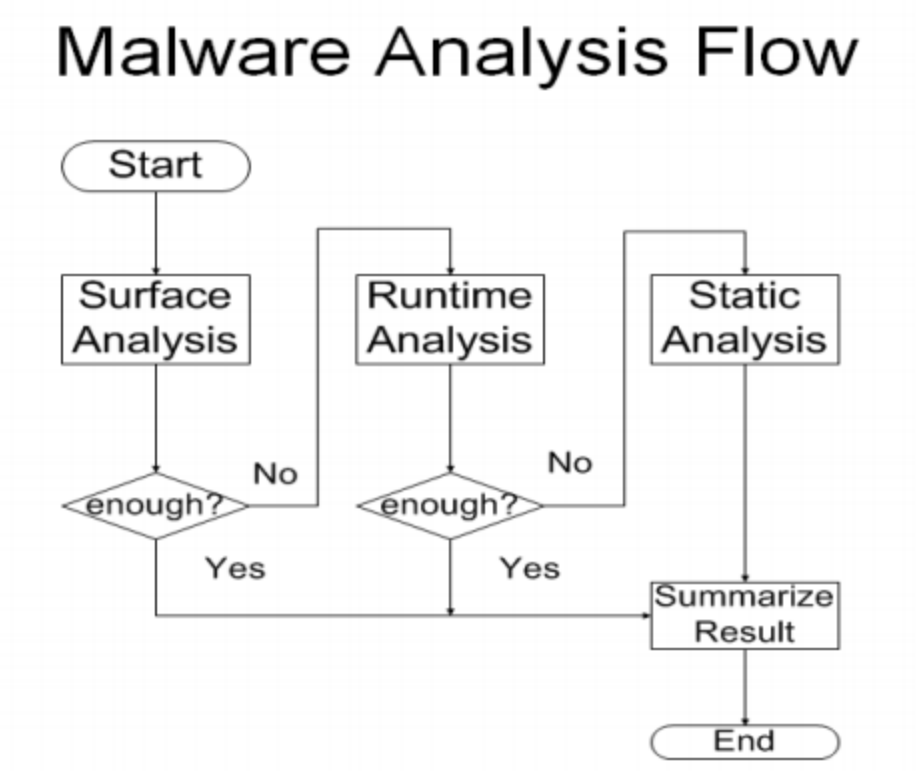
Dalam bahasa kita sehari-hari kita lebih sering menyebut *virus* meskipun sebenarnya kurang tepat, media massa bahkan sangat sering menggunakan istilah ini. Sebuah software disebut sebagai malware lebih karena faktor tujuan pembuatannya, daripada fitur-fitur khusus yang dimilikinya. Malware mencakup **virus**, **worm**, **trojan horse**, sebagian besar *rootkit*, *spyware*, *adware* yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

Berdasarkan sifat dan tujuannya malware dikategorikan ke dalam tiga kelompok.

- Kelompok pertama adalah malware yang menginfeksi komputer, yakni virus dan worm
- Kelompok kedua adalah malware yang bersembunyi (bergerilya) di dalam komputer, antara lain *trojan horse*, *rootkit*, dan *backdoor*
- Kelompok ketiga adalah malware yang mencari dan mencuri keuntungan, yaitu spyware, adware yang tidak jujur, *botnet*, *keystroke logger* dan *dialer*.

'Malware" adalah program komputer yang di ciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari software. Umumnya Malware diciptakan untuk membobol atau merusak suatu software atau operating sistem.

Cara mendeteksi malware adalah :



Nama : Ratih Gustifa
NIM : 09011281320007
Tugas : Keamanan Jaringan Komputer

## SURFACE ANALISIS

Metode surface analysis adalah 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).

## RUNTIME ANALYSIS

Pada metode runtime analysis 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.

Nama : Ratih Gustifa
NIM : 09011281320007
Tugas : Keamanan Jaringan Komputer

## STATIC ANALYSIS

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)

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

## KEGIATAN SETELAH MELAKUKAN MALWARE ANALYSIS

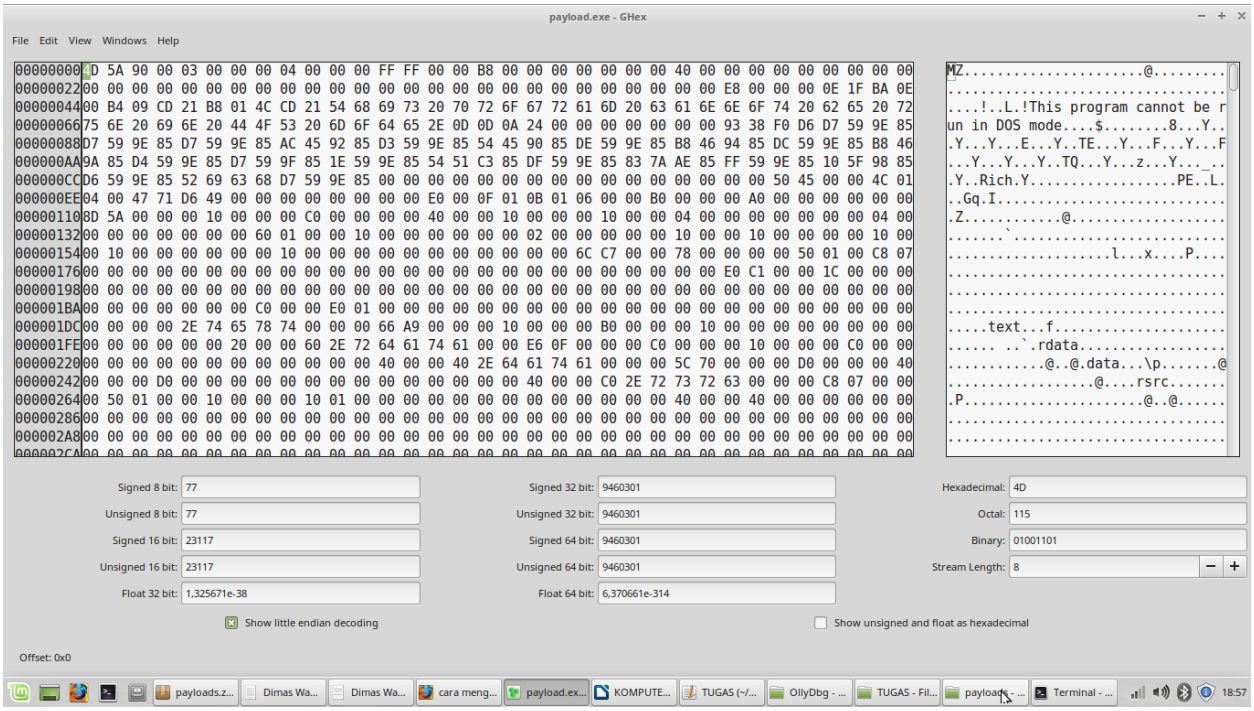
Setelah serangkaian tahapan dan metode Malware Analysis sudah dilakukan. Maka dapat dilakukan penyusunan informasi mengenai malware yang diperiksa tersebut. Sekiranya beberapa hal yang bisa menjadi fokus kegiatan setelah melakukan Malware Analysis adalah sebagai berikut [1].

1. Final Conclusion, membuat kesimpulan akhir apakah file yang diperiksa merupakan malware atau hanya file biasa.
2. Mengklasifikasikan malware tersebut berjenis apa.
3. Membuat informasi secara umum dan detail mengenai malware yang diperiksa seperti tipe file, fingerprint dan informasi lainnya yang diusahakan dicari sebanyakbanyaknya terutama yang bersifat spesifik sehingga bisa menjadi semacam indikasi bagi pengguna komputer lain. Tampilan informasi secara umum kemudian mendetail akan memudahkan pengguna awam tentang informasi mengenai malware.
4. Membuat daftar dampak yang ditimbulkan oleh malware bila berhasil menginfeksi komputer dari hasil Malware Analysis (terutama dari metode Runtime Analysis dan Static Analysis). Dampak yang dituliskan termasuk pula perubahan spesifik yang dilakukan oleh malware (registry, file, proses komputer).
5. Memberikan informasi tentang celah bagaimana akhirnya malware dapat menyerang komputer dan sertakan juga cara penanganan atau penyelesaian agar bisa terhindar dari malware tersebut. Berikan rekomendasi untuk menghindari malware tersebut dan indikasi mengenai keberadaan malware tersebut di dalam komputer.

Nama : Ratih Gustifa
NIM : 09011281320007
Tugas : Keamanan Jaringan Komputer

6. Membuat sebuah pusat data yang menyimpan informasi tentang seluruh malware yang pernah dilakukan analisis beserta hasil kesimpulan analisisnya sehingga nantinya bisa menjadi pustaka atau referensi bagi penelitian selanjutnya. 7. Malware Analysis bisa dilanjutkan untuk kegiatan reverse engineering atau menjadi bahan penelitian untuk membuat antivirus.

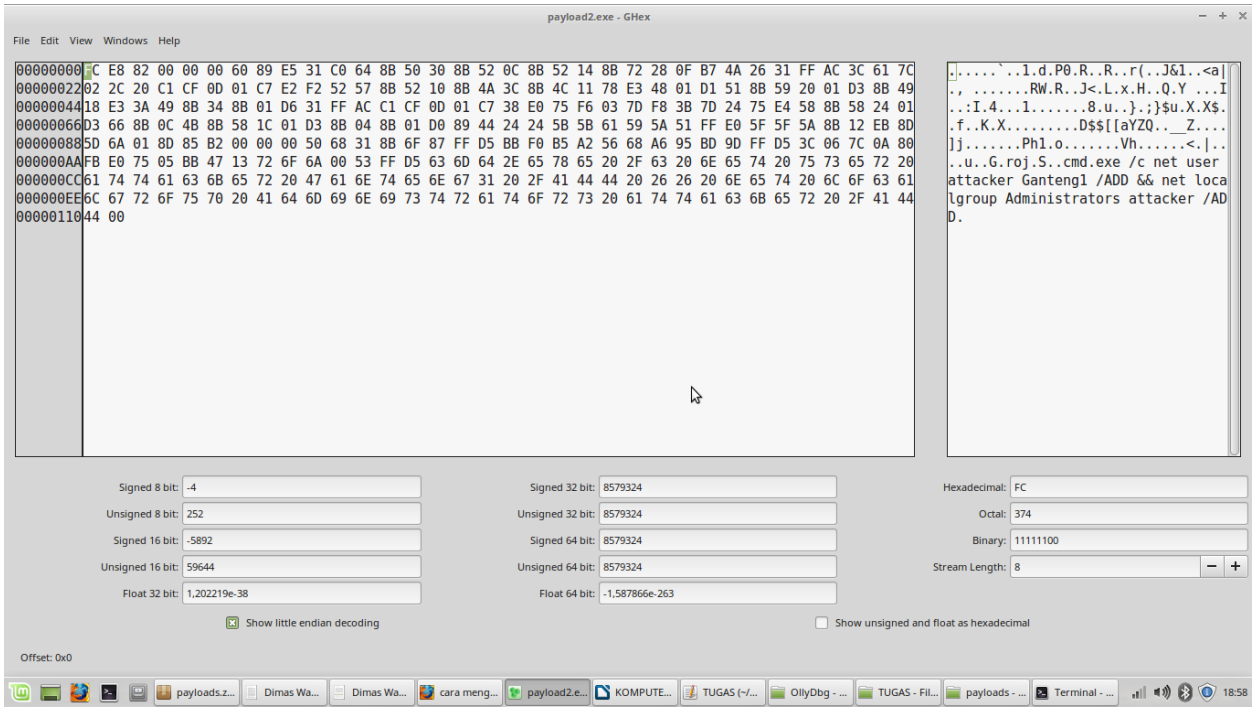
## Percobaan Payload
## Tool : ghex



Nama : Ratih Gustifa
NIM : 09011281320007
Tugas : Keamanan Jaringan Komputer

## Percobaan Payload2

## Tool : Ghex




## DAFTAR PUSTAKA


[1] M. F. Agung, “Konsep Dasar Malware Analysis,” 2011.

[2] http://www.catatanteknisi.com/2011/12/pengertian-jenis-jenis-malware.html