Nama : Muhamad Yusup
NIM : 09011281419061

"Malware Threat"

Modus operandi kejahatan di dunia cyber sangatlah beragam dan bervariasi. Teknik yang dipergunakan oleh para kriminal pun semakin lama semakin mutakhir dan kompleks. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai "malicious software" atau "malware" – yang dalam terjemahan bebasnya adalah program jahat (karena sifatnya yang merusak atau bertujuan negatif).

Malware merupakan salah satu masalah bagi dunia keamanan komputer. Perkembangannya yang sangat pesat dari tahun ke tahun menjadi tantangan tersendiri bagi para praktisi keamanan. Varian yang baru semakin banyak muncul sehingga keberadaan program antivirus kadang tidak dapat mengantisipasi sepenuhnya. Oleh karena itu, kemampuan untuk menganalisis malware tetap diperlukan terutama bagi organisasi yang mengandalkan sistem komputerisasi dalam operasi bisnisnya.

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik. 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 di dalam 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;
- 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.
  Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan

tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan.

1. Surface Analysis.

Sesuai dengan namanya, "surface analysis" adalah suatu kajian pendeteksian malware 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.

2. Runtime Analysis.

Pada dasarnya ada kesamaan antara runtime analysis dengan surface analysis, yaitu keduanya sama-sama berada dalam ranah mempelajari ciri-ciri khas yang selayaknya ada pada sebuah program yang normal. Bedanya adalah bahwa dalam runtime analysis, dipersiapkan sebuah prosedur dan lingkungan untuk mengeksekusi atau menjalankan program yang dicurigai mengandung atau sebagai malware tersebut.

3. Static Analysis.

Dari ketiga metode yang ada, static analysis merupakan model kajian yang paling sulit dilakukan karena sifat analisanya yang "white box" alias pengkajian melibatkan proses melihat dan mempelajari isi serta algoritma program malware dimaksud, sambil mengamati sekaligus menjalankan/mengeksekusinya.

Malware sendiri terdiri dari beberapa jenis :

a) Virus

Virus adalah salah satu sebutan dari malware, dan Malware belum tentu virus. Tapi virus sudah pasti adalah malware. Virus dapat menyebar dan berkembang didalam system komputer, kemudian ada beberapa virus yang tidak terasa dampaknya pada system dan juga ada salah satu yang dampaknya besar. Contohnya dampak yang terasa adalah berkurangnya ruang memory atau hardisk

b) Worm

Worm hampir sama dengan virus yang dapat memperbanyak diri, tetapi bedanya worm itu sifatnya jinak, jadi tidaklah terlalu berbahaya

c) Trojan

Jenis malware ini merupakan program tersembunyi yang menyamar sebagai program atau aplikasi yang seolah-olah berguna bagi sang pemakai. Padahal didalm program tersebut terdapat malware lain seperti Worm dan Virus yang tujuannya untuk merusak system. Bahakan yang lebih berbahaya lagi, jika didalam Trojan telah diisi "Spyware" yang nantinya dapat digunakan untuk mencuri data, contohnya seperti password

d) Spyware

Spyware yang berarti mata-mata adalah sebuah program yang berfungsi untuk mengintip data pada perangkat yang terinfeksi. Data tersebut bisa berupa Password dll. Yang berarti tujuannya untuk membobol akun yang telah diketahui passwordnya.

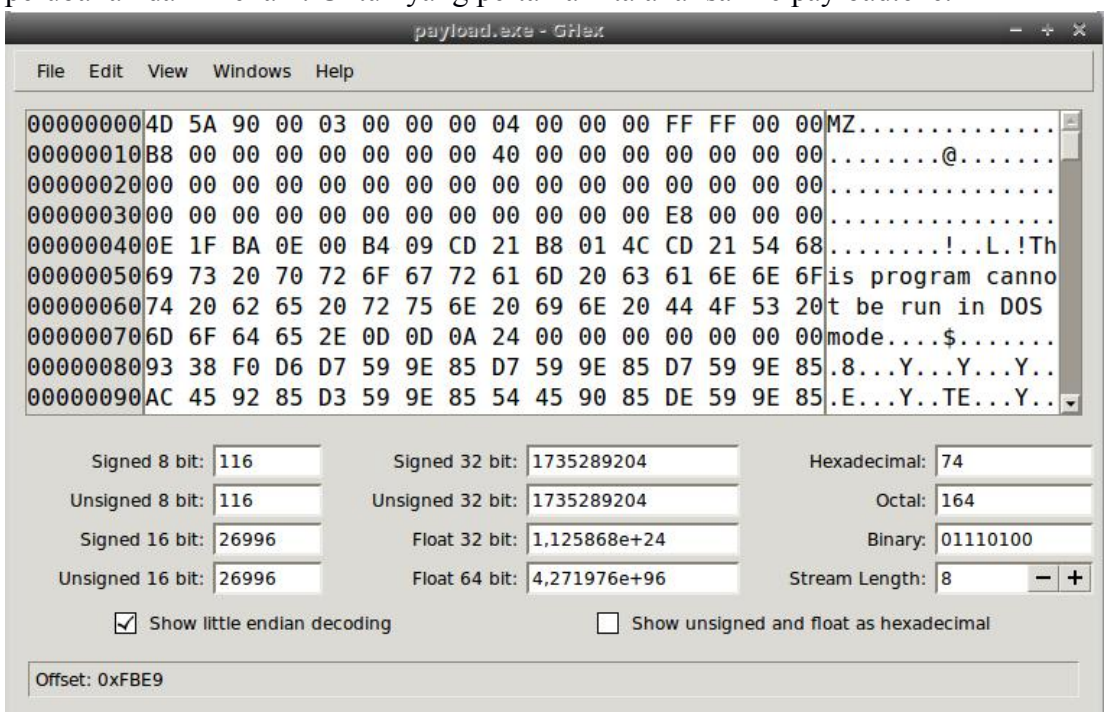
Dan masih banyak lagi jenis malware itu sendiri, contohnya Backdoor, Hijacker, Botnet, Dialer, Rootkit, Adware, Wabbit dan lainnya.

Dalam tugas ini, ada dua file yang akan dilakukan analisa apakah tergolong ke dalam sebuah malware, atau bukan. Analisa dilakukan dengan menggunakan sebagian dari tools yang biasa digunakan dalam analisis statis dasar.

Beberapa tools yang dapat digunakan diantaranya Ghex, hexdump, strings, ollydbg, serta IDA pro yang beberapa berjalan dalam sistem operasi linux, dan sebagian di windows.

Gambar 1. *File payload yang akan dianalisa*

Untuk tahapan awal dalam melakukan analisa, kita bisa melihat file signature yang terdapat di dalam software tersebut, apakah benar file tersebut memiliki ekstensi yang sesuai dengan yang terlihat, atau justru file tersebut merupakan perubahan dari file lain. Untuk yang pertama kita analisa file payload.exe.



Gambar 2. *Penggunaan tools Ghex*

Dari hasil analisa tersebut didapat sebuah signature MZ yang jika ditelusuri merupakan signature file dari file ekstension .exe, hal ini sesuai dengan list of file signature yang ada pada website wikipedia sebagai parameter untuk melihat ekstensi file.

lz	lzip compressed file	0	LZIP	4C 5A 49 50
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
zip jar odt ods odp docx xlsx pptx	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive)

Gambar 3. *List of file signature dari Wikipedia*

Ada sebuah string menarik dalam hasil analisis file signature yang dilakukan dalam Ghex, yakni adanya beberapa string yang menunjukkan identitas file yang sebenernya, kemudian kita lakukan analisa lebih jauh menggunakan string untuk mendeteksi apakah benar ada malware yang tertanam di dalam file tersebut, dan jika ada, apa yang bisa terjadi jika program tersebut di running di dalam sistem.

```
gray-CA10AB payloads # strings payload.exe > payload.txt
```

Gambar 4. *Penggunaan tools Strings*

Dari hasil analisa tersebut, di dapat beberapa word yang readable sehingga bisa kita analisa seperti printf, signal, malloc, calloc, fflush, fclose, dan perror yang merupakan fungsi-fungsi standar di dalam library. Namun ada satu strings yang menarik di dalamnya, yakni seperti pada gambar di bawah ini :

```
 Licensed to The Apache Software Foundation, http://www.apache.org/<br>
 Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
 This is ApacheBench, Version %s <i>&lt;%s&gt;</i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
    -h              Display usage information (this message)
    -r              Don't exit on socket receive errors.
    -e filename     Output CSV file with percentages served
    -g filename     Output collected data to gnuplot format file.
    -S              Do not show confidence estimators and warnings.
    -d              Do not show percentiles served table.
    -k              Use HTTP KeepAlive feature
    -V              Print version number and exit
    -X proxy:port   Proxyserver and port number to use
    -P attribute    Add Basic Proxy Authentication, the attributes
                    are a colon separated username and password.
    -A attribute    Add Basic WWW Authentication, the attributes
                    Inserted after all normal header lines. (repeatable)
    -H attribute    Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
    -C attribute    Add cookie, eg. 'Apache=1234. (repeatable)
    -z attributes   String to insert as td or th attributes
    -y attributes   String to insert as tr attributes
    -x attributes   String to insert as table attributes
```

Gambar 5. *Hasil Analisa Menggunakan Strings*

Ada beberapa strings yang menunjukkan bahwa program payload merupakan file master apache, dalam penelusuran menggunakan website www.virustotal.com didapatkan bahwa file merupakan file apache.

FileVersionInfo properties

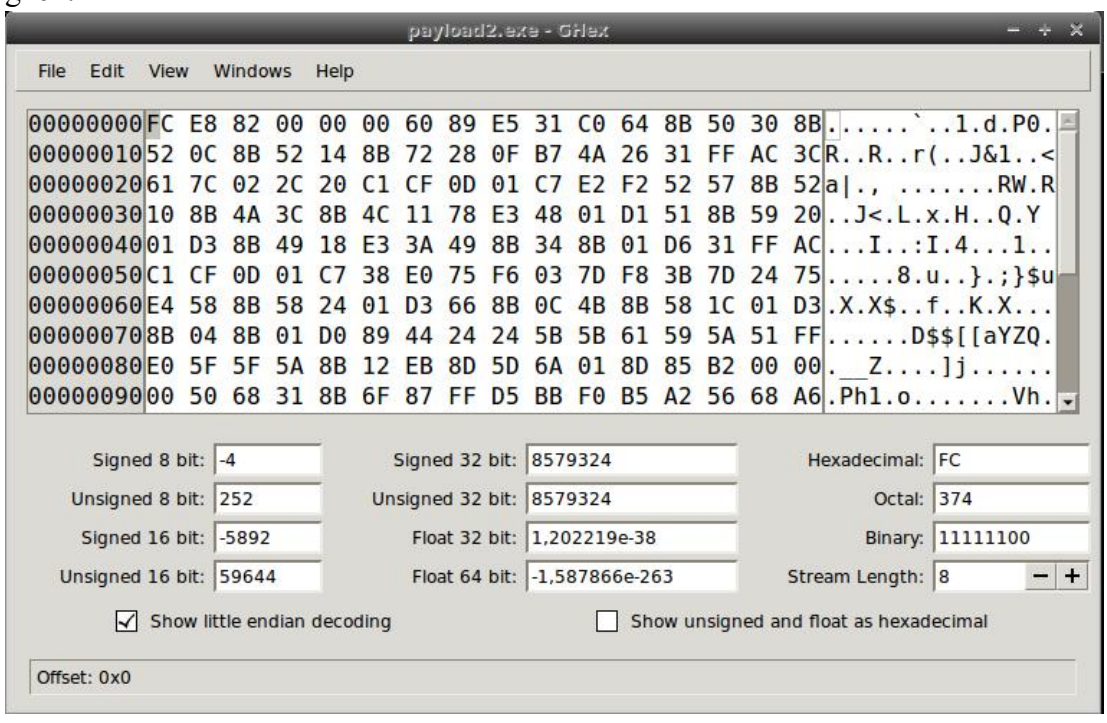
Copyright	Copyright 2009 The Apache Software Foundation.
Product	Apache HTTP Server
Original name	ab.exe
Internal name	ab.exe
File version	2.2.14
Description	ApacheBench command line utility
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Gambar 6. *File Version Info*

Di website tersebutpun kita dapat melakukan analisa virus yang terkandung di dalam program *payload.exe* dengan rujukan beberapa database dari antivirus yang ada, dari hasil analisa melalui website tersebut didapatkan adanya Gen:Variant.Trojan.Metasploit.1, Trojan/Win32.Shell.R1283, Win32.Trojan.Wisdom Eyes.16070401.9500.9999, dan beberapa jenis trojan lainnya.

Virus trojan disisipkan ke dalam software kemudian menjadikan software tersebut sebagai jalan untuk masuk dan menjadikan komputer tersebut menjadi korban dalam virus trojan horse.

Kemudian kita lakukan analisa terhadap file payload2.exe, dengan tahapan yang sama dengan sebelumnya, kita lakukan analisa signature file menggunakan tools ghex.



Gambar 7. *Analisa payload2.exe menggunakan ghex*

Dari analisa tersebut kita mendapatkan bahwa file tersebut mengandung sebuah metasploit, lebih jelasnya, kita lakukan analisa menggunakan tools strings,

Gambar 8. *Analisa payload2.exe menggunakan strings*

Dari hasil analisa menggunakan strings, kita bisa melihat adanya sebuah kode readable yang akan menambahkan user ke dalam sebuah sistem dengan sebuah hak akses administrator. Maka ketika program ini berjalan di dalam komputer, attacker akan mendapatkan hak akses admin di dalam sistem. Hal ini jelas akan membahayakan dari sisi keamanan sistem yang dibuat.

Demikian salah satu penerapan dan analisa malware dengan jenis trojan serta cara kerja nya di dalam sistem yang mampu mendesablekan, menambahkan, bahkan menghapus file-file penting di dalam komputer.