Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

ANALISA MALWARE

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.

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.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan. Ketiga pendekatan dimaksud akan dijelaskan dalam masing-masing paparan sebagai berikut :

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. Analisa ini memiliki ciri-ciri sebagai berikut :

- Program yang dikaji tidak akan dijalankan, hanya akan dilihat "bagian luarnya" saja (sebagai analogi selayaknya orang yang ingin membeli buah-buahan, untuk mengetahui apakah buah yang bersangkutan masih mentah atau sudah busuk cukup dengan melihat permukaan kulitnya, membauinya, dan meraba-raba tekstur atau struktur kulitnya). Dari sini akan dicoba ditemukan hal-hal yang patut untuk dicurigai karena berbeda dengan ciri khas program kebanyakan yang serupa dengannya.
- Sang pengkaji tidak mencoba untuk mempelajari "source code" program yang bersangkutan untuk mempelajari algoritma maupun struktur datanya (sebagaimana layaknya melihat sebuah kotak hitam atau "black box".

Saat ini cukup banyak aplikasi yang bebas diunduh untuk membantu melakukan kegiatan surface analysis ini, karena cukup banyak prosedur kajian yang perlu dilakukan, seperti misalnya: 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).

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.

Model analisa ini menghasilkan kajian yang lebih mendalam karena selain dihilangkannya proses "menduga-duga", dengan mengeksekusi malware dimaksud akan dapat dilihat "perilaku" dari program dalam menjalankan "skenario jahatnya" sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.

Oleh karena itulah maka aplikasi pendukung yang dipergunakan harus dapat membantu mensimulasikan kondisi yang diinginkan, yaitu melihat ciri khas dan karakteristik sistem, sebelum dan sesudah sebuah malware dieksekusi. Agar aman, maka program utama yang perlu dimiliki adalah software untuk menjalankan virtual machine, seperti misalnya: VMWare, VirtualBoz, VirtualPC, dan lain sebagainya. Sementara itu aplikasi pendukung lainnya yang kerap dipergunakan dalam melakukan kajian ini adalah: Process Explorer, Regshot, Wireshark, TCPView, Process Monitor, FUNdelete, Autoruns, Streams/ADSSpy, dan lain-lain. Keseluruhan aplikasi tersebut biasanya dijalankan di sisi klien; sementara di sisi server-nya diperlukan FakeDNS, netcat/ncat, tcpdump/tshark, dan lain sebagainya.

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.

Karena sifat dan ruang lingkupnya yang cukup luas dan mendalam, strategi khusus perlu dipersiapkan untuk melakukan kajian ini. Disamping itu, kajian ini juga memerlukan sumber daya yang khusus – misalnya adalah SDM yang memiliki pengetahuan dan pengalaman dalam membuat serta membaca program berbahasa mesin atau rakitan (assembly language) serta ahli arsitektur dan organisasi piranti komputasi seperti komputer, PDA, tablet, mobile phone, dan lain sebagainya.

Cukup banyak aplikasi pendukung yang diperlukan, tergantung dari kompleksitas malware yang ada. Contohnya adalah: IDA Pro (Disassembler); Hex-Rays, .NET Reflector, and VB Decompiler (Decompiler); MSDN Library, Google (Library); OllyDbg, Immunity Debugger,

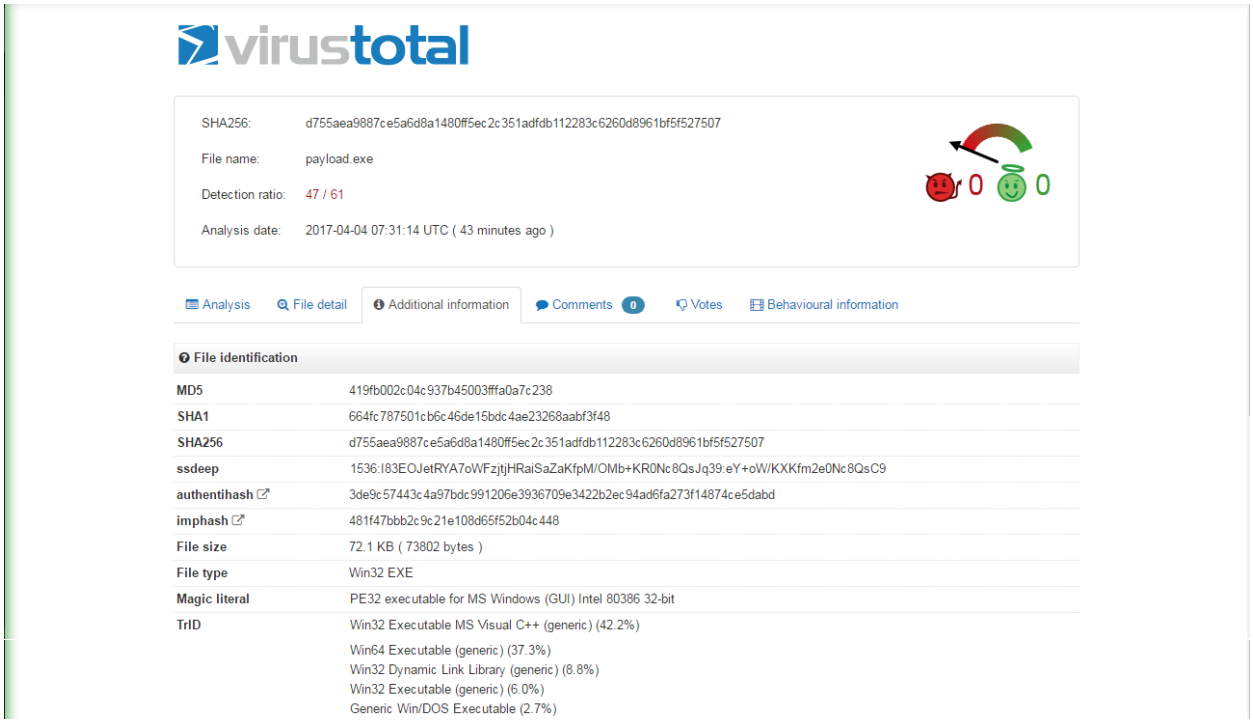
WinDbg/Syser (Debugger); HxD, WinHex, 010editor (Hex Editor); Python, Lunux Shell/Cygwin/MSYS (Others) dan lain-lain.

TUGAS :

Lakukan analisis terhadap 2 file payload : payload.exe dan payload2.exe. Analisis proses kerja dan skema dari payload tersebut, menggunakan beberapa bantuan tools seperti : ghex, hexdump, strings (linux), ollydbg (win) atau ida pro (linux,win).

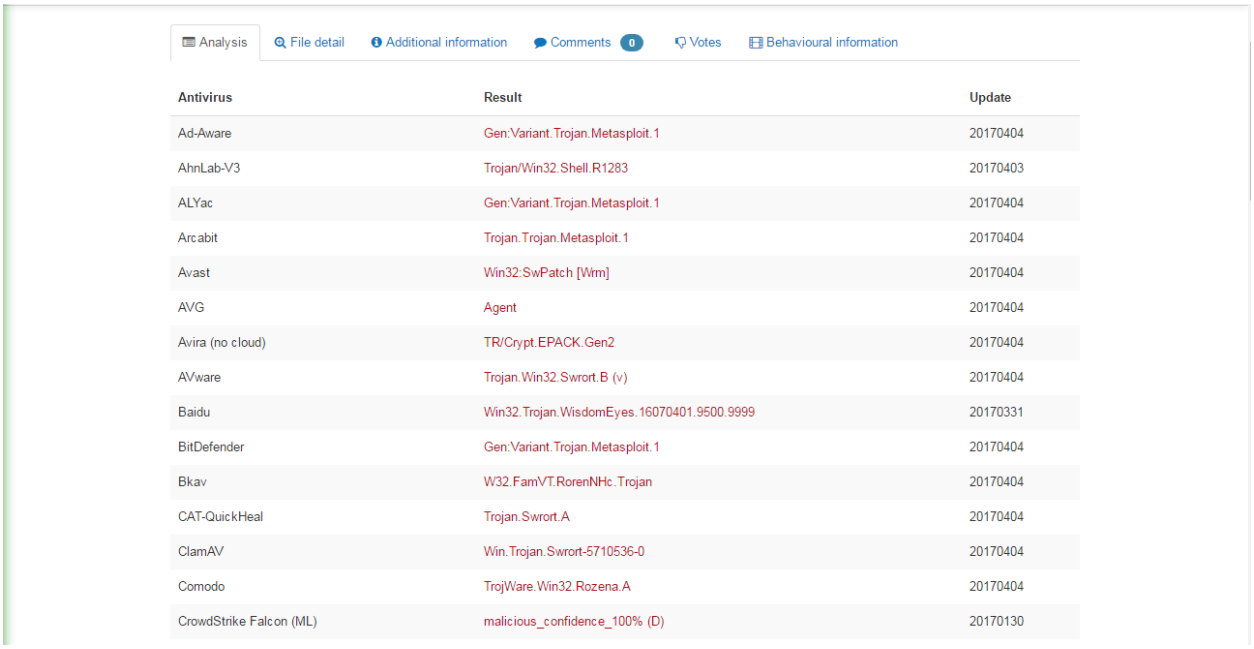
Disini saya melakukan analisis malware menggunakan metode statik dengan bantuan https://virustotal.com/ dan metode dinamik dengan bantuan strings, ghex dan ida pro.

Teknik pertama dalam analisis statis adalah mengupload executable yang mencurigakan ke https://virustotal.com/ yang menjalankan eksekusi terhadap beberapa solusi AV dan memberikan hasilnya. Seperti pada Gambar.1 dan Gambar.4 dibawah ini yang menyatakan bahwa rasio deteksi file payload.exe adalah 47 dari 61 dan rasio deteksi file payload2.exe adalah 3 dari 56.



Gambar.1 Additional Information File Payload.exe

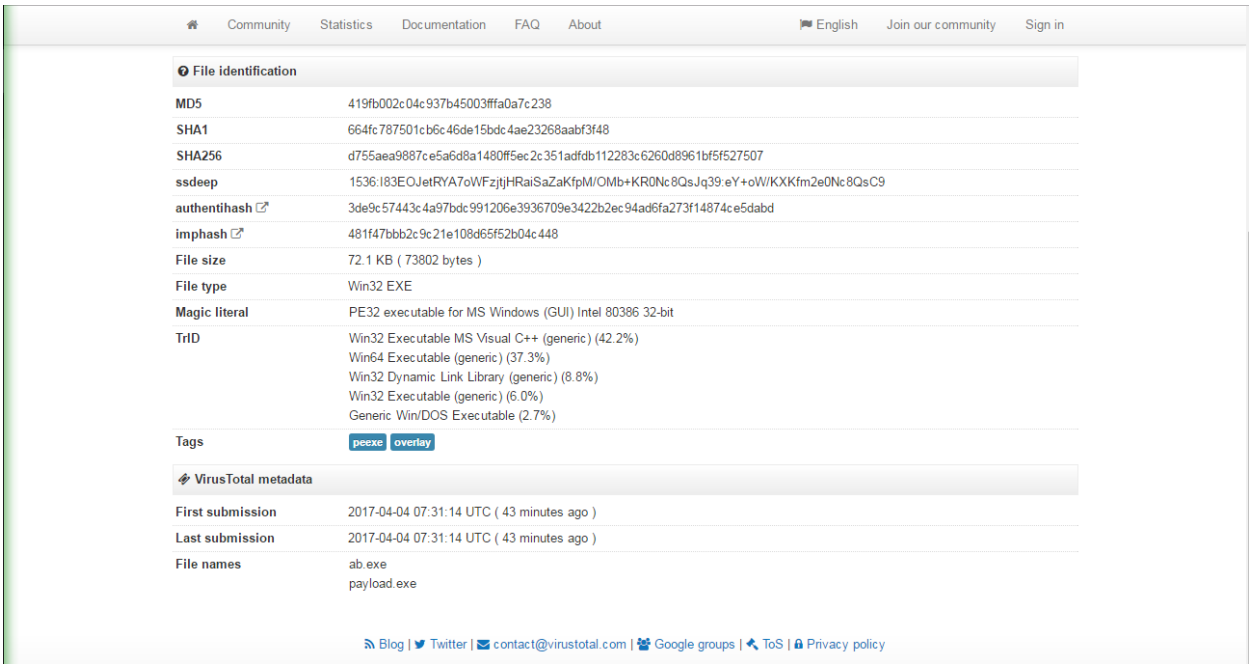
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Trojan.Metasploit.1	20170404
AhnLab-V3	Trojan/Win32.Shell.R1283	20170403
ALYac	Gen:Variant.Trojan.Metasploit.1	20170404
Arcabit	Trojan.Trojan.Metasploit.1	20170404
Avast	Win32:SwPatch [Wrm]	20170404
AVG	Agent	20170404
Avira (no cloud)	TR/Crypt.EPACK.Gen2	20170404
AVware	Trojan.Win32.Swrort.B (v)	20170404
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9999	20170331
BitDefender	Gen:Variant.Trojan.Metasploit.1	20170404
Bkav	W32.FamVT.RorenNHc.Trojan	20170404
CAT-QuickHeal	Trojan.Swrort.A	20170404
ClamAV	Win.Trojan.Swrort-5710536-0	20170404
Comodo	TrojWare.Win32.Rozena.A	20170404
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170130

Gambar.2 Analisis File Payload.exe



Community | Statistics | Documentation | FAQ | About | English | Join our community | Sign in

File identification

MD5	419fb002c04c937b45003fffa0a7c238
SHA1	664fc787501cb6c46de15bdc4ae23268aabf3f48
SHA256	d755aea9887ce5a6d8a1480ff5ec2c351adfdb112283c6260d8961bf5f527507
ssdeep	1536:I83EOJetRYA7oWFzjtjHRaiSaZaKfpM/OMb+KR0Nc8QsJq39:eY+oW/KXKfm2e0Nc8QsC9
authentihash	3de9c57443c4a97bdc991206e3936709e3422b2ec94ad6fa273f14874ce5dabd
imphash	481f47bbb2c9c21e108d65f52b04c448
File size	72.1 KB (73802 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (42.2%) Win64 Executable (generic) (37.3%) Win32 Dynamic Link Library (generic) (8.8%) Win32 Executable (generic) (6.0%) Generic Win/DOS Executable (2.7%)
Tags	peexe overlay

VirusTotal metadata

First submission	2017-04-04 07:31:14 UTC (43 minutes ago)
Last submission	2017-04-04 07:31:14 UTC (43 minutes ago)
File names	ab.exe payload.exe

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Gambar.3 Detail File Payload.exe

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

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.

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2009-04-03 20:27:51
Entry Point	0x00005A8D
Number of sections	4

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	43366	45056	7.03	27ad3b9b1595f290866fe9a0812ed638
.rdata	49152	4070	4096	5.32	25d7ceee3aa85bb3e8c5174736f6f830
.data	53248	28764	16384	4.41	283b5f792323d57b9db4d2bcc46580f8
.rsrc	86016	1992	4096	1.96	c13a9413aea7291b6fc85d75bfcde381

Overlays

MD5	95eb479e8f470740aa86bcb86cb13966
File type	data
Offset	73728
Size	74
Entropy	4.61

PE imports

[+] ADVAPI32.dll
[+] KERNEL32.dll
[+] MSVCRT.dll
[+] WS2_32.dll
[+] WSOCK32.dll

Number of PE resources by type

RT_VERSION	1

Number of PE resources by language

ENGLISH US	1

PE resources

465417d96548ce85076f6509efac41e5ad02fee2b8f712416e8b6aa08d93c494	data

Debug information

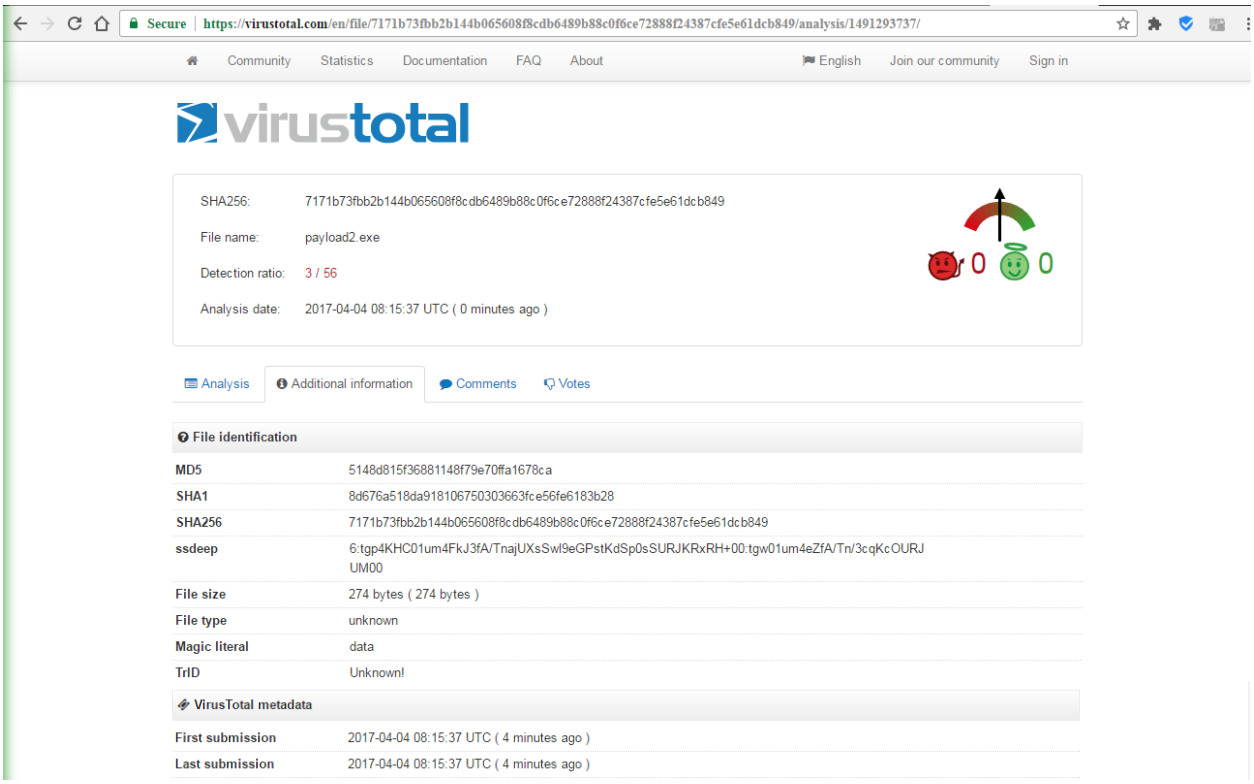
Type	Timestamp	Offset	Size
IMAGE_DEBUG_TYPE_CODEVIEW (2)	Tue Sep 29 03:34:14 2009	73728	74 Bytes

ExifTool file metadata

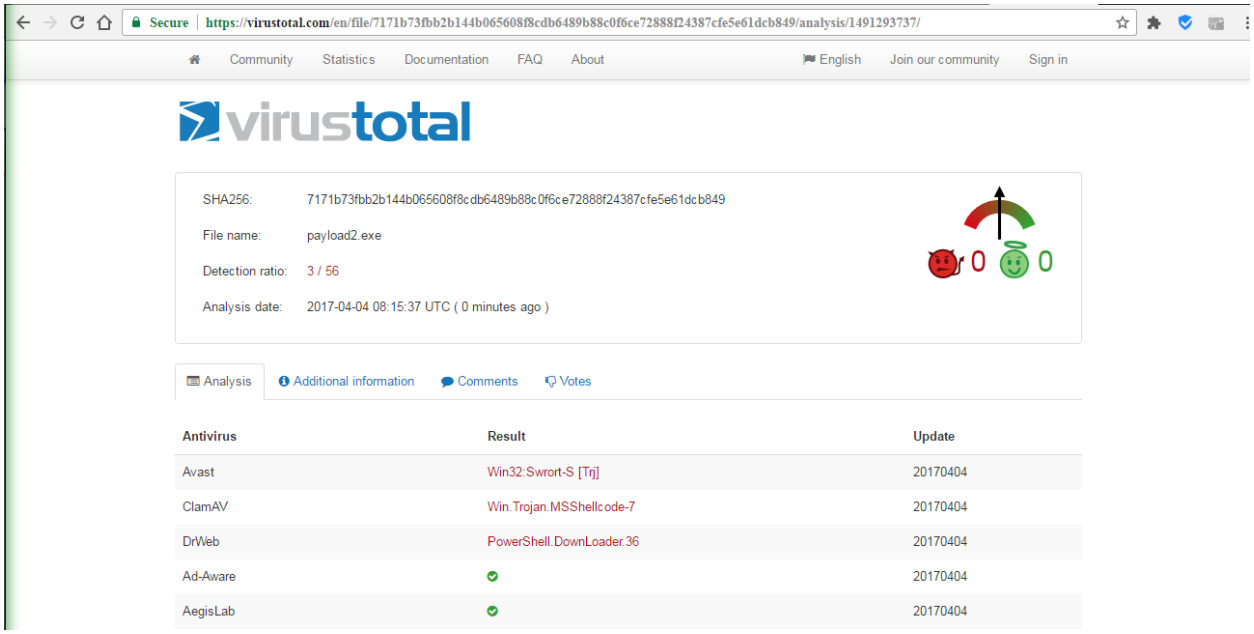
FileDescription	ApacheBench command line utility
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
InitializedDataSize	40960
ImageVersion	0.0
ProductName	Apache HTTP Server
FileVersionNumber	2.2.14.0
LanguageCode	English (U.S.)
FileFlagsMask	0x003f
CharacterSet	Unicode
LinkerVersion	6.0
FileTypeExtension	exe
OriginalFileName	ab.exe
MIMEType	application/octet-stream
Subsystem	Windows GUI
FileVersion	2.2.14
TimeStamp	2009:04:03 21:27:51+01:00
FileType	Win32 EXE
PEType	PE32
InternalName	ab.exe
SubsystemVersion	4.0
ProductVersion	2.2.14
UninitializedDataSize	0
OSVersion	4.0
FileOS	Win32
LegalCopyright	Copyright 2009 The Apache Software Foundation.
MachineType	Intel 386 or later, and compatibles
CompanyName	Apache Software Foundation
CodeSize	45056
FileSubtype	0
ProductVersionNumber	2.2.14.0
EntryPoint	0x5a8d
ObjectFileType	Executable application

Gambar.3 Behavior Information File Payload.exe

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Gambar.4 Additional Information File Payload2.exe



Gambar.5 Analisis File Payload2.exe

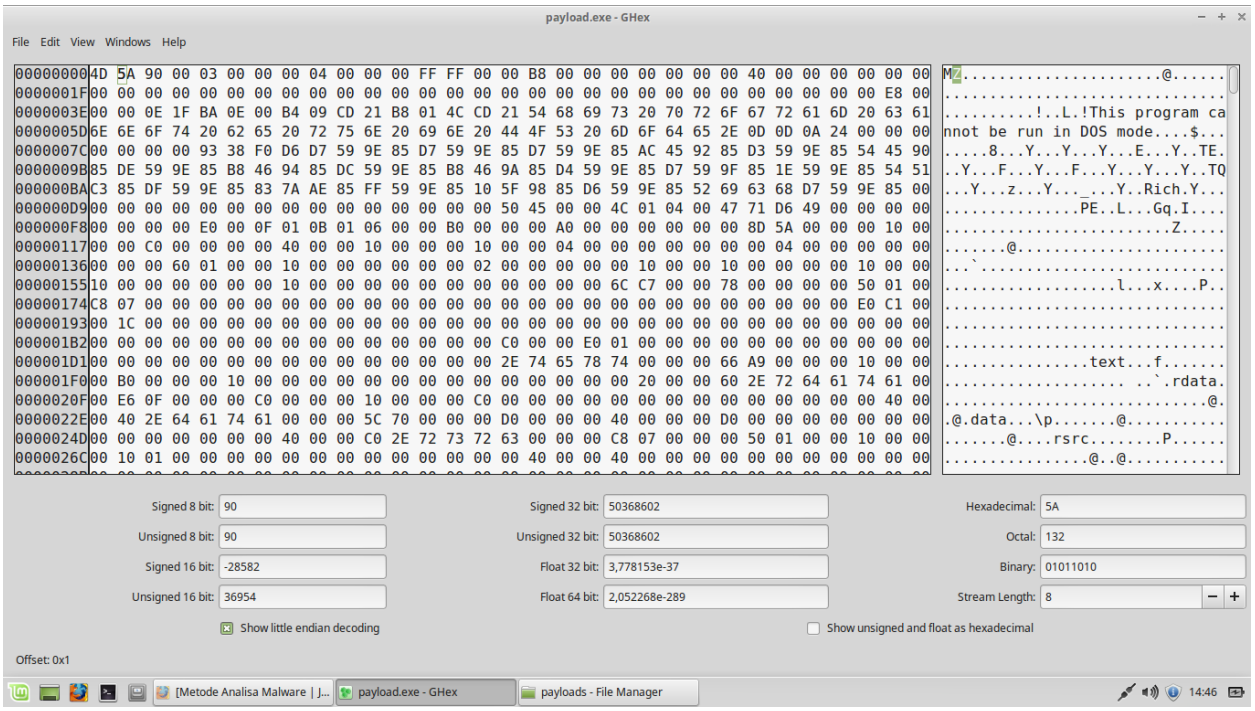
Selanjutnya pencarian menggunakan string bisa menjadi cara sederhana untuk mendapatkan petunjuk tentang fungsi dari sebuah program. Misalnya jika program mengakses URL, maka kita akan melihat URL yang diakses yang disimpan sebagai string dalam program. Menggunakan utilitas strings, file dapat dicari dengan perintah berikut : `#strings payload.exe` dan `#strings payload2.exe`. Dibawah ini adalah ekstraksi stringnya, seperti yang kita lihat hasilnya memberikan kita informasi tentang ntdll.dll, shell32, ws2_32, advapi32, kernel32. Dan pada Gambar 7 dan Gambar 8 merupakan editor hexa dari file payload.exe dan payload2.exe dengan menggunakan tool ghex.

```
leny@leny-Satellite-Pro-C640 /media/leny/AnNie Cheesers/Document/Semester 8/KJK/
TUGAS_kjk/payloads $ sudo su
[sudo] password for leny:
leny-Satellite-Pro-C640 payloads # ls
payload2.exe  payload.exe
leny-Satellite-Pro-C640 payloads # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
AH@C
8SShL@A
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
```

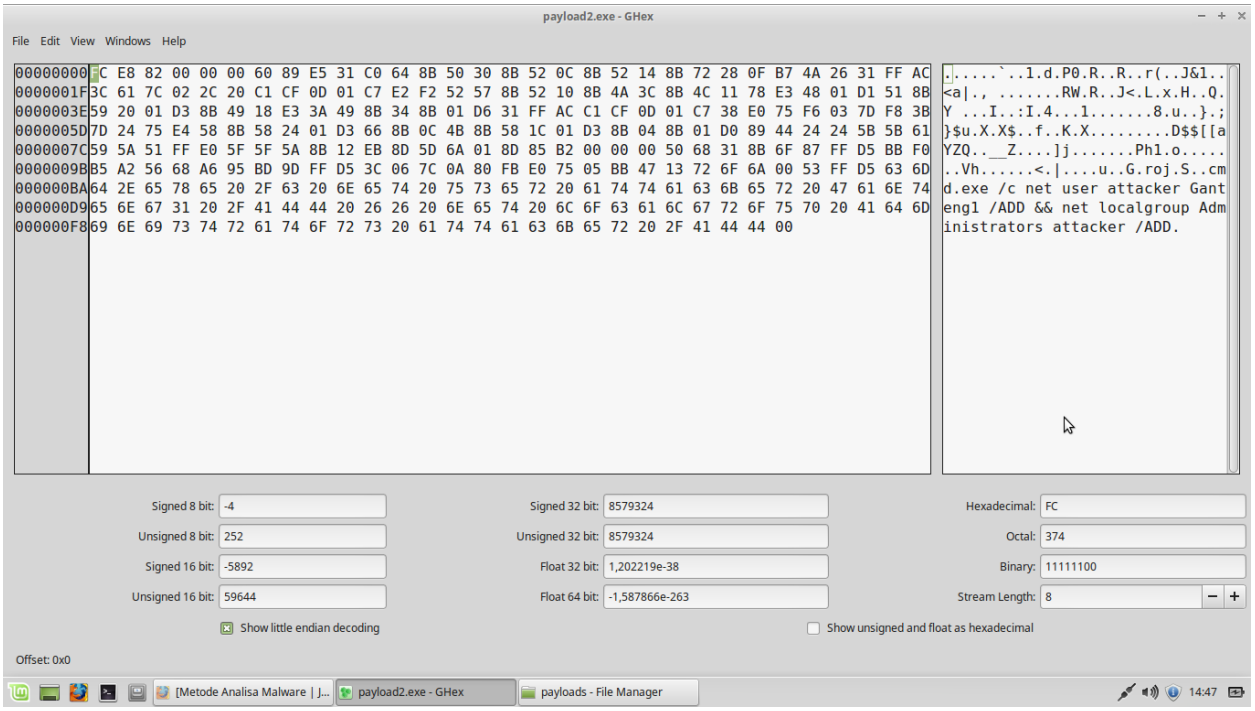
```
 Licensed to The Apache Software Foundation, http://www.apache.org/<br>
 Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
 This is ApacheBench, Version %s <i>&lt;%s&gt;</i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 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
```

Gambar.6 Hasil Ekstraksi Strings

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



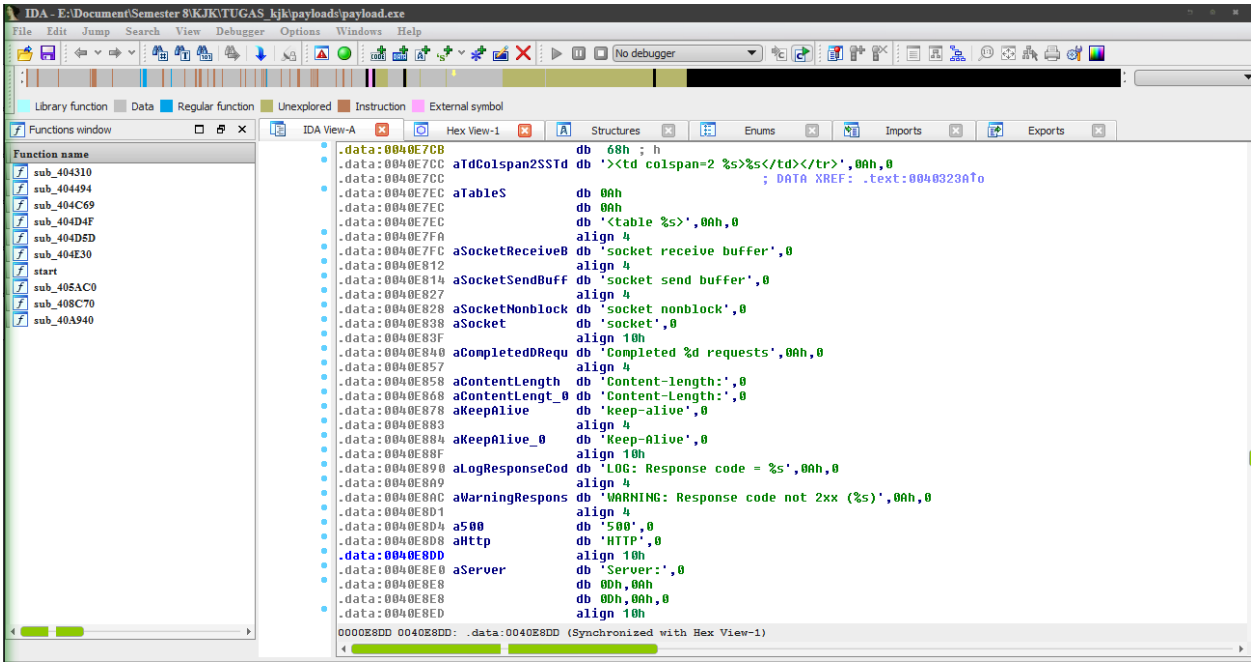
Gambar.7 Editor Hexa dari File Payload.exe



Gambar.8 Editor Hexa dari File Payload2.exe

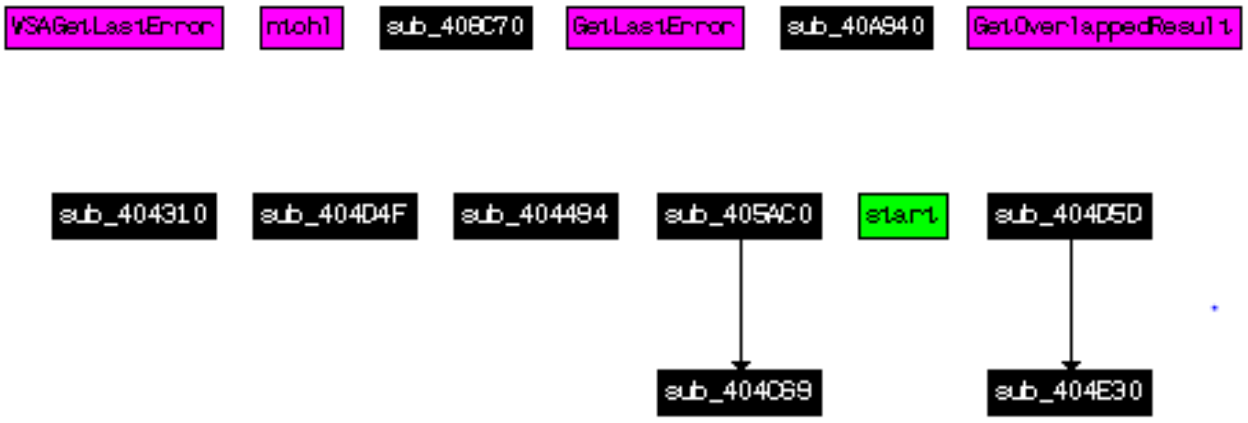
Sering kali pembuat malware mengaburkan kode mereka sehingga file-file tersebut sulit untuk dibaca. Ketika paket program berjalan, program wrapper juga berjalan untuk membongkar itu. Dengan analisis statis, benar-benar sulit untuk memprediksi file mana yang dikemas.

Skema dari payload.exe dapat kita lihat seperti grapik pada Gambar 10 dibawah ini dengan menggunakan tool IDA Pro.

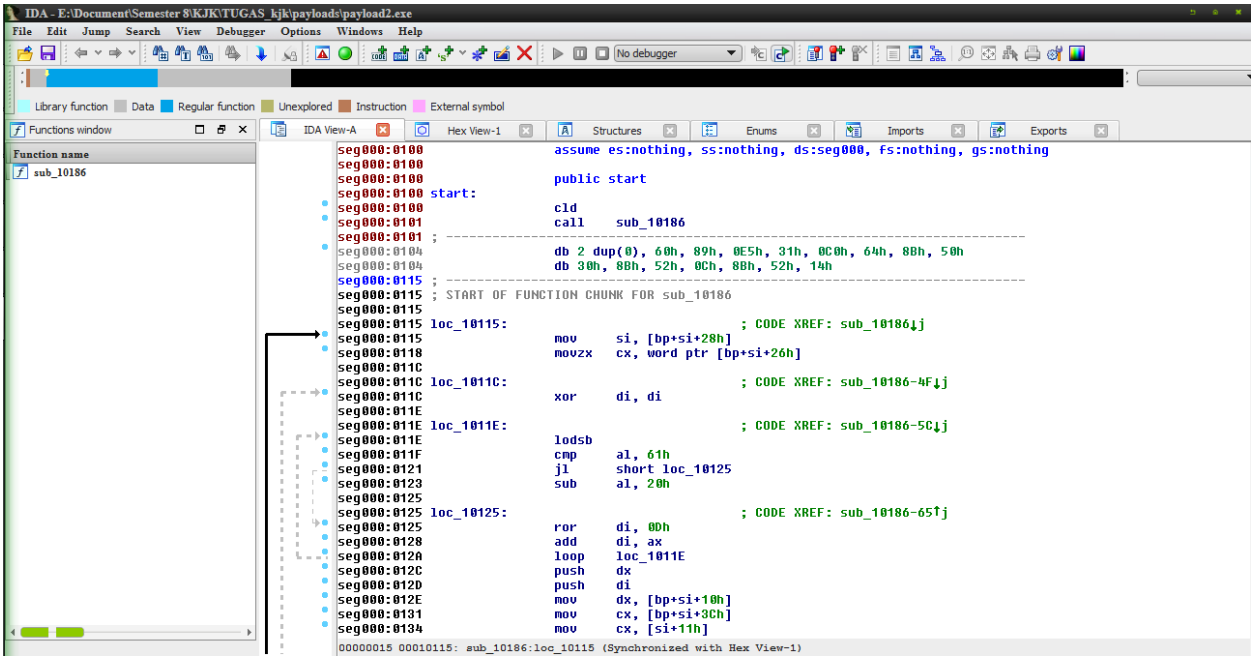


Gambar.9 Tampilan IDA Pro File Payload.exe

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Gambar.10 Grafik Payload.exe



Gambar.11 Tampilan IDA Pro File Payload2.exe

Proses kerja terlihat dimana program berusaha menyiapkan koneksi dengan memanggil instruksi socket dan menyiapkan koneksi tersebut lewat socket yang akan dipakai.