

Malware Analysis Workshop

Cyber Security Seminar & Workshop

Yohanes Syailendra, CEH, ECSCA

16 May 2017 | Marquee, Cyber 2 Tower 17th | Jakarta, Indonesia

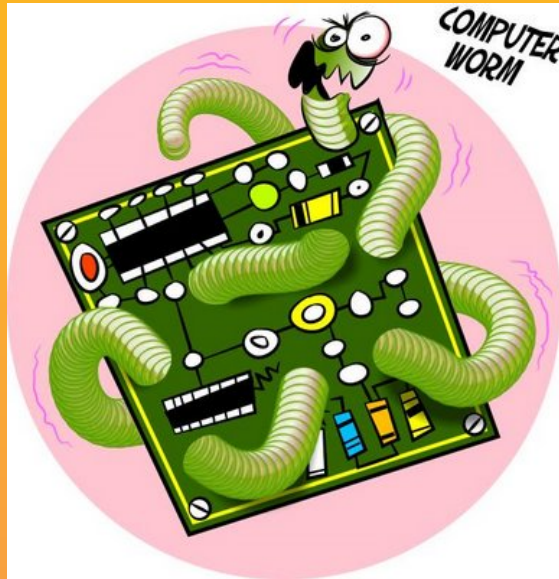


Indonesia HoneyNet Project

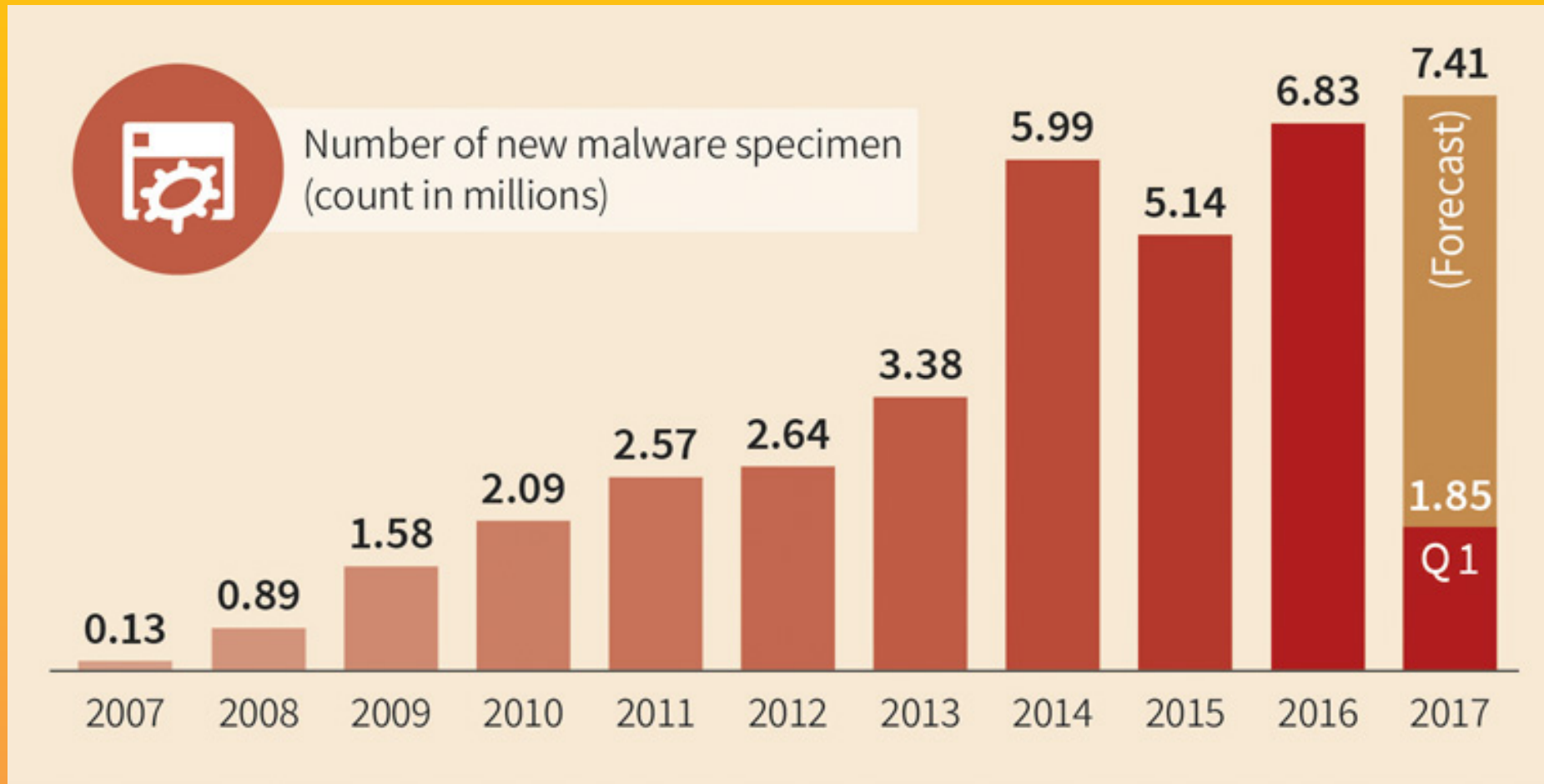


What is Malware

- Malware (Malicious Software)
 - All kind of software that disrupt computer operations, gather sensitive information or gain access to private computer systems



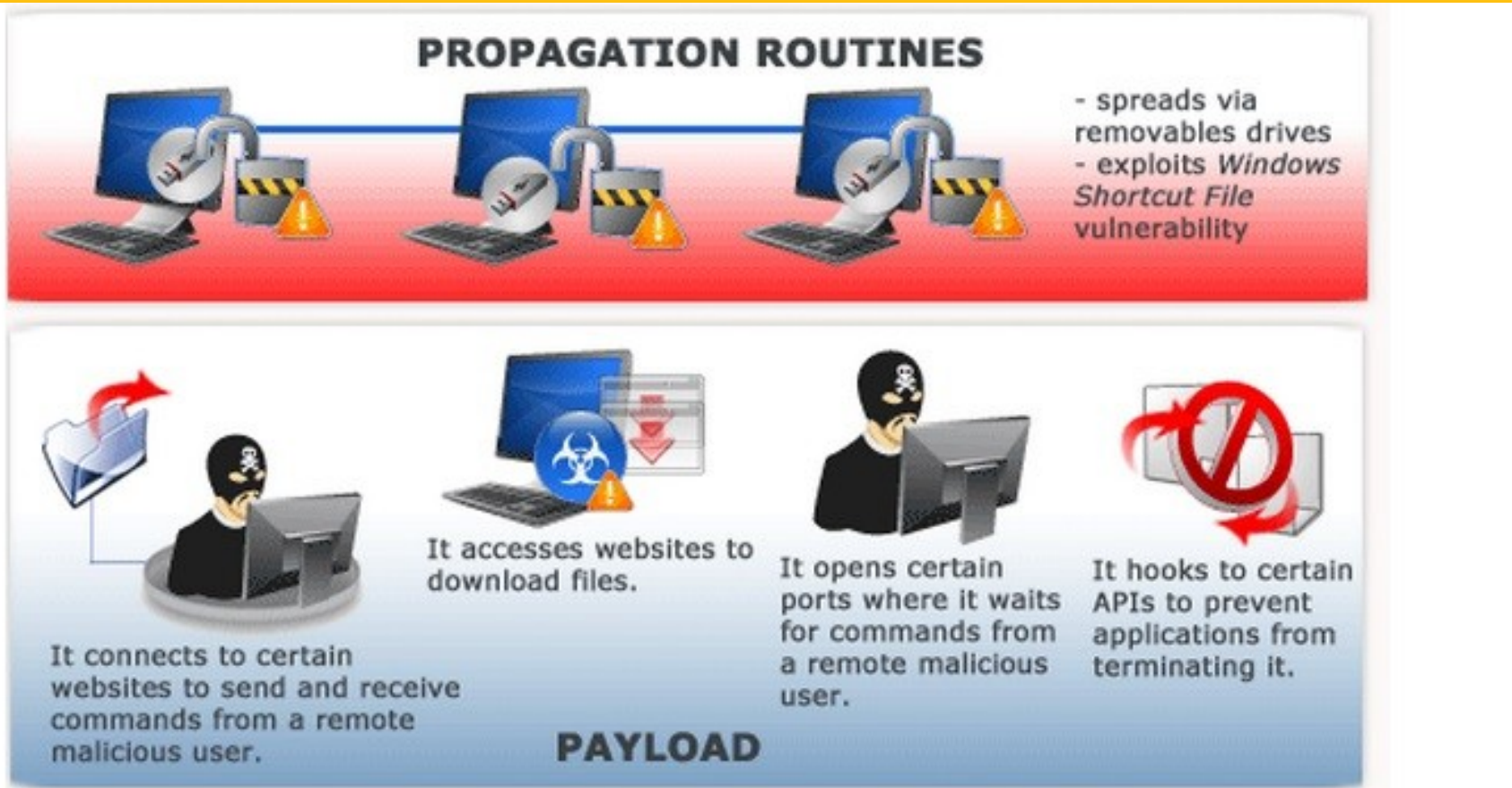
Statistics say it all



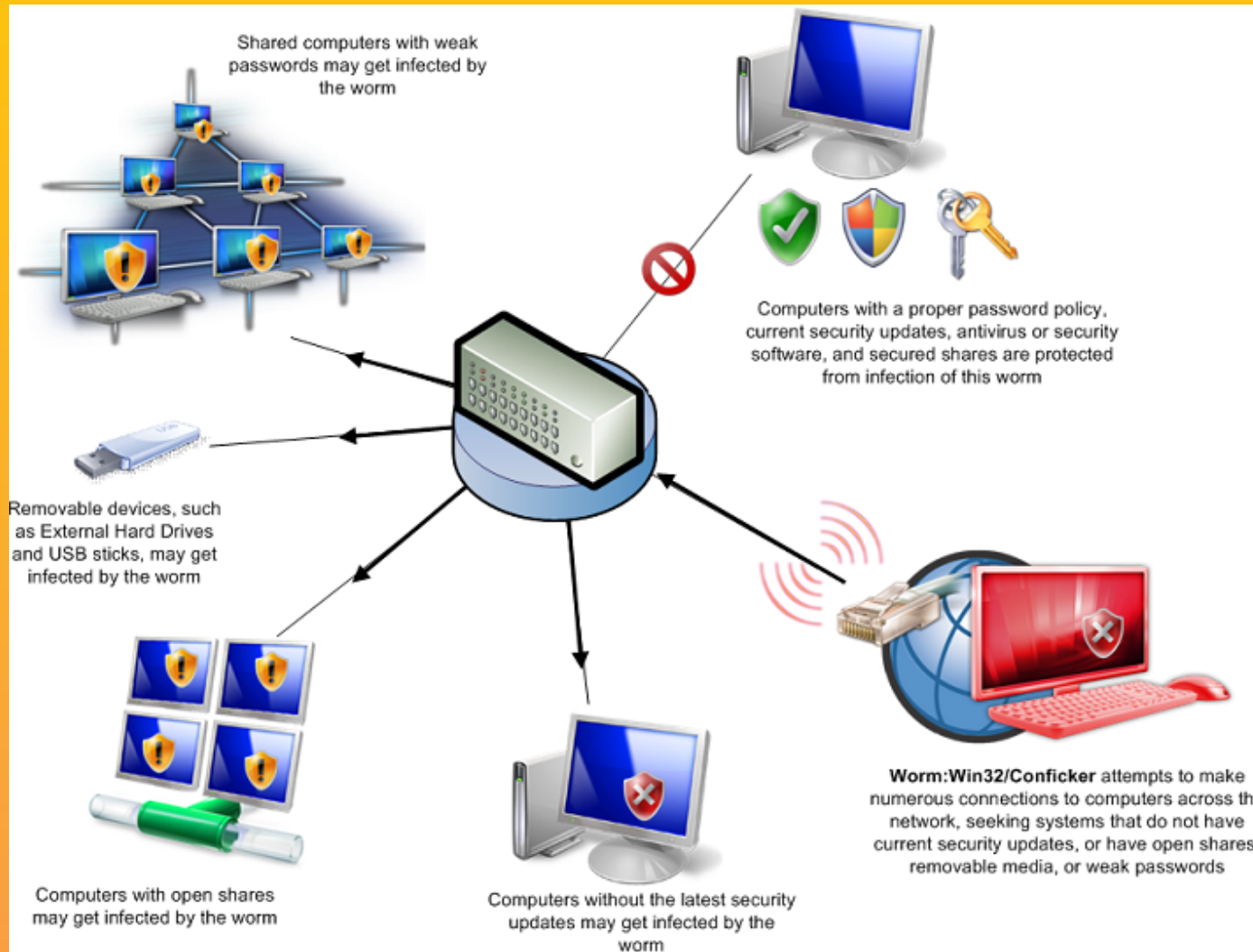
5 Stages Malware attack



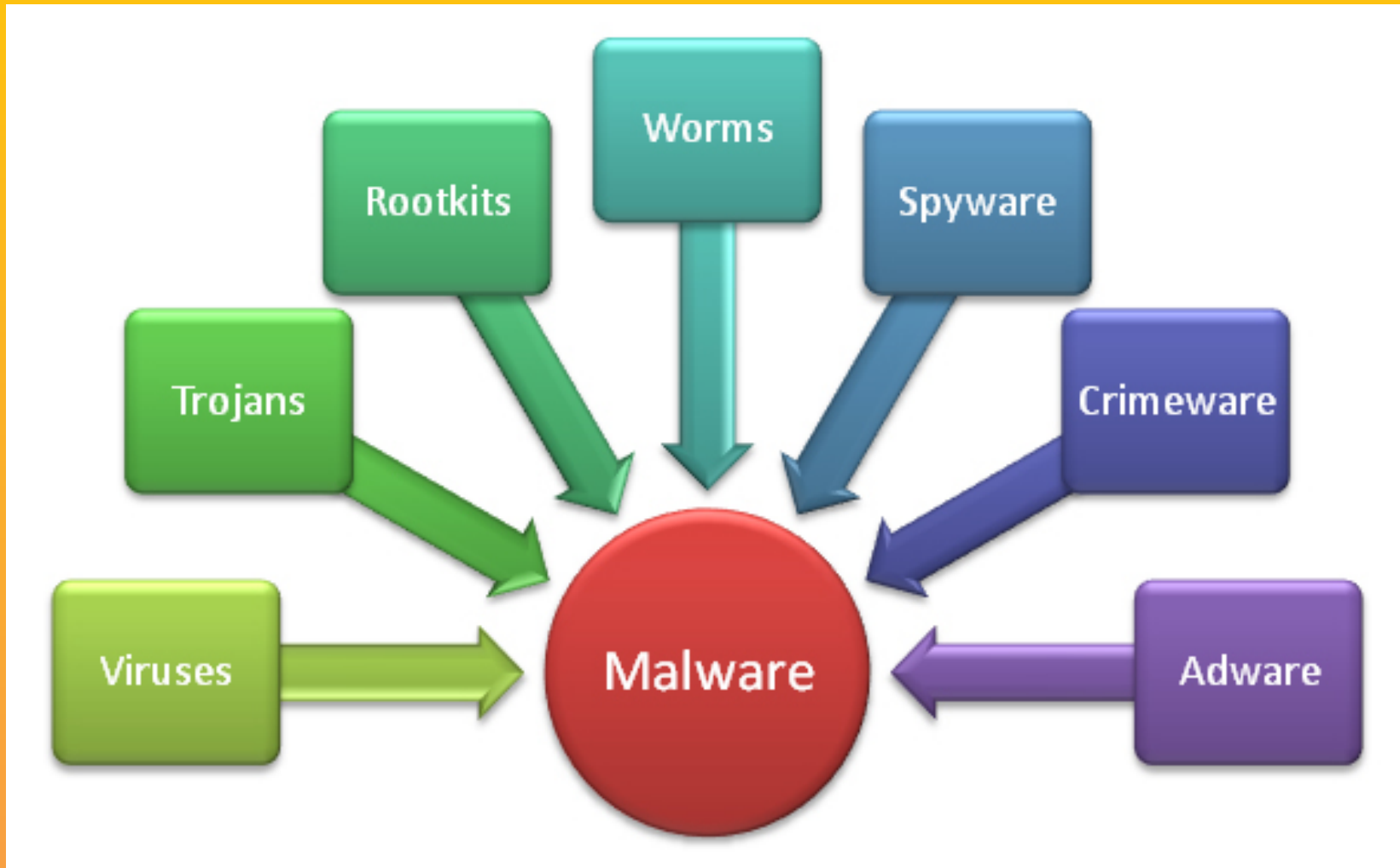
Malware Propagation



Malware Propagation



Malware Types



Malware Defense Mechanism

- Anti Detection
 - Polymorphism
 - Metamorphism
 - Hide inside kernel or other process
 - “Kill Switch”
 - Detect internet access
 - Time based malware
 - Detect Environment



Malware Defense Mechanism

- Anti Analysis
 - Encryption
 - Anti-Debugging
 - Anti-VM



Purpose of Malware Analysis

- Identify a Malware
- Malware Capabilities / Behavior
- Malware Propagation Technique
- Malware Signatures / How to Detect
- How to Resolve from Infection



Type Malware Analysis

Static
Analysis

A method of examining computer program/code **without** executing the program

Dynamic
Analysis

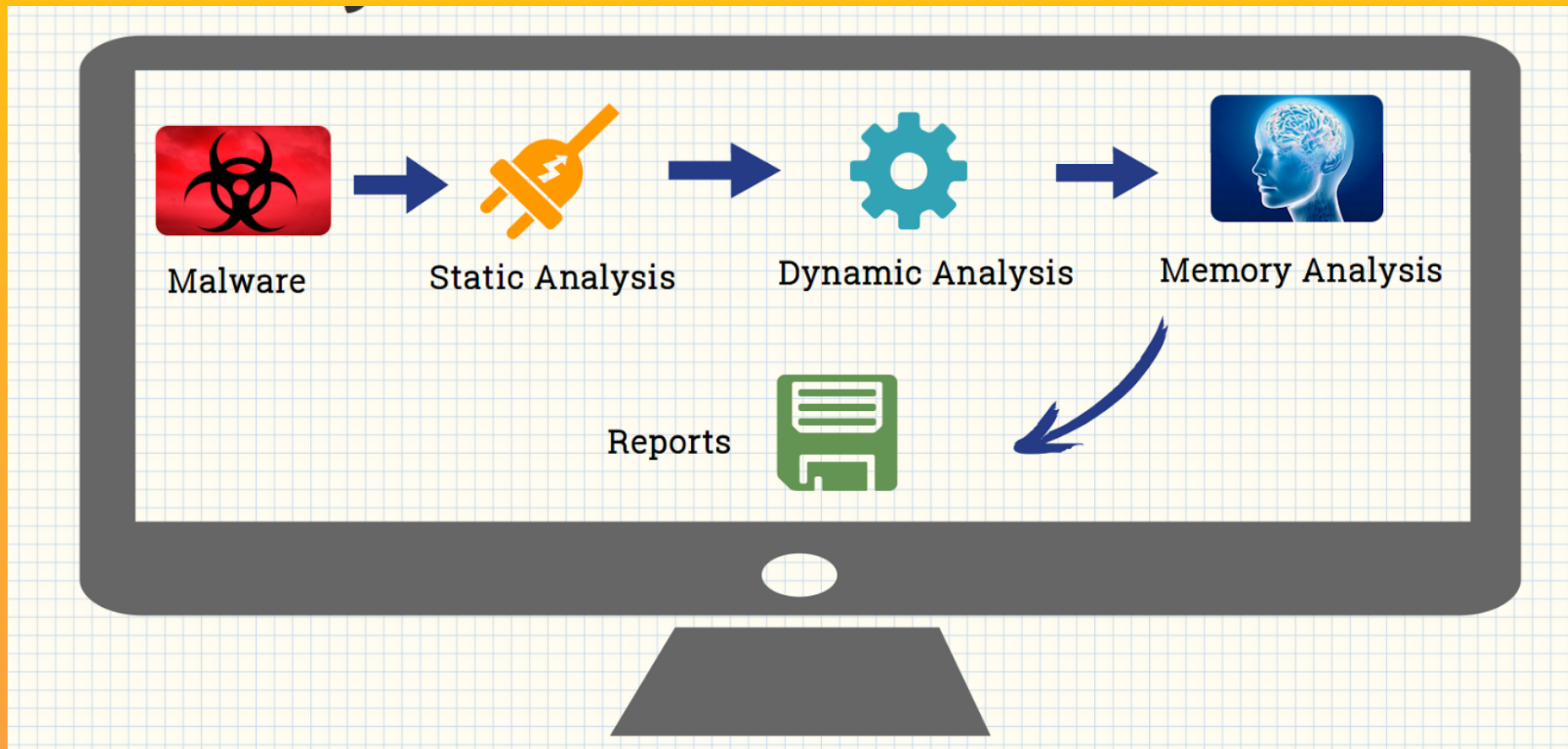
A method of examining computer program/code **while** executing the program in a real or virtual processor

Memory
Analysis

A method of examining computer program/code **after** executing the program in a real or virtual processor



Malware Analysis Process



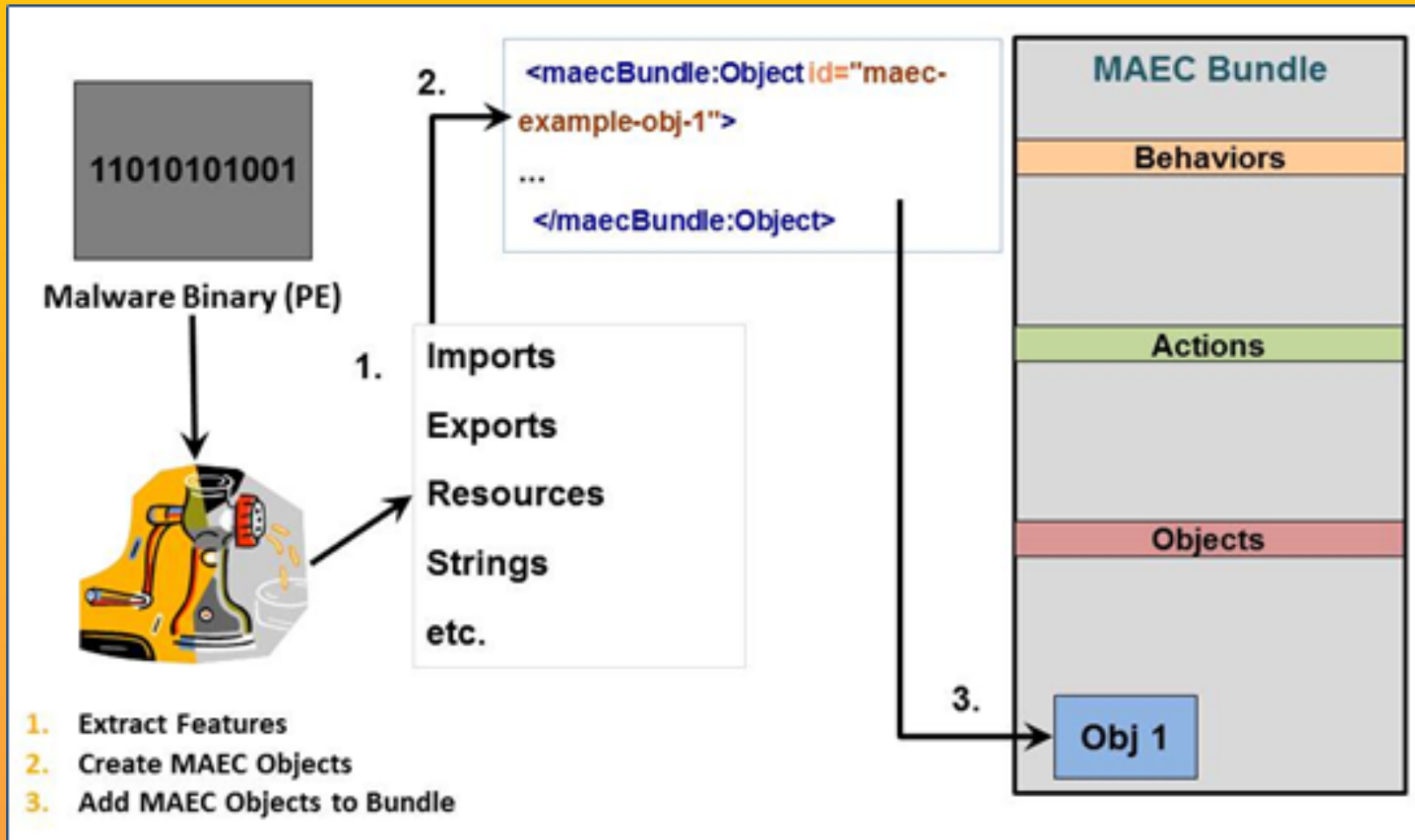
Static Analysis



Indonesia Honeynet Project



Malware Static Analysis



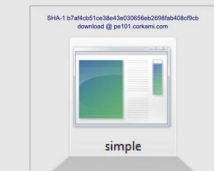
Inside of a File

PE¹⁰¹ a windows executable walkthrough



Ange Albertini
corkami.com

Dissected PE



simple.exe

technical details about the executable

sections

contents of the executable

header

sections table

code

imports

data

DOS header
shows it's a binary

PE header
shows it's a "modern" binary

optional header
executable information

data directories
pointers to extra structures (exports, imports,...)

sections table
defines how the file is loaded in memory

code
what is executed

imports
link between the executable and (Windows) libraries

data
information used by the code

Hexadecimal dump	ASCII dump	Fields	Values	Explanation
4D 5A 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....	e_magic	'MZ'	constant signature
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00@...	e_lfanew	0x40	offset of the PE Header ①
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PE.....	Signature	'PE', 0, 0	constant signature
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Machine	0x14c [intel 386]	processor: ARM/MIPS/Intel...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	NumberOfSections	3	number of sections ②
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SizeOfOptionalHeader	0xe0	relative offset of the section table ②
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Characteristics	0x102 [32b EXE]	EXE/DLL...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Magic	0x10b [32b]	32 bits/64 bits
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	AddressOfEntryPoint	0x40000	address where the file should be mapped in memory
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SectionAlignment	0x1000	where sections should start in memory ②
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	FileAlignment	0x200	where sections should start on file ②
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MajorSubsystemVersion	4 [NT 4 or later]	required version of Windows
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SizeOfImage	0x4000	total memory space required
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SizeOfHeaders	0x200	total size of the headers ③
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Subsystem	2 [GUI]	driver/graphical/command line...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	NumberOfRvaAndSizes	16	number of data directories ④
00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ImportsVA	0x2000	RVA of the imports ④

Sections table						
Name	VirtualSize	VirtualAddress	SizeOfRawData	physical size	PointerToRawData	physical offset
.text	0x1000	0x1000	0x200	0x200	0x400	CODE_EXECUTE_READ
.rdata	0x1000	0x2000	0x200	0x400	0x400	INITIALIZED_READ
.data	0x1000	0x3000	0x200	0x600	0x600	DATA_READ_WRITE

For each section, a SizeOfRawData sized block is read from the file at PointerToRawData offset. It will be loaded in memory at address ImageBase + VirtualAddress in a VirtualSize sized block, with specific characteristics.

x86 assembly	Equivalent C code
push 0	
push 0x403000	
push 0x403017	
push 0	
call [0x402070]	MessageBox(0, "hello world!", "a simple PE executable", 0);
push 0	
call [0x402068]	ExitProcess(0);

Imports structures	Consequences
0x203c	kernel32.dll, 0x204c, 0
0x2078	kernel32.dll, 0, ExitProcess
0x2068	kernel32.dll, 0x204c, 0
0x2044	kernel32.dll, 0x205a, 0
0x2085	kernel32.dll, 0, MessageBox
0x2070	kernel32.dll, 0x205a, 0

after loading, 0x2068 will point to kernel32.dll's ExitProcess, 0x2070 will point to user32.dll's MessageBoxA

Strings
a simple PE executable\Hello world!

Inside of a File – Hex Version

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f		
00000000h:	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	; MZP.....ÿÿ..	
00000010h:	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	;@.....	DOS HEADER
00000020h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000030h:	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	;	
00000040h:	BA	10	00	0E	1F	B4	09	CD	21	B8	01	4C	CD	21	90	90	; °....'í!..Lí![]	
00000050h:	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	; This program mus	DOS STUB
00000060h:	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	; t be run under W	
00000070h:	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	; in32..\$7.....	
00000080h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000a0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000c0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000000f0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
00000100h:	50	45	00	00	4C	01	08	00	19	5E	42	2A	00	00	00	00	; PE..L....^B*....	PE HEADER
00000110h:	00	00	00	00	E0	00	8E	81	0B	01	02	19	00	A0	02	00	;à.ž[].....	
00000120h:	00	DE	00	00	00	00	00	00	B4	AD	02	00	00	10	00	00	; .B.....'.....	
00000130h:	00	B0	02	00	00	00	00	00	40	00	00	10	00	00	02	00	; °....@.....	Signature
00000140h:	01	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	;	
00000150h:	00	D0	03	00	00	04	00	00	00	00	00	00	02	00	00	00	; .D.....	FileHeader
00000160h:	00	00	10	00	00	40	00	00	00	00	10	00	00	10	00	00	;@.....	
00000170h:	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	;	
00000180h:	00	D0	02	00	1E	18	00	00	00	40	03	00	00	8E	00	00	; .D.....@...ž..	OptionalHeader
00000190h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000001a0h:	00	10	03	00	04	2B	00	00	00	00	00	00	00	00	00	00	;+.....	DATA DIRECTORY
000001b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000001c0h:	00	00	03	00	18	00	00	00	00	00	00	00	00	00	00	00	;	
000001d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000001e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	;	
000001f0h:	00	00	00	00	00	00	00	00	43	4F	44	45	00	00	00	00	;CODE....	
00000200h:	88	9E	02	00	00	10	00	00	00	A0	02	00	00	04	00	00	; ^ž.....	SECTION TABLE
00000210h:	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	;	
00000220h:	44	41	54	41	00	00	00	00	D4	06	00	00	00	B0	02	00	; DATA....ô....°..	

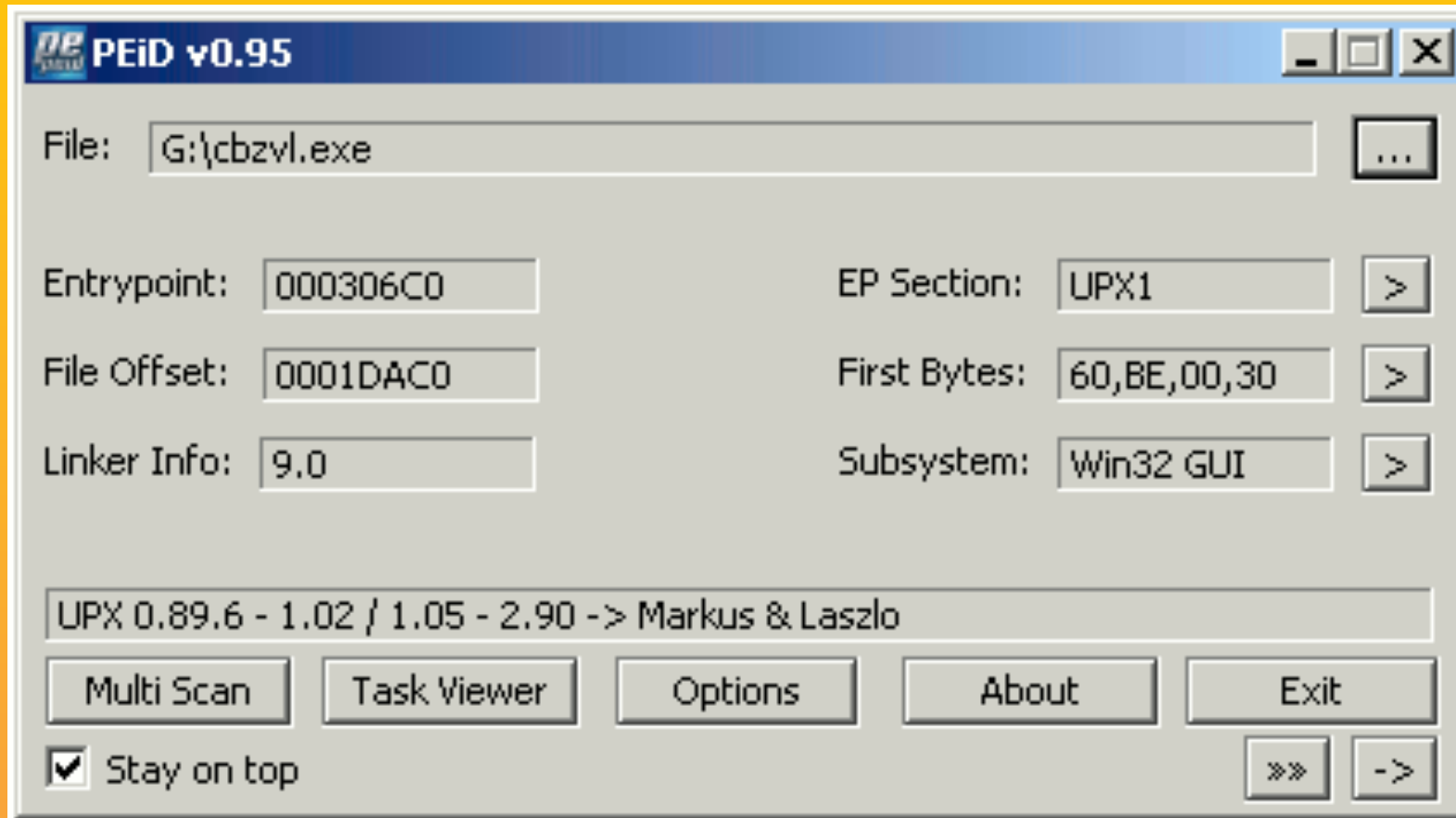


Check file type

- Open File with Hexa Editor
- Search 2 first character with the website
 - http://garykessler.net/library/file_sigs.html
- File [filename] → Check for file type
- Cek Bunch of Files below :
 - <http://45.126.133.156/yohanes/files/tebak1>
 - <http://45.126.133.156/yohanes/files/tebak2>
 - <http://45.126.133.156/yohanes/files/tebak3>
 - <http://45.126.133.156/yohanes/files/tebak4>



PEID



PEID Used to check initial information of a file



PESCANNER

```
remnux@remnux: ~/analysis
File Edit Tabs Help

Sections
=====
Name      VirtAddr  VirtSize  RawSize  MD5                               Entropy
-----
.text     0x1000    0x16414   0x17000   2a7865468f9de73a531f0ce00750ed17 5.427415
.rdata    0x18000   0x945     0x1000    c663fda3d7b936dfc47c996cdb0fbe57 3.023484
.data     0x19000   0xc92     0x1000    5bd6727d52ce29a93bdec4b619bc282c 4.931830
.rsrc     0x1a000   0x375a0   0x38000   746376cceec9bf357c62cea98995c126 7.983700 [SUSPICIOUS]

Resource entries
=====
Resource type  Total
-----
RT_FONT        : 2

Imports
=====
[1] kernel32.dll
[2] ctl3d32.dll
[3] crypt32.dll
[4] user32.dll
[5] dbnmpntw.dll

Suspicious IAT alerts
=====
[1] CopyFileA
[2] CreateDirectoryW
[3] FindNextFileW
[4] GetDriveTypeW
[5] GetProcAddress
[6] GetStartupInfoA
[7] GetTickCount
[8] LoadLibraryA

remnux@remnux:~/analysis$
```

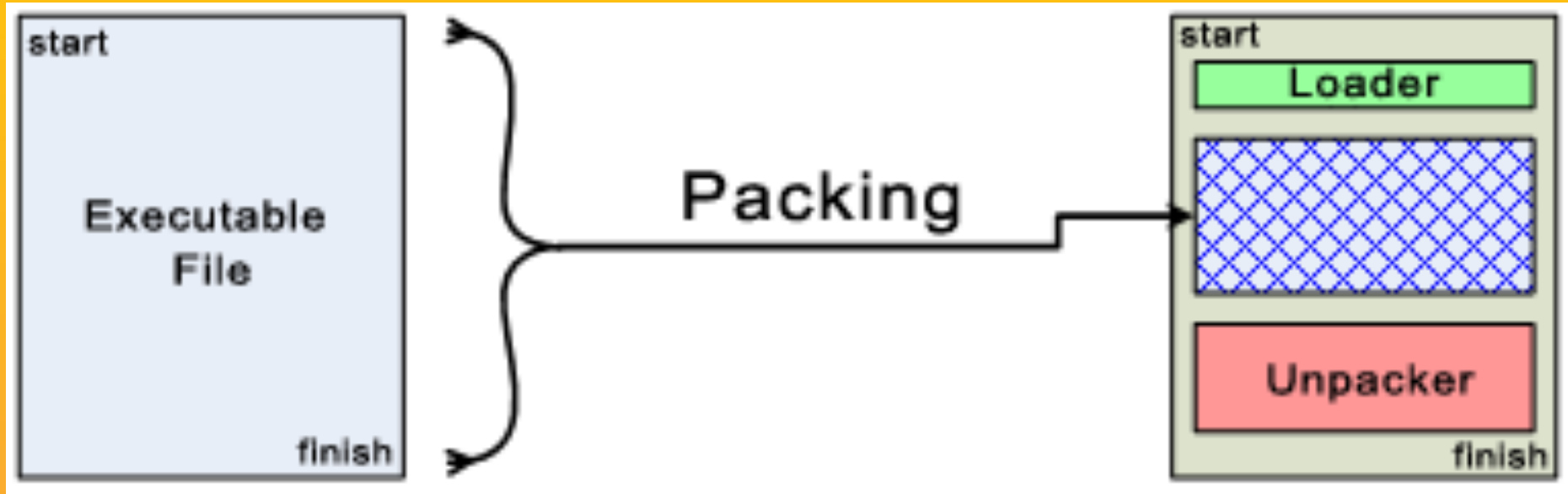


Check Static Features

- Check Strings inside a file :
- Strings [filename]
- Pescanner [filename]
 - <http://45.126.133.156/yohanes/files/file1.exe>
 - <http://45.126.133.156/yohanes/files/file2.exe>
 - <http://45.126.133.156/yohanes/files/file3.exe>
 - <http://45.126.133.156/yohanes/files/file4.exe>
 - <http://45.126.133.156/yohanes/files/file5.exe>
 - <http://45.126.133.156/yohanes/files/file6.exe>



Packed Executables



Static Analysis of malware

- Hexdump malware
- Pescanner [malware]
- Strings [malware]
- Clamscan [malware]
- Analyze this 2 malwares:
 - <http://45.126.133.156/yohanes/files/malware1.bin>
 - <http://45.126.133.156/yohanes/files/malware2.bin>



Find the Flags (CTF)

- <http://45.126.133.156/yohanes/files/1>
- <http://45.126.133.156/yohanes/files/2>
- <http://45.126.133.156/yohanes/files/5>
- <http://45.126.133.156/yohanes/files/6>



Dynamic Analysis



Indonesia Honeynet Project

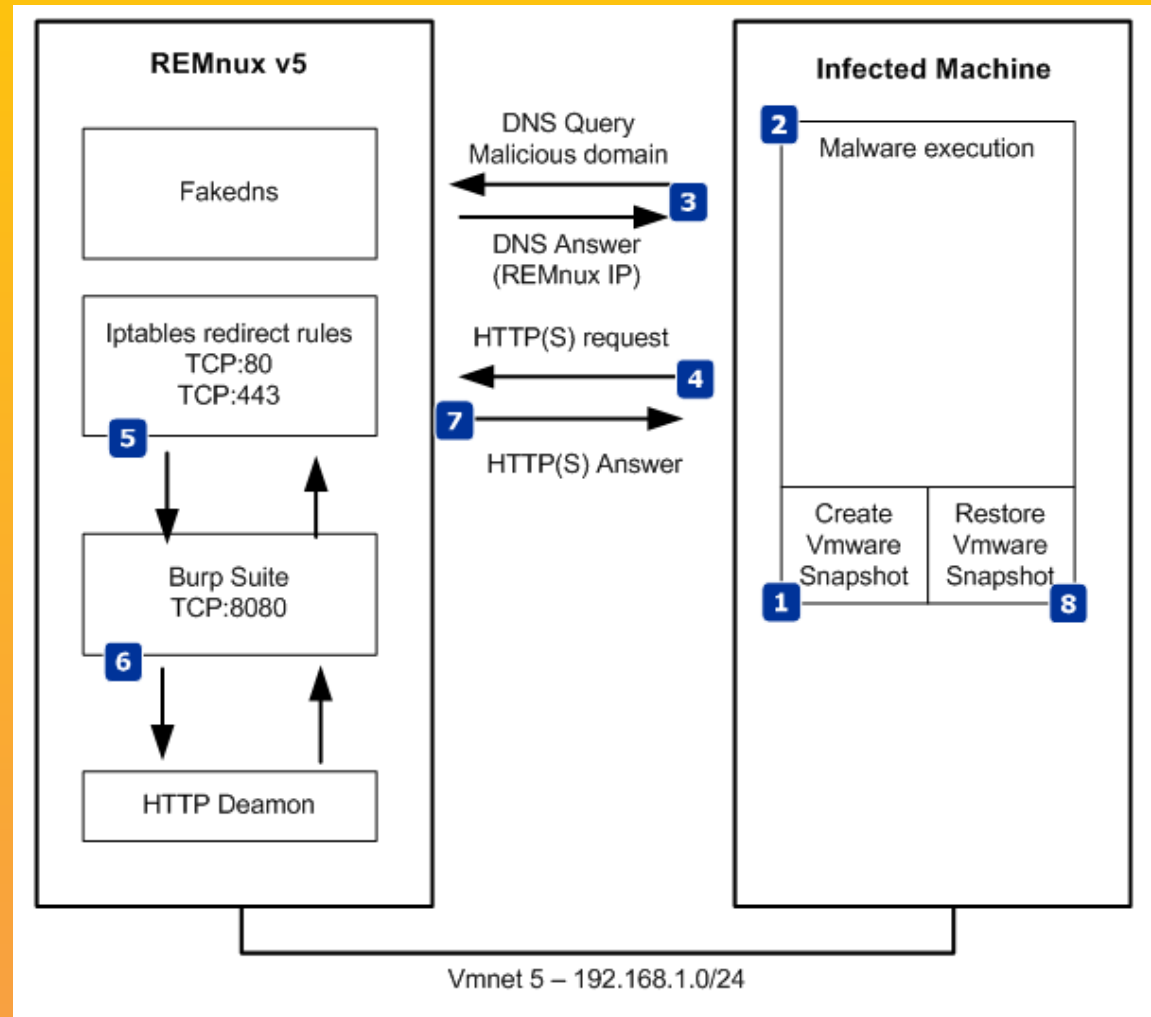


Malware Dynamic Analysis

- Running Malware deliberately, while monitoring the results
- Requires a safe environments
- Must prevent malware from spreading to production machines
- Real machines can be airgapped – no network connection to the internet or to other machine



Topology Dynamic Analysis



Process Monitoring

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

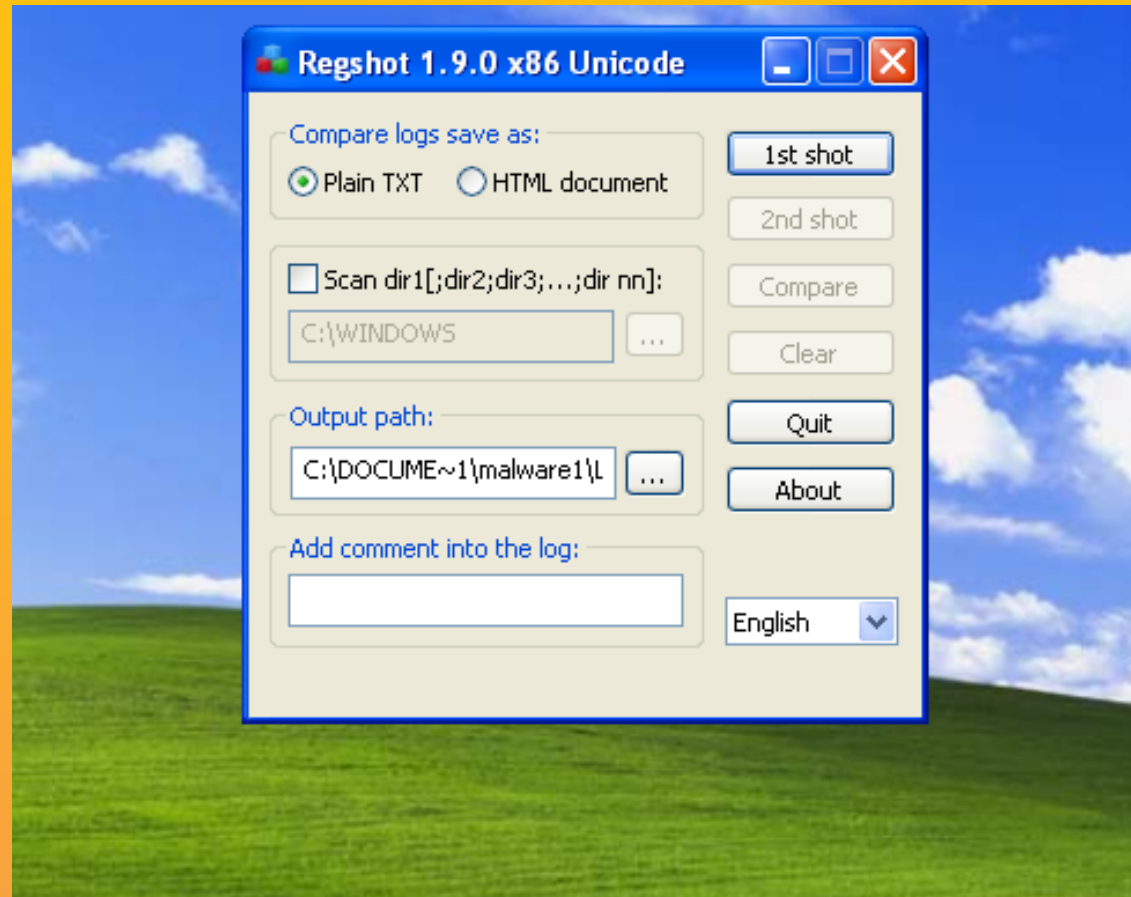
Time...	Process Name	PID	Operation	Path	Result	Detail
12:07:...	lsass.exe	700	Process Profiling		SUCCESS	User Time: 0.1101...
12:07:...	VBoxService.exe	856	Process Profiling		SUCCESS	User Time: 0.0400...
12:07:...	svchost.exe	900	Process Profiling		SUCCESS	User Time: 0.0300...
12:07:...	svchost.exe	988	Process Profiling		SUCCESS	User Time: 0.0200...
12:07:...	svchost.exe	1072	Process Profiling		SUCCESS	User Time: 1.1416...
12:07:...	svchost.exe	1124	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	svchost.exe	1312	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	spoolsv.exe	1608	Process Profiling		SUCCESS	User Time: 0.0200...
12:07:...	Explorer.EXE	1632	Process Profiling		SUCCESS	User Time: 8.2017...
12:07:...	VBoxTray.exe	1964	Process Profiling		SUCCESS	User Time: 0.0300...
12:07:...	GoogleUpdate...	248	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	NitroPDFReade...	824	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	alg.exe	196	Process Profiling		SUCCESS	User Time: 0.0200...
12:07:...	wscntfy.exe	508	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	MasWin.exe	244	Process Profiling		SUCCESS	User Time: 0.0500...
12:07:...	GoogleUpdate...	484	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	GoogleUpdate...	500	Process Profiling		SUCCESS	User Time: 0.0200...
12:07:...	wmiprvse.exe	1920	Process Profiling		SUCCESS	User Time: 0.0100...
12:07:...	GoogleUpdate...	500	RegCreateKey	HKLM\Software\Google\Update\Client...	SUCCESS	Desired Access: All...
12:07:...	GoogleUpdate...	500	RegSetValue	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	Type: REG_DWD...
12:07:...	GoogleUpdate...	500	RegCloseKey	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	
12:07:...	GoogleUpdate...	500	RegCreateKey	HKLM\Software\Google\Update\Client...	SUCCESS	Desired Access: All...
12:07:...	GoogleUpdate...	500	RegSetValue	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	Type: REG_DWD...
12:07:...	GoogleUpdate...	500	RegCloseKey	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	
12:07:...	GoogleUpdate...	500	RegCreateKey	HKLM\Software\Google\Update\Client...	SUCCESS	Desired Access: All...
12:07:...	GoogleUpdate...	500	RegSetValue	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	Type: REG_DWD...
12:07:...	GoogleUpdate...	500	RegCloseKey	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	
12:07:...	GoogleUpdate...	500	RegCreateKey	HKLM\Software\Google\Update\Client...	SUCCESS	Desired Access: All...
12:07:...	GoogleUpdate...	500	RegSetValue	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	Type: REG_DWD...
12:07:...	GoogleUpdate...	500	RegCloseKey	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	
12:07:...	GoogleUpdate...	500	RegCreateKey	HKLM\Software\Google\Update\Client...	SUCCESS	Desired Access: All...
12:07:...	GoogleUpdate...	500	RegSetValue	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	Type: REG_DWD...
12:07:...	GoogleUpdate...	500	RegCloseKey	HKLM\SOFTWARE\Google\Update\Cli...	SUCCESS	

Showing 25,888 of 59,353 events (43%) Backed by virtual memory

start malware Analysis MasWin MasWin Tools Process Monitor - Sys... 12:08 PM

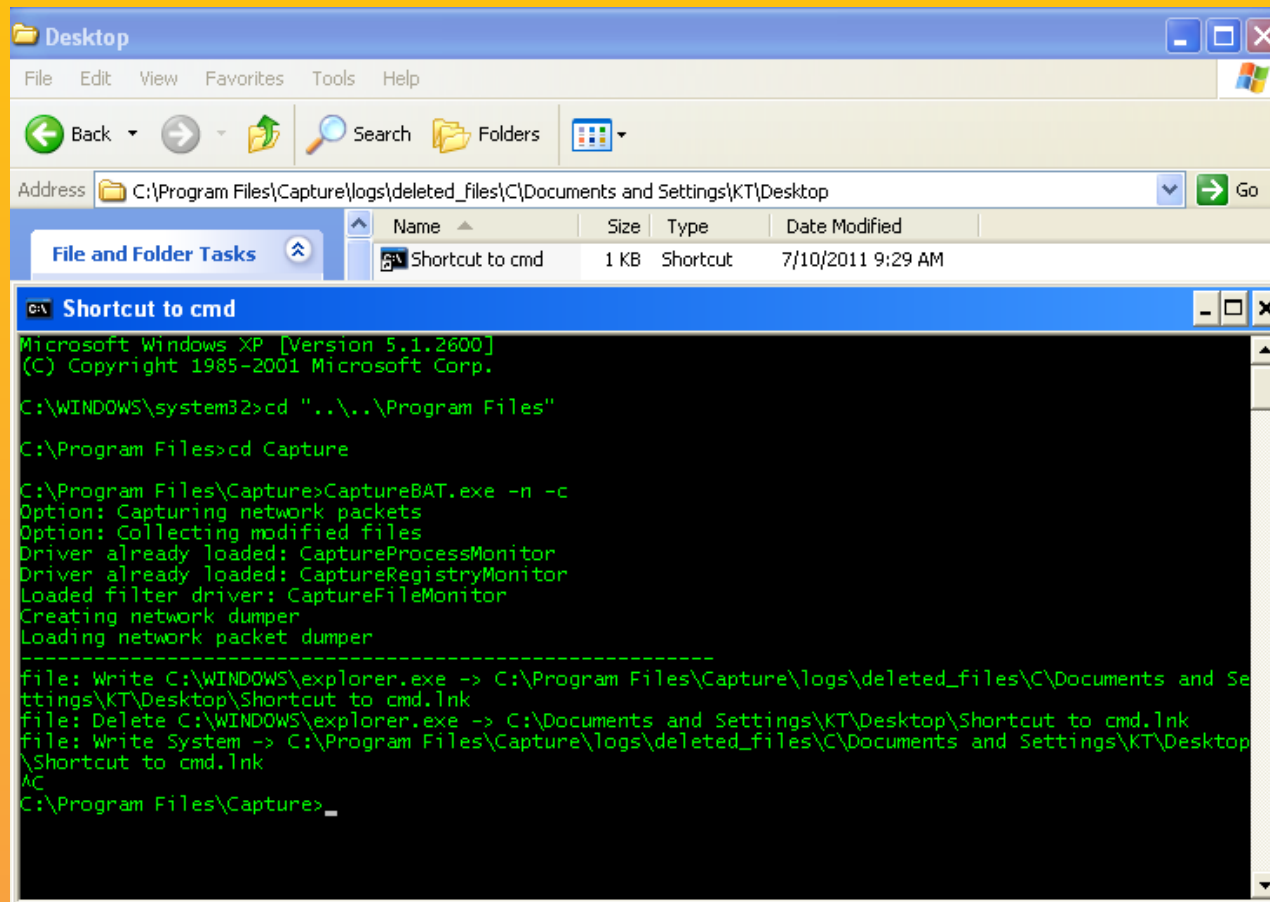


Registry Monitoring (Regshot)



CaptureBAT

- CaptureBAT.exe -c -n -l test.exe
- Open With Wireshark



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

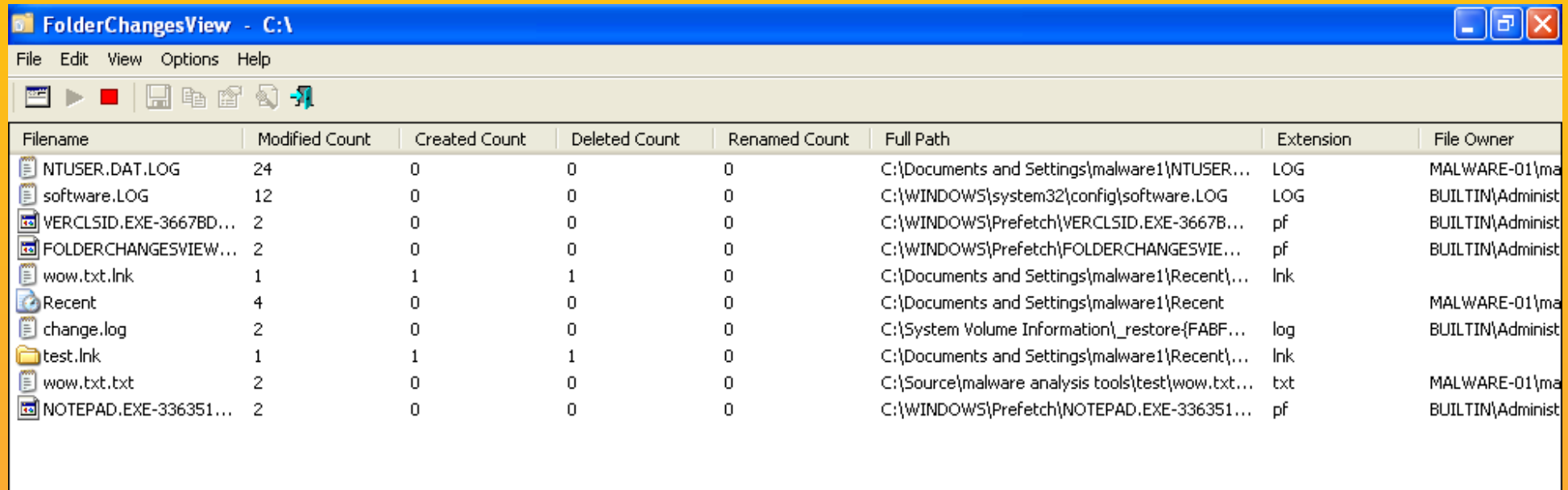
C:\WINDOWS\system32>cd "..\..\Program Files"

C:\Program Files>cd Capture

C:\Program Files\Capture>CaptureBAT.exe -n -c
Option: Capturing network packets
Option: Collecting modified files
Driver already loaded: CaptureProcessMonitor
Driver already loaded: CaptureRegistryMonitor
Loaded filter driver: CaptureFileMonitor
Creating network dumper
Loading network packet dumper
-----
file: Write C:\WINDOWS\explorer.exe -> C:\Program Files\Capture\logs\deleted_files\C\Documents and Settings\KT\Desktop\Shortcut to cmd.lnk
file: Delete C:\WINDOWS\explorer.exe -> C:\Documents and Settings\KT\Desktop\Shortcut to cmd.lnk
file: Write System -> C:\Program Files\Capture\logs\deleted_files\C\Documents and Settings\KT\Desktop\Shortcut to cmd.lnk
^C
C:\Program Files\Capture>
```



Folderchangeview



The screenshot shows the FolderChangesView application window with a menu bar (File, Edit, View, Options, Help) and a toolbar. The main area displays a table with the following columns: Filename, Modified Count, Created Count, Deleted Count, Renamed Count, Full Path, Extension, and File Owner.

Filename	Modified Count	Created Count	Deleted Count	Renamed Count	Full Path	Extension	File Owner
NTUSER.DAT.LOG	24	0	0	0	C:\Documents and Settings\malware1\NTUSER...	LOG	MALWARE-01\ma
software.LOG	12	0	0	0	C:\WINDOWS\system32\config\software.LOG	LOG	BUILTIN\Administ
VERCLSID.EXE-3667BD...	2	0	0	0	C:\WINDOWS\Prefetch\VERCLSID.EXE-3667B...	pf	BUILTIN\Administ
FOLDERCHANGESVIEW...	2	0	0	0	C:\WINDOWS\Prefetch\FOLDERCHANGESVIE...	pf	BUILTIN\Administ
wow.txt.lnk	1	1	1	0	C:\Documents and Settings\malware1\Recent\...	lnk	
Recent	4	0	0	0	C:\Documents and Settings\malware1\Recent		MALWARE-01\ma
change.log	2	0	0	0	C:\System Volume Information_restore{FABF...	log	BUILTIN\Administ
test.lnk	1	1	1	0	C:\Documents and Settings\malware1\Recent\...	lnk	
wow.txt.txt	2	0	0	0	C:\Source\malware analysis tools\test\wow.txt...	txt	MALWARE-01\ma
NOTEPAD.EXE-336351...	2	0	0	0	C:\WINDOWS\Prefetch\NOTEPAD.EXE-336351...	pf	BUILTIN\Administ



Cuckoo Sandbox

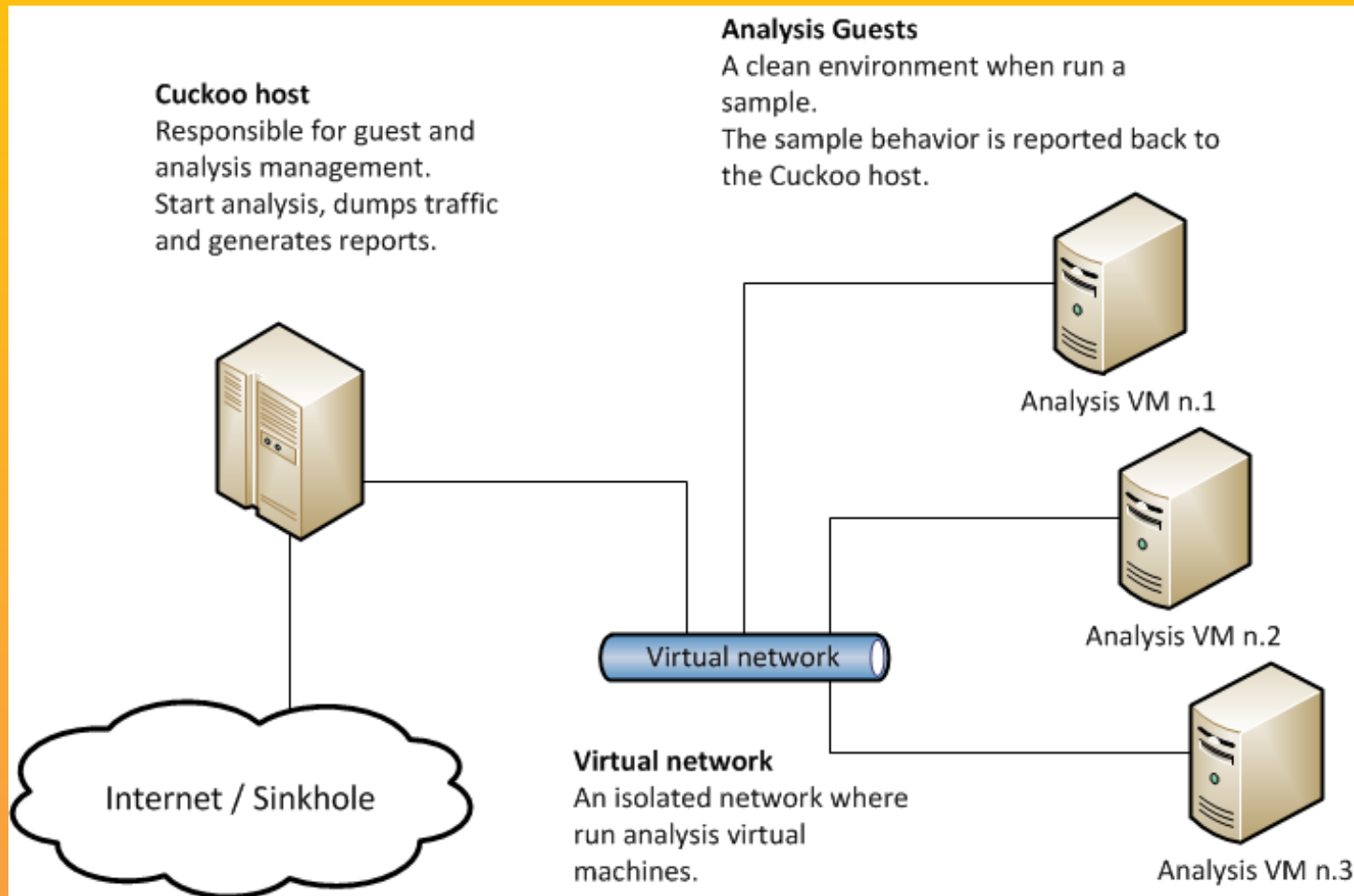
Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-07-20 19:57:37	2013-07-20 20:00:02	145 seconds	0.6

File Details

File name	iwmsax.exe
File size	473558 bytes
File type	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
CRC32	C5CF164C
MD5	ccdabe0075b01bde734c61eece0d1e46
SHA1	3051356e74ed3c84194513f2d93111c41ad13871
SHA256	baf6d9cdac23c577146801a53324332455c5bbbe8dbc5d726bef2b394a43c726
SHA512	a40b0b1bd8afa6020a3d12976bad21c54051bdda3fd676f20151a8877211e4e3b502869c4d549c12ae3116c21b52dd423b1537626391e4a93af24eca09bd6480
Ssdeep	None
PEID	None matched
Yara	None matched



Cuckoo Sandbox



Analysis test

- <http://45.126.133.156/yohanes/files/malware1.bin>
- <http://45.126.133.156/yohanes/files/malware2.bin>



Simple Reverse Engineering



Indonesia HoneyNet Project



Radare2

```
remnux@remnux: ~  
File Edit Tabs Help  
16c46  
| 0x00400553 488910 mov [rax], rdx  
| 0x00400556 48b96c61682. mov rcx, 0x33743453206  
8616c  
| 0x00400560 48894808 mov [rax+0x8], rcx  
| 0x00400564 48be6b346d6. mov rsi, 0x676e69626d3  
46b  
| 0x0040056e 48897010 mov [rax+0x10], rsi  
| 0x00400572 bf24064000 mov edi, str.12  
| 0x00400577 e884feffff call sym.imp.puts  
| sym.imp.puts(unk)  
| 0x0040057c 8b45fc mov eax, [rbp-0x4]  
| 0x0040057f 89c6 mov esi, eax  
| 0x00400581 bf29064000 mov edi, str.d  
| 0x00400586 b800000000 mov eax, 0x0  
| 0x0040058b e880feffff call sym.imp.printf  
| sym.imp.printf()  
| 0x00400590 b800000000 mov eax, 0x0  
| 0x00400595 c9 leave  
| 0x00400596 c3 ret  
[0x00400440]>
```



Install GCC

- Test apakah ada GCC untuk kompilasi C
 - `#!/locate glibc =>`
 - harusnya muncul
`:"/usr/share/man/man7/glibc.7.gz"`
 - `#!/gcc` → harusnya muncul :
 - "gcc: fatal error: no input files" => Berarti sudah terinstall
 - kalo ga ada : install GCC :
 - `#!/apt-get install gcc`



Create Hello file.c

```
#include <stdio.h>
int main()
{
    printf("Haloo");
    return 0;
}
```



Open at edb kali linux

- Search for Helloo string and replace with another string
- Edit the string to another



Search for the Flag

- R2 [filename]
- Type 'aa' → to start analyze all
- Type 'pdf@main' → to find the int main function
- Find the flag:
 - <http://45.126.133.156/yohanes/files/wow>
 - <http://45.126.133.156/yohanes/files/wow1>



Memory Analysis



Indonesia Honeynet Project



Volatility

```
jniето@behindthefirewalls:/home/volatility-2.1$ python vol.py -f zeus.vmem pstree
Volatile Systems Volatility Framework 2.1
Name                               Pid    PPid   Thds   Hnds  Time
-----
0x810b1660:System                   4      0      58     379  1970-01-01 00:00:00
. 0xff2ab020:smss.exe                544     4       3      21  2010-08-11 06:06:21
.. 0xff1ec978:winlogon.exe           632    544     24     536  2010-08-11 06:06:23
... 0xff255020:lsass.exe              688    632     21     405  2010-08-11 06:06:24
... 0xff247020:services.exe          676    632     16     288  2010-08-11 06:06:24
.... 0xff1b8b28:vmtoolsd.exe          1668    676      5     225  2010-08-11 06:06:35
..... 0xff224020:cmd.exe                 124   1668      0     - - - - - 2010-08-15 19:17:55
.... 0x80ff88d8:svchost.exe             856    676     29     336  2010-08-11 06:06:24
.... 0xff1d7da0:spoolsv.exe             1432    676     14     145  2010-08-11 06:06:26
.... 0x80fbf910:svchost.exe             1028    676     88    1424  2010-08-11 06:06:24
..... 0x80f60da0:wuauc.lt.exe            1732   1028      7     189  2010-08-11 06:07:44
..... 0x80f94588:wuauc.lt.exe            468    1028      4     142  2010-08-11 06:09:37
..... 0xff364310:wscntfy.exe             888    1028      1      40  2010-08-11 06:06:49
.... 0xff217560:svchost.exe             936    676     11     288  2010-08-11 06:06:24
.... 0xff143b28:TPAutoConnSvc.e         1968    676      5     106  2010-08-11 06:06:39
..... 0xff38b5f8:TPAutoConnect.e        1084   1968      1      68  2010-08-11 06:06:52
.... 0xff22d558:svchost.exe            1088    676      7      93  2010-08-11 06:06:25
.... 0xff218230:vmacthlp.exe            844    676      1      37  2010-08-11 06:06:24
.... 0xff25a7e0:alg.exe                 216    676      8     120  2010-08-11 06:06:39
.... 0xff203b80:svchost.exe            1148    676     15     217  2010-08-11 06:06:26
.... 0xff1fdc88:VMUpgradeHelper        1788    676      5     112  2010-08-11 06:06:38
.. 0xff1ecda0:csrss.exe                608    544     10     410  2010-08-11 06:06:23
0xff3865d0:explorer.exe             1724   1708     13     326  2010-08-11 06:09:29
. 0xff374980:VMwareUser.exe           452    1724      8     207  2010-08-11 06:09:32
. 0xff3667e8:VMwareTray.exe           432    1724      1      60  2010-08-11 06:09:31
```



Download the images

- <http://45.126.133.156/yohanes/files/cridex.zip>
- <http://45.126.133.156/yohanes/files/zaptftis.rar>



Volatility

- `./vol.py imageino -f <Destination of the memory Dump>`
- `./vol.py -profile=WinXPSP2x86 pslist -f <Destination of the memory Dump> → show all running process`
- `./vol.py -profile=WinXPSP2x86 kdbgscan -f <Destination of the memory Dump> → show kernel debugger block (show hidden process)`



Volatility

- `./vol.py -profile=WinXPSP2x86 kpcrscan -f <Destination of the memory Dump> → show processor specific data`
- `./vol.py -profile=WinXPSP2x86 dlllist-f <Destination of the memory Dump> → show all running dll`
- `./vol.py -profile=WinXPSP2x86 dlldump -D <Destination Directory> -f <memory image location> → Dump all DLL into folder`



Volatility

- `./vol.py -profile=WinXPSP2x86 psscan-D <Destination Directory> -f <memory image location> → scan all process`
- `./vol.py -profile=WinXPSP2x86 -f <memory image location> → Show all process in a tree`
- `./vol.py -profile=WinXPSP2x86 connection -f <memory image location> → Show all running connection`



Volatility

- `./vol.py -profile=WinXPSP2x86 sockets -f <memory image location> → show all open sockets (ports)`
- `./vol.py -profile=WinXPSP2x86 hivescan -f <memory image location> → search for any injected process`
- `./vol.py -profile=WinXPSP2x86 hivelist -f <memory image location> → search for any injected process on virtual memory`



Volatility

- `./vol.py -profile=WinXPSP2x86 svcscan -f <memory image location> → show all services on memory`





Indonesia HoneyNet Project

