OFFICIAL (ISC)² CHAPTER NIGERIA

in association with

InventOnUs
Invent | Optimize | Utilize

Importance of Malware Analysis

Outline

- Malware Analysis: The basics…
- How does one get malware? The bad way
- Importance
- Goals of Malware Analysis
- Types of Malware
- Mass vs Targeted Malware
- Malware Analysis Techniques and Tools
- Techniques involved in Static and Dynamic analysis
- Approach
- Tools used for Static and Dynamic analysis
- Understanding of Sample Malware
- Understanding of CryptoLocker working
- Malware Analyst Job Function
- Job Description and skills set required
- Need of Malware Analyst
- Demo

Malware Analysis: The basics…

Generally

- Malware is any form of malicious software.
- Any code that "performs evil"

Today

Executable content with unknown functionality that is resident on a system of investigative interest

- Viruses
- Worms
- Intrusion Tools
- Spyware
- Rootkits

How does one get malware? The bad way

- Phishing or spear-phishing
- Exploit kits
- Drive-by download
- USB drive or other removable media
- Network (shares, SMB)
- Manual installation (RDP, VNC, TeamViewer, …)
- Watering hole (Strategic Web Compromise)
- Other malware that downloads and/or installs 'companions'

Importance

Assess	the damages from an intrusion or a security incident
Discover	points or indicators of compromise and locating the affected machines
Determine	the level of sophistication of the malware involved
Identify	the source of the attack, the vulnerability exploited by the malware and preparing for patching it accordingly
Learn	from the present incident and taking appropriate measures to ensure that the same cause is not the reason behind any security incident in the future.

Goals of Malware Analysis

- To develop signatures/indicators to detect malware infections on a network.
- Using the signatures to understand how a specific piece of malware functions so that defences can be built to protect the network.
- To detect malicious code on victim computers.
- Identify files created or modified by the malware or specific changes that it makes to the registry.
- Used to detect malicious code by monitoring network traffic.

Types of Malware

- Backdoor
  - Allows attacker to control the system
- Botnet
  - All infected computers receive instructions from the same Command-and-Control (C&C) server
- Downloader
  - Malicious code that exists only to download other malicious code
  - Used when attacker first gains access
- Information-stealing malware
  - Sniffers, keyloggers, password hash grabbers

Types of Malware

- Launcher
  - Malicious program used to launch other malicious programs
  - Often uses nontraditional techniques to ensure stealth or greater access to a system
- Rootkit
  - Malware that conceals the existence of other code
  - Usually paired with a backdoor
- Scareware
  - Frightens user into buying something
- Spam-sending malware
  - Attacker rents machine to spammers

Types of Malware

- Worms or viruses
  - Malicious code that can copy itself and infect additional computers
- Adware
  - uses pop-up windows which cannot be closed and are included with free software and browser toolbars
- Reverse Shell
  - A reverse shell is a connection initiated from the infected host to the attacker and provides the attacker with a shell access to the host often created by a Trojan
- RAT – Remote Access Trojan
  - sometimes called a Remote Administration Tool or Remote Access Tool, is software which allows an attacker to take control of the infected host using a backdoor.

Types of Malware

- Browser Hijacker
  - control your browser settings like the homepage for example, or the standard search provider.
- Information Stealing Malware
  - Information stealing malware often comes in the form as keyloggers, password (hash) grabbers and sniffers.
- Keyloggers
  - software (or hardware) which records your keystrokes in order to retrieve passwords, conversations and other personal details.
- Ransomware
  - often encrypts your hard drive or files and demands money in exchange for the decryption key.

Mass v. Targeted Malware

- Mass malware
  - Intended to infect as many machines as possible
  - Most common type
- Targeted malware
  - Tailored to a specific target
  - Very difficult to detect, prevent, and remove
  - Requires advanced analysis
  - Ex: Stuxnet

Malware Analysis Techniques and Tools

Two fundamental approaches to malware analysis: **Static and Dynamic**.

- Static analysis involves analysing the code or structure of a program to determine its function without running it.

- Dynamic analysis involves running the malware and observing its behaviour on the system. Before running the malware safely, you must set up an environment that will allow you to study the running malware without damaging to your system or network.

Technique involved in Static and Dynamic Analysis

Static analysis

- It involves analyzing the signature of the malware binary file which is a unique identification for the binary file.
- The binary file can be reverse-engineered using a disassembler such as IDA to convert the machine-executable code into assembly language code to make it human readable.
- Some of the techniques used for static analysis are file fingerprinting, virus scanning, memory dumping, packer detection, and debugging.

Dynamic analysis

- It involves analyzing the behaviour of malware in a sandbox environment so that it won’t affect other systems.
- Manual analysis is replaced by automated analysis through commercial sandboxes.

Approach

Static analysis

- uses a signature-based approach to malware detection and analysis.
- A signature is nothing but a unique identifier for a specific malware which is a sequence of bytes.
- Signature-based antimalware programs are effective against most common types of malware but are ineffective against sophisticated and advanced malware programs.

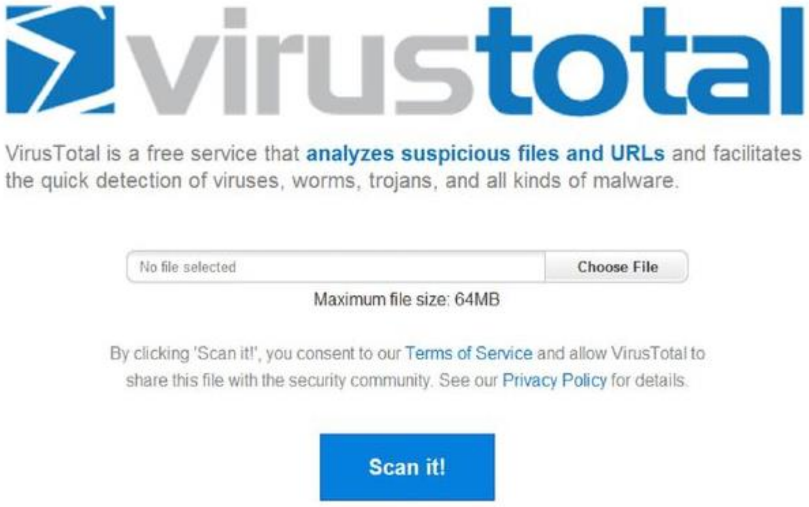
Dynamic analysis

- uses a behaviour-based approach to determine the functionality of the malware by studying the actions performed by the given malware.

Basic Static Analysis - Antivirus Scanning

- Rely on file signatures of known suspicious code, and behavioural and pattern-matching analysis (heuristics) to identify suspected files.
- Definition files contain file signatures for malware that have been encountered.
- Heuristics allow an antivirus program to identify new or modified types of malware, even without definition files.
- Because the various antivirus programs use different signatures and heuristics, it's useful to run several different antivirus programs against the same piece of suspected malware.

Basic Static Analysis - Antivirus Scanning



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 64MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

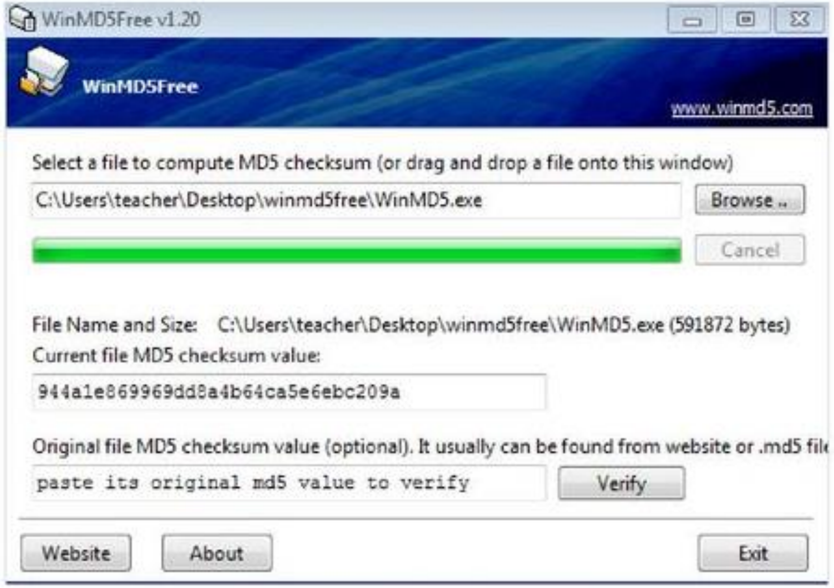
Source: https://www.virustotal.com/en/

VirusTotal allow you to upload a malware for scanning by multiple antivirus engines.

BASIC STATIC ANALYSIS - HASHING

- The malicious software is run through a hashing program that produces a unique hash (fingerprint) that identifies that malware.
- Message-Digest Algorithm 5 (MD5, 128-bit) hash function is the one most used for malware analysis.
- Secure Hash Algorithm 1 (SHA-1, 160-bit) hash function is also popular.
- Tools available: md5deep, WinMD5, md5sum

BASIC STATIC ANALYSIS - HASHING



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Users\teacher\Desktop\winmd5free\WinMD5.exe

File Name and Size: C:\Users\teacher\Desktop\winmd5free\WinMD5.exe (591872 bytes)

Current file MD5 checksum value:

944a1e869969dd8a4b64ca5e6ebc209a

Original file MD5 checksum value (optional). It usually can be found from website or .md5 fil

paste its original md5 value to verify

Source: http://www.winmd5.com/

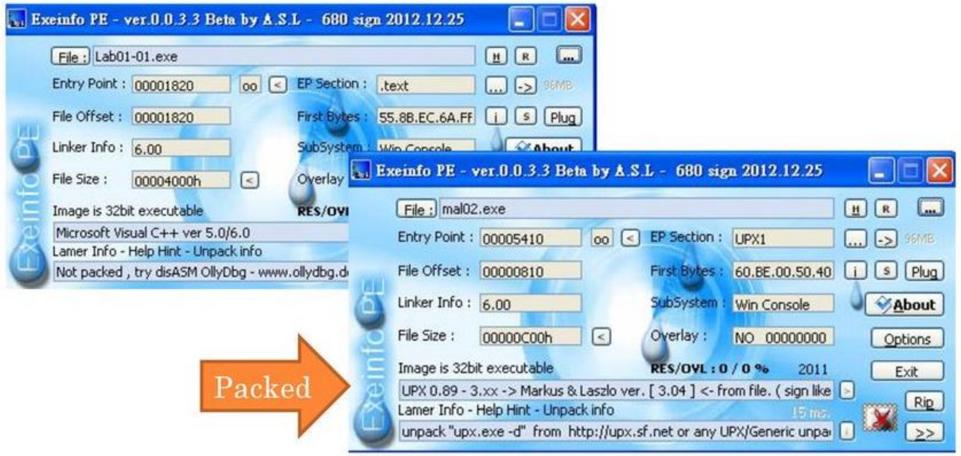
The unique hash of a malware can be used as:

- A label to identify the malware
- Share with other analysts to help them to identify malware
- Search for the hash online to see if the malware has already been identified

BASIC STATIC ANALYSIS - PACKED MALWARE

- To bypass firewalls and antivirus scanners, malware authors use packing or obfuscation to make their files more difficult to detect or analyse.
- Packers are software programs that compress and encrypt other executable files in a disk and restore the original executable images when the packed files are loaded into memories.
- Example: UPX (http://upx.sourceforge.net/)
- Before performing any analysis, the packed malware must be unpacked.

BASIC STATIC ANALYSIS - PACKED MALWARE



Exeinfo PE - ver.0.0.3.3 Beta by A.S.L - 680 sign 2012.12.25

File : Lab01-01.exe
Entry Point : 00001820
EP Section : .text
File Offset : 00001820
First Bytes : 55.8B.EC.6A.FF
Linker Info : 6.00
SubSystem : Win Console
File Size : 00004000h
Overlay
Image is 32bit executable
RES/OVI
Microsoft Visual C++ ver 5.0/6.0
Lamer Info - Help Hint - Unpack info
Not packed , try disASM OllyDbg - www.ollydbg.d

Exeinfo PE - ver.0.0.3.3 Beta by A.S.L - 680 sign 2012.12.25

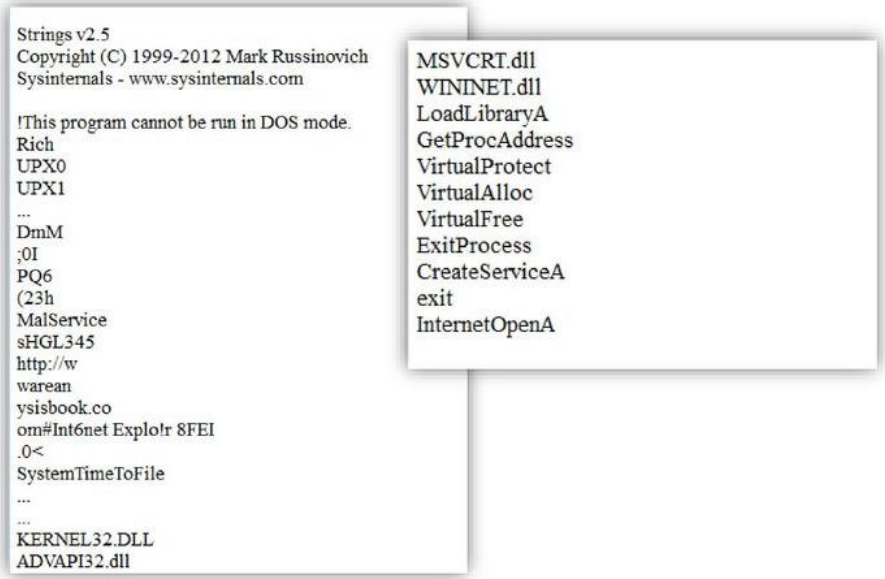
File : mal02.exe
Entry Point : 00005410
EP Section : UPX1
File Offset : 00000810
First Bytes : 60.BE.00.50.40
Linker Info : 6.00
SubSystem : Win Console
File Size : 00000C00h
Overlay : NO 00000000
Image is 32bit executable
RES/OVL : 0 / 0 % 2011
UPX 0.89 - 3.xx -> Markus & Laszlo ver. [3.04] <- from file. (sign like
Lamer Info - Help Hint - Unpack info
15 ms.
unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpa

PEiD and Exeinfo PE are two popular packer detectors.

BASIC STATIC ANALYSIS - STRING SEARCHING

- Strings in an executable are typically stored in either ASCII (1 byte/character) or Unicode format (2 bytes/character).
- A program may contain strings if it prints a message, connects to a website (URL), copies a file to a specific location.
- Searching through the strings can be a simple way to get hints about the functionality of a program.
- Tool: Windows Sysinternals Utilities: Strings

BASIC STATIC ANALYSIS - STRING SEARCHING



```
Strings v2.5
Copyright (C) 1999-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
...
DmM
;0I
PQ6
(23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
...
...
KERNEL32.DLL
ADVAPI32.dll
```

```
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
```

Results of running Strings against a file

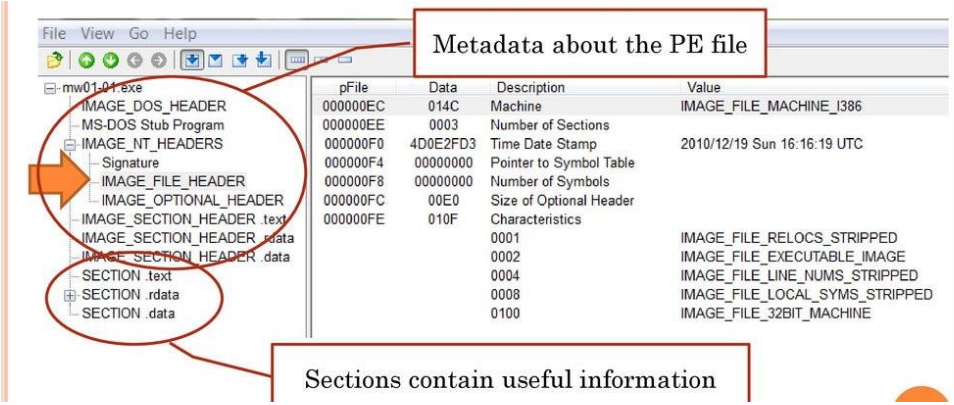
BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT

- The Portable Executable (PE) format is a file format for executables, object code, DLLs, used in 32-bit and 64-bit versions of Windows operating systems.
- PE files begin with a header that includes information about the code, the type of application, required library functions, and space requirements.
- Nearly every file with executable code that is loaded by Windows is in the PE file format. So the information in the PE header is of great value to the malware analyst.

BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT

- The most useful pieces of information about an executable is the list of functions that it imports.
- Imports are functions used by one program that are actually stored in a different program, such as code libraries that contain functionality common to many programs.
- Code libraries can be connected to the main executable by statically, at runtime, or dynamically linking. Dynamic linking is the most common.
- Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) and builds a hierarchical tree diagram of all dependent modules.

BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT



Metadata about the PE file

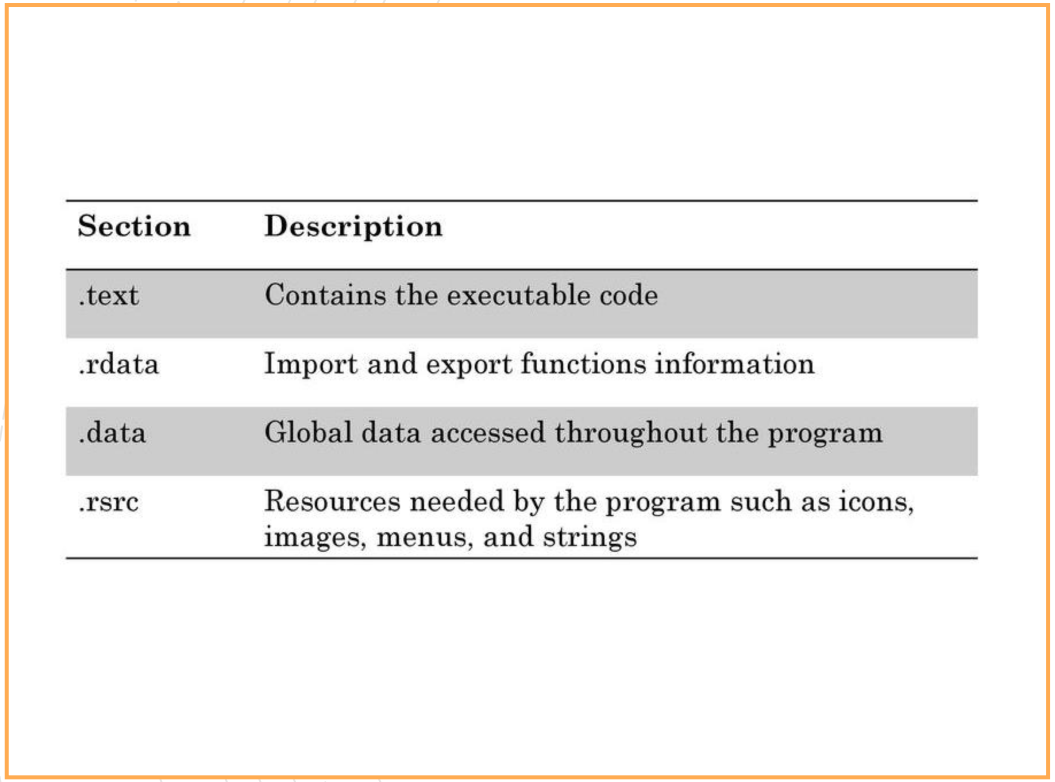
```
mw01-01.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  SECTION .text
  SECTION .rdata
  SECTION .data
```

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

Sections contain useful information

- Using PEview to analyze malware

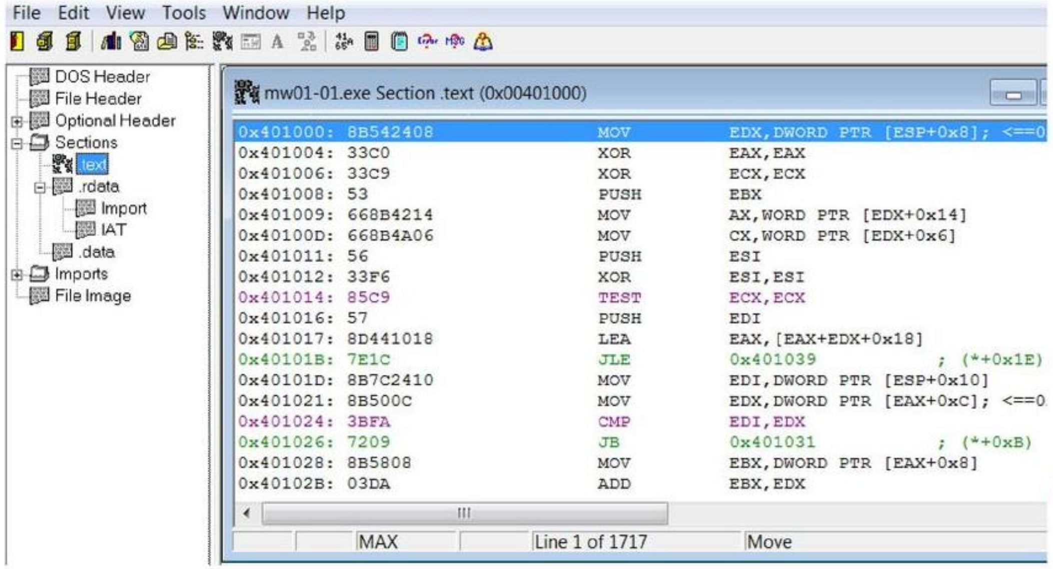
BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT



Section	Description
.text	Contains the executable code
.rdata	Import and export functions information
.data	Global data accessed throughout the program
.rsrc	Resources needed by the program such as icons, images, menus, and strings

Common sections in a PE file

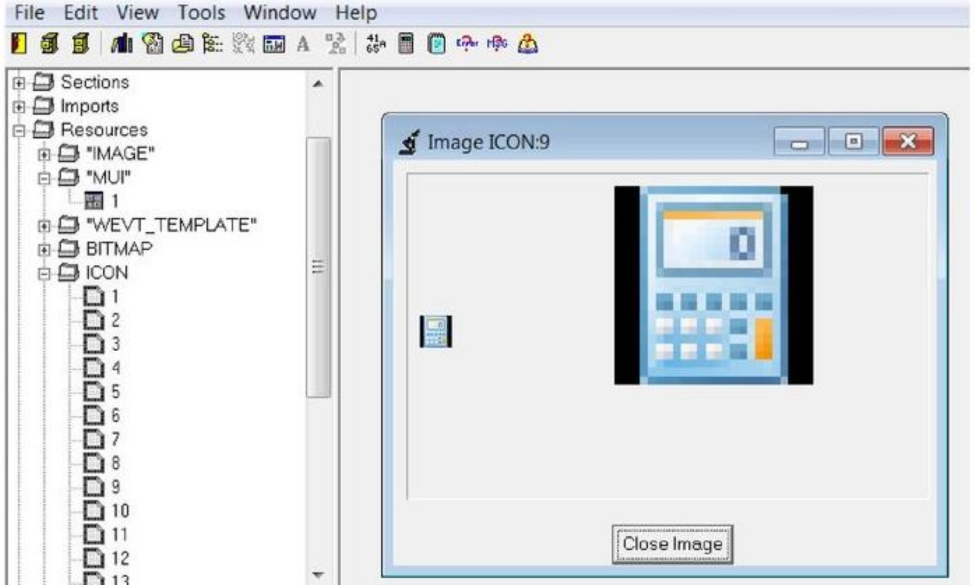
BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT



```
0x401000: 8B542408          MOV     EDX,DWORD PTR [ESP+0x8]; <==0
0x401004: 33C0              XOR     EAX,EAX
0x401006: 33C9              XOR     ECX,ECX
0x401008: 53                PUSH    EBX
0x401009: 668B4214          MOV     AX,WORD PTR [EDX+0x14]
0x40100D: 668B4A06          MOV     CX,WORD PTR [EDX+0x6]
0x401011: 56                PUSH    ESI
0x401012: 33F6              XOR     ESI,ESI
0x401014: 85C9              TEST    ECX,ECX
0x401016: 57                PUSH    EDI
0x401017: 8D441018          LEA     EAX,[EAX+EDX+0x18]
0x40101B: 7E1C              JLE     0x401039          ; (*+0x1E)
0x40101D: 8B7C2410          MOV     EDI,DWORD PTR [ESP+0x10]
0x401021: 8B500C            MOV     EDX,DWORD PTR [EAX+0xC]; <==0
0x401024: 3BFA              CMP     EDI,EDX
0x401026: 7209              JB      0x401031          ; (*+0xB)
0x401028: 8B5808            MOV     EBX,DWORD PTR [EAX+0x8]
0x40102B: 03DA              ADD     EBX,EDX
```

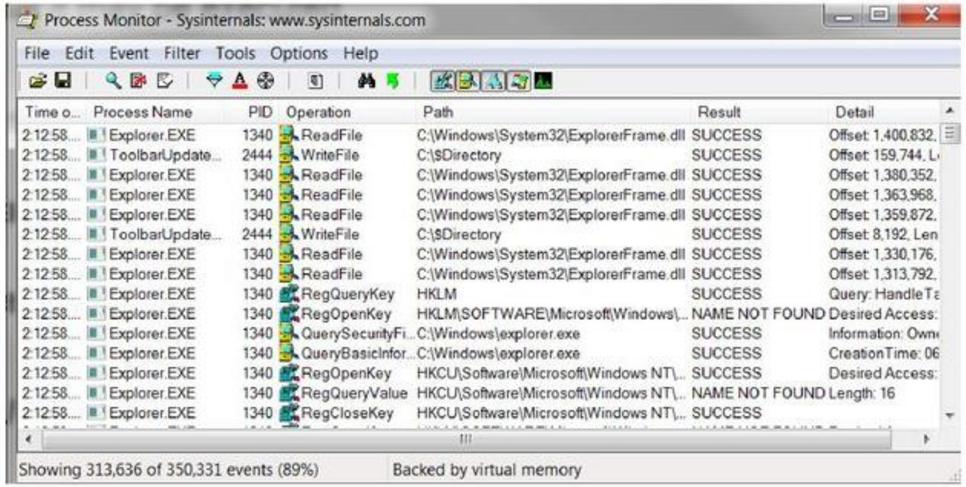
Using PEBrowse Professional to disassemble the .text section of a malware

BASIC STATIC ANALYSIS - PORTABLE EXECUTABLE FILE FORMAT



Using PEBrowse Professional to view the .rsrc section of a program

BASIC DYNAMIC ANALYSIS - KEY TOOLS



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,400,832,
2:12:58....	ToolbarUpdate...	2444	WriteFile	C:\$Directory	SUCCESS	Offset: 159,744, L
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,380,352,
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,363,968,
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,359,872,
2:12:58....	ToolbarUpdate...	2444	WriteFile	C:\$Directory	SUCCESS	Offset: 8,192, Len
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,330,176,
2:12:58....	Explorer.EXE	1340	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1,313,792,
2:12:58....	Explorer.EXE	1340	RegQueryKey	HKLM	SUCCESS	Query: HandleTa
2:12:58....	Explorer.EXE	1340	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access:
2:12:58....	Explorer.EXE	1340	QuerySecurityFi...	C:\Windows\explorer.exe	SUCCESS	Information: Own
2:12:58....	Explorer.EXE	1340	QueryBasicInfor...	C:\Windows\explorer.exe	SUCCESS	CreationTime: 06
2:12:58....	Explorer.EXE	1340	RegOpenKey	HKCU\Software\Microsoft\Windows NT\...	SUCCESS	Desired Access:
2:12:58....	Explorer.EXE	1340	RegQueryValue	HKCU\Software\Microsoft\Windows NT\...	NAME NOT FOUND	Length: 16
2:12:58....	Explorer.EXE	1340	RegCloseKey	HKCU\Software\Microsoft\Windows NT\...	SUCCESS	

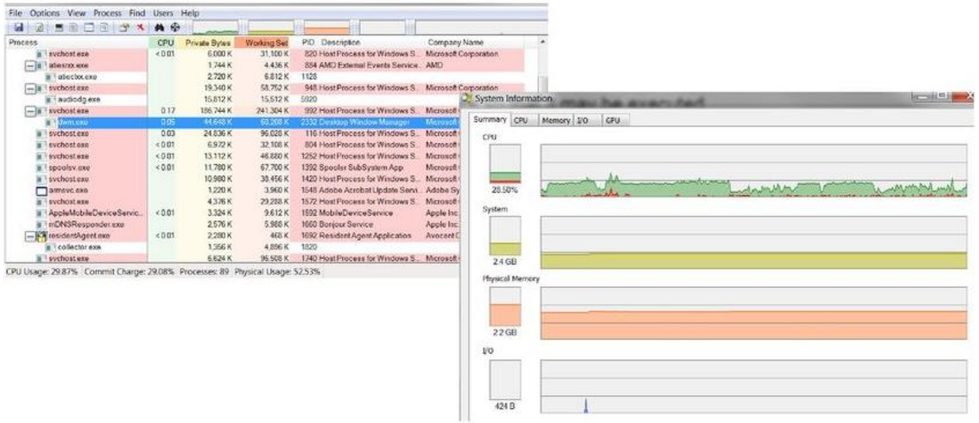
Showing 313,636 of 350,331 events (89%) Backed by virtual memory

Processor Monitor (procmon)

Source: Microsoft

An advanced monitoring tool for Windows that shows real-time file system, registry and process/thread activity.

BASIC DYNAMIC ANALYSIS - KEY TOOLS



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	6,000 K	31,100 K	820	Host Process for Windows S...	Microsoft Corporation
atiesrxx.exe		1,744 K	4,436 K	884	AMD External Events Service...	AMD
atieclxx.exe		2,720 K	6,812 K	1128		
svchost.exe		19,340 K	58,752 K	948	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,812 K	15,512 K	5920		
svchost.exe	0.17	186,744 K	241,304 K	992	Host Process for Windows S...	Microsoft
dwm.exe	0.05	44,648 K	60,208 K	2332	Desktop Window Manager	Microsoft
svchost.exe	0.03	24,836 K	96,028 K	116	Host Process for Windows S...	Microsoft
svchost.exe	< 0.01	6,972 K	32,108 K	804	Host Process for Windows S...	Microsoft
svchost.exe	< 0.01	13,112 K	46,880 K	1252	Host Process for Windows S...	Microsoft
spoolsv.exe	< 0.01	11,780 K	67,700 K	1392	Spooler SubSystem App	Microsoft
svchost.exe		10,980 K	38,456 K	1420	Host Process for Windows S...	Microsoft
armsvc.exe		1,220 K	3,960 K	1548	Adobe Acrobat Update Servi...	Adobe Sy
svchost.exe		4,376 K	29,288 K	1572	Host Process for Windows S...	Microsoft
AppleMobileDeviceServic...	< 0.01	3,324 K	9,612 K	1592	MobileDeviceService	Apple Inc.
mDNSResponder.exe		2,576 K	5,988 K	1660	Bonjour Service	Apple Inc.
residentAgent.exe	< 0.01	2,280 K	468 K	1692	Resident Agent Application	Avocent C
collector.exe		1,356 K	4,896 K	1820		
svchost.exe		6,624 K	96,508 K	1740	Host Process for Windows S...	Microsoft

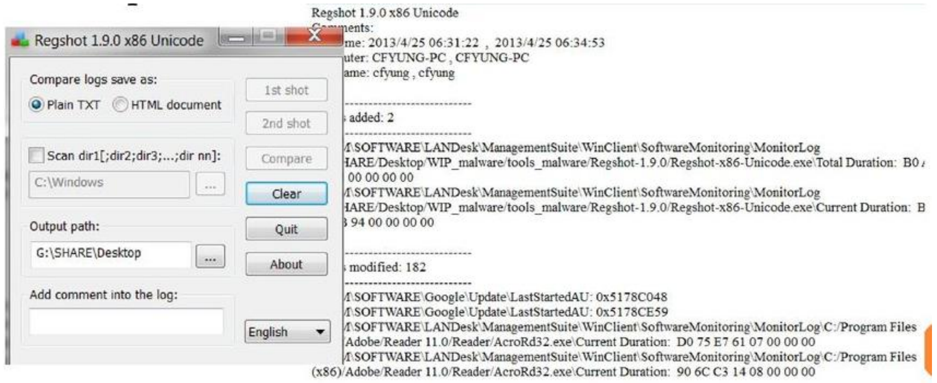
CPU Usage: 29.87% Commit Charge: 29.08% Processes: 89 Physical Usage: 52.53%

Process Explorer

Source: Microsoft

List active processes, DLLs loaded by a process and overall system information.

BASIC DYNAMIC ANALYSIS - KEY TOOLS



Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

Output path:

G:\SHARE\Desktop

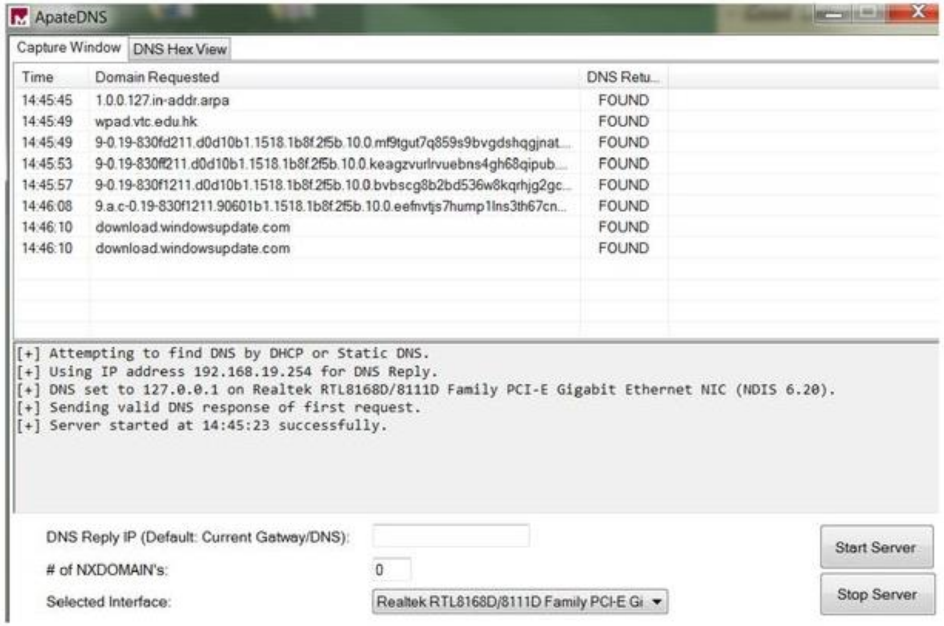
Add comment into the log:

```
Regshot 1.9.0 x86 Unicode
C   nents:
me: 2013/4/25 06:31:22 , 2013/4/25 06:34:53
uter: CFYUNG-PC , CFYUNG-PC
ame: cfyung , cfyung

----------------------------
 added: 2
----------------------------
\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog
ARE/Desktop/WIP_malware/tools_malware/Regshot-1.9.0/Regshot-x86-Unicode.exe\Total Duration:  B0 
 00 00 00 00
\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog
ARE/Desktop/WIP_malware/tools_malware/Regshot-1.9.0/Regshot-x86-Unicode.exe\Current Duration:  B
 94 00 00 00 00

----------------------------
 modified: 182
----------------------------
\SOFTWARE\Google\Update\LastStartedAU: 0x5178C048
\SOFTWARE\Google\Update\LastStartedAU: 0x5178CE59
\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog\C:/Program Files
Adobe/Reader 11.0/Reader/AcroRd32.exe\Current Duration:  D0 75 E7 61 07 00 00 00
\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog\C:/Program Files
(x86)/Adobe/Reader 11.0/Reader/AcroRd32.exe\Current Duration:  90 6C C3 14 08 00 00 00
```

Regshot

An open source registry comparison tool that allows you to take and compare two registry snap-shots.

BASIC DYNAMIC ANALYSIS - KEY TOOLS



Time	Domain Requested	DNS Retu...
14:45:45	1.0.0.127.in-addr.arpa	FOUND
14:45:49	wpad.vtc.edu.hk	FOUND
14:45:49	9-0.19-830fd211.d0d10b1.1518.1b8f.2f5b.10.0.mf9tgut7q859s9bvgdshqgjnat...	FOUND
14:45:53	9-0.19-830ff211.d0d10b1.1518.1b8f.2f5b.10.0.keagzvurlrvuebns4gh68qipub...	FOUND
14:45:57	9-0.19-830f1211.d0d10b1.1518.1b8f.2f5b.10.0.bvbscg8b2bd536w8kqrhjg2gc...	FOUND
14:46:08	9.a.c-0.19-830f1211.90601b1.1518.1b8f.2f5b.10.0.eefnvtjs7hump1lns3th67cn...	FOUND
14:46:10	download.windowsupdate.com	FOUND
14:46:10	download.windowsupdate.com	FOUND

```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 192.168.19.254 for DNS Reply.
[+] DNS set to 127.0.0.1 on Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet NIC (NDIS 6.20).
[+] Sending valid DNS response of first request.
[+] Server started at 14:45:23 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS):

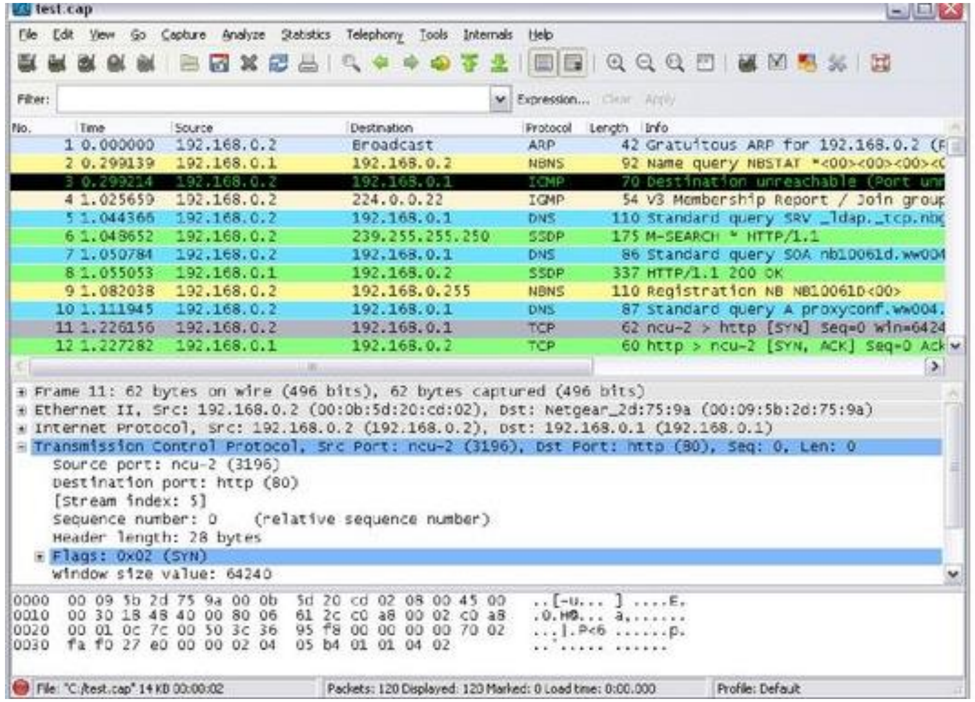
# of NXDOMAIN's: 0

Selected Interface: Realtek RTL8168D/8111D Family PCI-E Gi

ApateDNS

A free tool to capture DNS requests made by malware.

BASIC DYNAMIC ANALYSIS - KEY TOOLS


test.cap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.    Time       Source         Destination      Protocol  Length  Info
     1 0.000000   192.168.0.2    Broadcast        ARP         42 Gratuitous ARP for 192.168.0.2 (R
     2 0.299139   192.168.0.1    192.168.0.2      NBNS        92 Name query NBSTAT *<00><00><00><C
     3 0.299214   192.168.0.2    192.168.0.1      ICMP        70 Destination unreachable (Port unr
     4 1.025659   192.168.0.2    224.0.0.22       IGMP        54 V3 Membership Report / Join group
     5 1.044366   192.168.0.2    192.168.0.1      DNS        110 Standard query SRV _ldap._tcp.nbc
     6 1.048652   192.168.0.2    239.255.255.250  SSDP       175 M-SEARCH * HTTP/1.1
     7 1.050784   192.168.0.2    192.168.0.1      DNS         86 Standard query SOA nb10061d.ww004
     8 1.055053   192.168.0.1    192.168.0.2      SSDP       337 HTTP/1.1 200 OK
     9 1.082038   192.168.0.2    192.168.0.255    NBNS       110 Registration NB NB10061D<00>
    10 1.111945   192.168.0.2    192.168.0.1      DNS         87 Standard query A proxyconf.ww004.
    11 1.226156   192.168.0.2    192.168.0.1      TCP         62 ncu-2 > http [SYN] Seq=0 Win=6424
    12 1.227282   192.168.0.1    192.168.0.2      TCP         60 http > ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size value: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 | Profile: Default

Wireshark

An open source sniffer to intercept and log network traffic.

BASIC DYNAMIC ANALYSIS - PRACTICAL STEPS

Basic dynamic analysis can assist and confirm the findings obtained from basic static analysis.

Step 1: Baseline

Before executing the malware, take a first snapshot of registry using Regshot.

Step 2: System status

During the running of malware, start Process Monitor and Process Explorer. Note any changes occurred.

BASIC DYNAMIC ANALYSIS - PRACTICAL STEPS

Step 3: Network traffic

Using ApateDNS and Wireshark to log network traffic generated by the malware.

Step 4: Comparison

Waiting for the malware to finish making any system changes. Take a second snapshot using Regshot. Compare the differences between two snapshots.

Understanding of Sample Malware

CryptoLocker

- CryptoLocker is a ransomware Trojan.
- Believed to have first been posted to the Internet on 5 September 2013.
- Smart enough to travel across your network and encrypt any files located on shared network drives.
- Uses AES-265 or RSA public-key cryptography, with the private key stored only on the malware's control servers.

CryptoLocker a.k.a Ransomware

- After Encryption, displays a message and popup which offers to decrypt the data if payment is made within stated deadline, and threatened to delete the private key if the deadline passes.
- Ransomwares generally has a 48-72 hour deadline which, once passed, causes the ransom to increase or leads to key deletion.
- Most ransoms start in the $100-$500 area or 0.5 BTC to 4 BTC.

Symptoms

- You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
- An alarming message has been set to your desktop background with instructions on how to pay to unlock your files.
- The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files.
- A window has opened to a ransomware program and you cannot close it.
- You have files with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML

Symptoms

you see a files similar to:

%PUBLIC% \desktop\help_restore_files_<random text>.html

%PUBLIC% \desktop\restore_files_<random text>.txt

%PUBLIC% \documents\help_restore_files _<random text>.txt

%PUBLIC% \documents\restore_files_<random text>.html

%PUBLIC% \favorites\restore_files_<random text>.html

%PUBLIC% \favorites\restore_files_<random text>.txt

CryptoLocker.lnk

HELP_TO_DECRYPT_YOUR_FILES.TXT

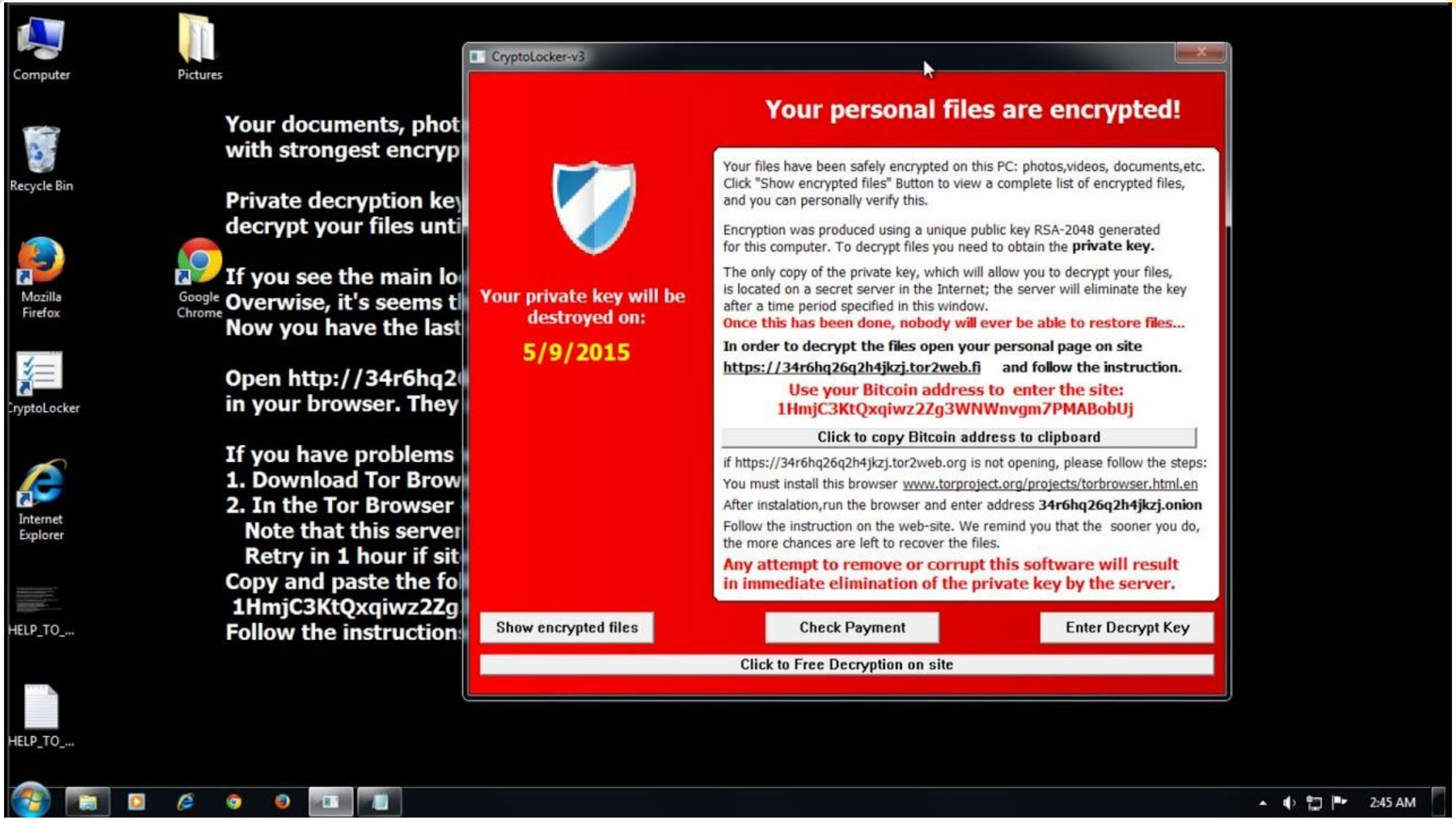
HELP_TO_DECRYPT_YOUR_FILES.BMP

HELP_TO_SAVE_FILES.bmp

HELP_TO_SAVE_FILES.txt

key.dat

log.html



CryptoLocker-v3

Your personal files are encrypted!

Your private key will be destroyed on:

5/9/2015

Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.

Use your Bitcoin address to enter the site:
1HmjC3KtQxqiwz2Zg3WNWnvgm7PMABobUj

Click to copy Bitcoin address to clipboard

if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Show encrypted files | Check Payment | Enter Decrypt Key

Click to Free Decryption on site

Your documents, phot
with strongest encryp

Private decryption key
decrypt your files unti

If you see the main lo
Overwise, it's seems t
Now you have the last

Open http://34r6hq2
in your browser. They

If you have problems
1. Download Tor Brow
2. In the Tor Browser
Note that this server
Retry in 1 hour if sit
Copy and paste the fo
1HmjC3KtQxqiwz2Zg
Follow the instruction

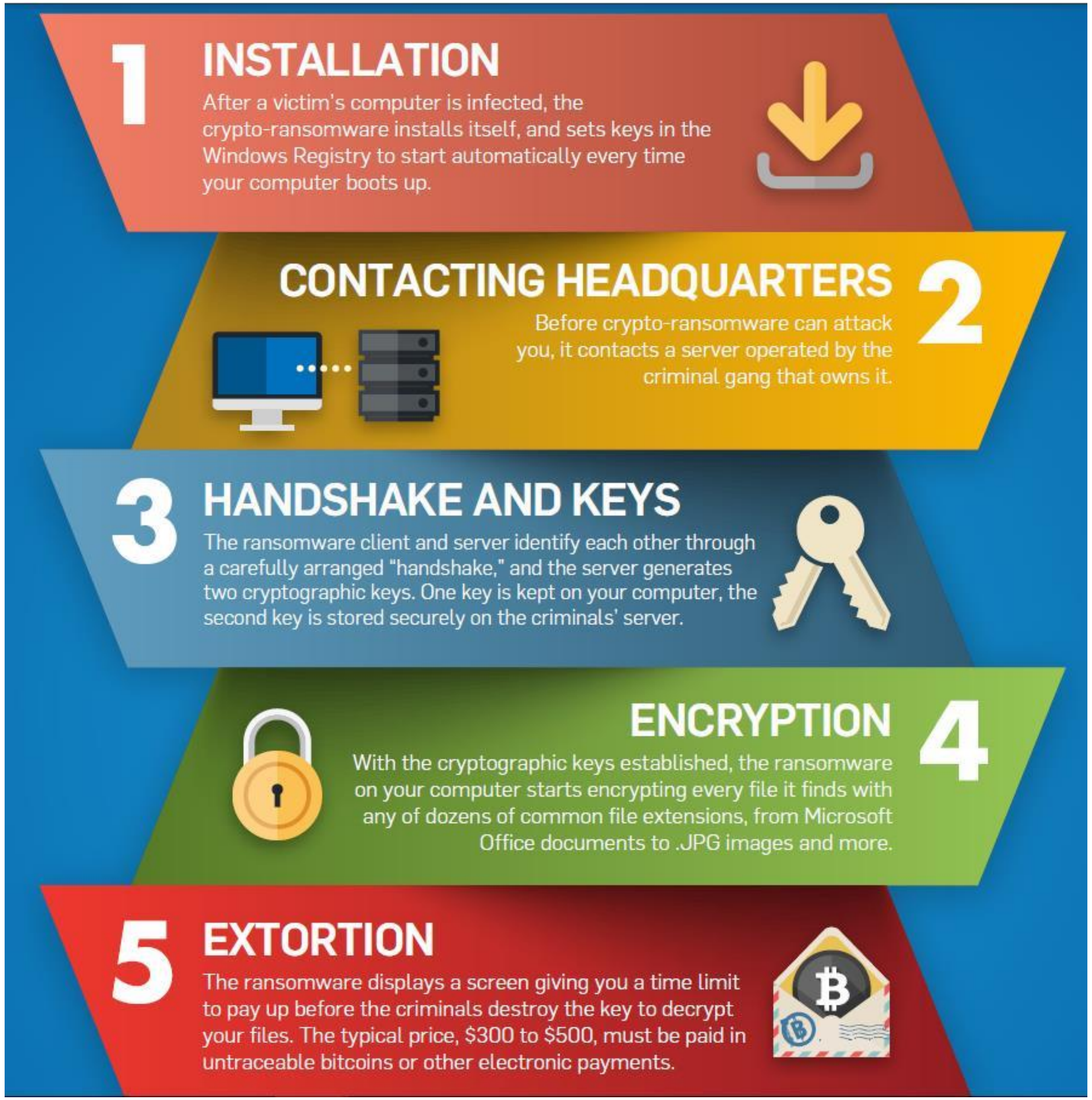
CryptoLocker Propagation

Propagate via

- phishing emails
- unpatched programs
- compromised websites
- online advertising
- free software downloads
- Prior existing Botnet

Understanding CryptoLocker Working

Anatomy of CryptoLocker



1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.

CONTACTING HEADQUARTERS 2

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.

3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.

ENCRYPTION 4

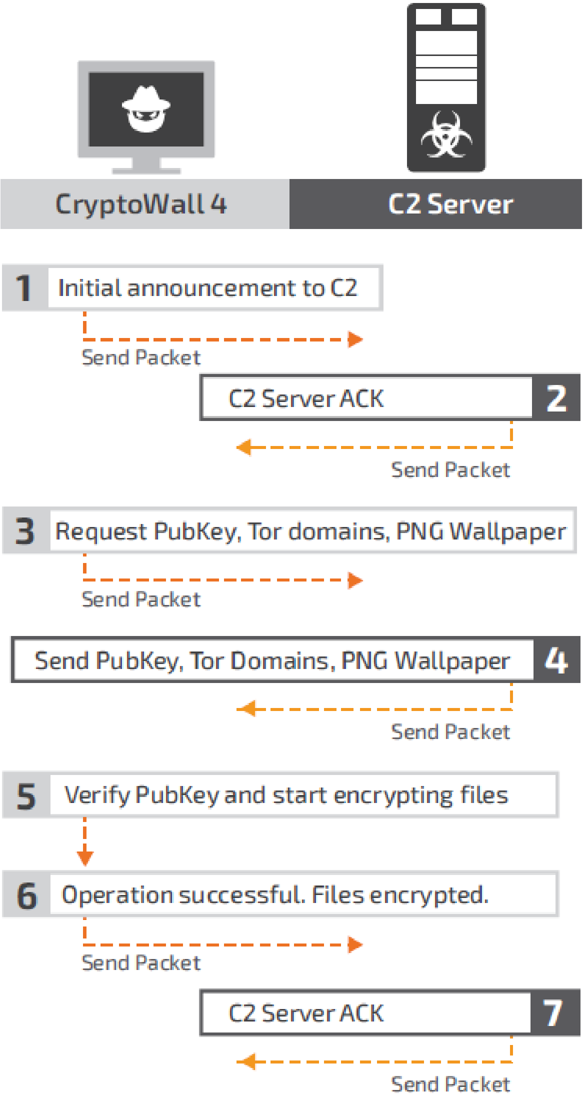
With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, $300 to $500, must be paid in untraceable bitcoins or other electronic payments.

Source: Sophos

CryptoWall network communication process with C2 server



1 Initial announcement to C2

C2 Server ACK 2

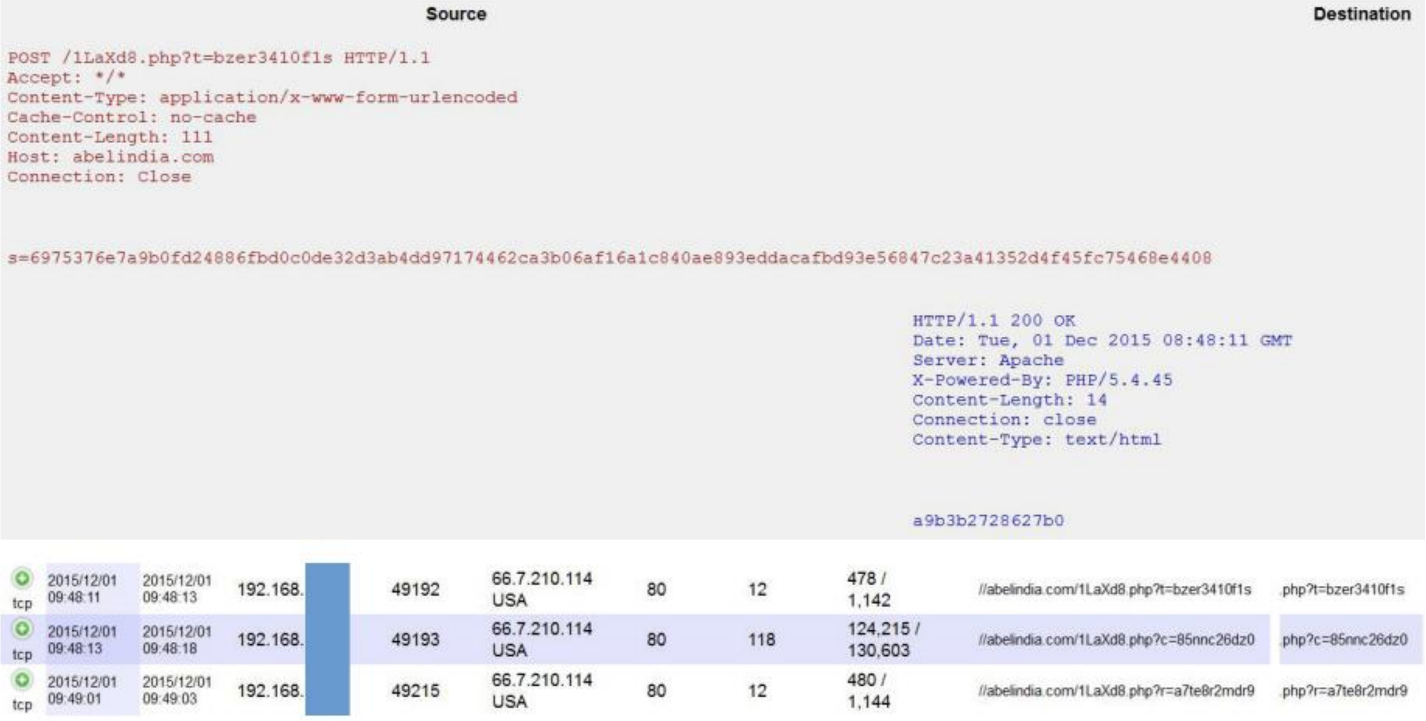
3 Request PubKey, Tor domains, PNG Wallpaper

Send PubKey, Tor Domains, PNG Wallpaper 4

5 Verify PubKey and start encrypting files

6 Operation successful. Files encrypted.

C2 Server ACK 7

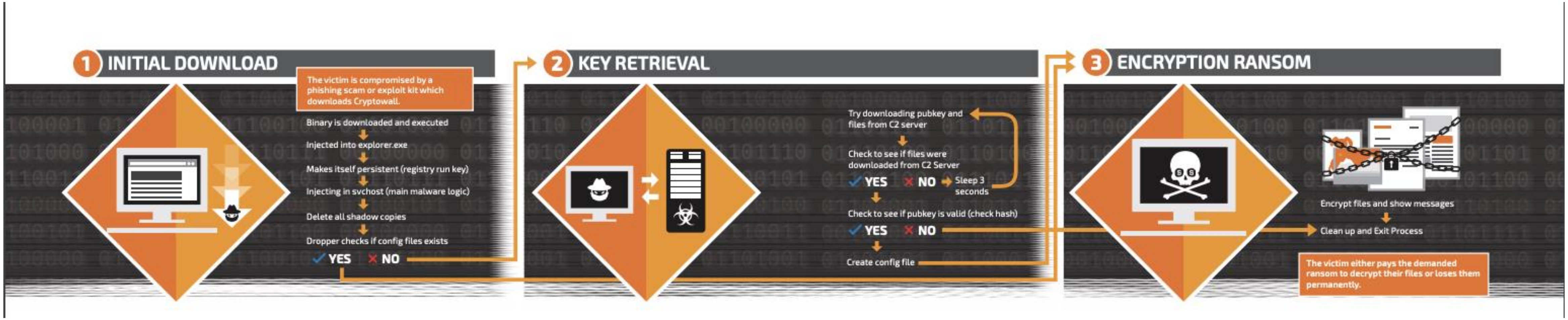


```
POST /1LaXd8.php?t=bzer3410f1s HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 111
Host: abelindia.com
Connection: Close


s=6975376e7a9b0fd24886fbd0c0de32d3ab4dd97174462ca3b06af16a1c840ae893eddacafbd93e56847c23a41352d4f45fc75468e4408
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Dec 2015 08:48:11 GMT
Server: Apache
X-Powered-By: PHP/5.4.45
Content-Length: 14
Connection: close
Content-Type: text/html


a9b3b2728627b0
```

tcp	2015/12/01 09:48:11	2015/12/01 09:48:13	192.168.	[redacted]	49192	66.7.210.114 USA	80	12	478 / 1,142	//abelindia.com/1LaXd8.php?t=bzer3410f1s	php?t=bzer3410f1s
tcp	2015/12/01 09:48:13	2015/12/01 09:48:18	192.168.	[redacted]	49193	66.7.210.114 USA	80	118	124,215 / 130,603	//abelindia.com/1LaXd8.php?c=85nnc26dz0	php?c=85nnc26dz0
tcp	2015/12/01 09:49:01	2015/12/01 09:49:03	192.168.	[redacted]	49215	66.7.210.114 USA	80	12	480 / 1,144	//abelindia.com/1LaXd8.php?r=a7te8r2mdr9	php?r=a7te8r2mdr9

Technical infection process of CryptoWall



1 INITIAL DOWNLOAD

The victim is compromised by a phishing scam or exploit kit which downloads Cryptowall.

Binary is downloaded and executed

Injected into explorer.exe

Makes itself persistent (registry run key)

Injecting in svchost (main malware logic)

Delete all shadow copies

Dropper checks if config files exists

✓ YES ✗ NO

2 KEY RETRIEVAL

Try downloading pubkey and files from C2 server

Check to see if files were downloaded from C2 Server

✓ YES ✗ NO → Sleep 3 seconds

Check to see if pubkey is valid (check hash)

✓ YES ✗ NO

Create config file

3 ENCRYPTION RANSOM

Encrypt files and show messages

Clean up and Exit Process

The victim either pays the demanded ransom to decrypt their files or loses them permanently.

Malware Analyst Job Function

- the primary function of a malware analyst is to identify, examine, and understand various forms of malware and their delivery methods
- after the organization's incident response team has identified and contained an attack the malware analyst will be called upon to disassemble, deconstruct, and reverse engineer the malicious code in an effort to allow the security team to better protect against a future attack of the same or similar origins and capabilities.
- malware analysts can sometimes be called in during the early stages of an attack to bring clarity to the type of attack and the methods being used by the attackers.
- malware analyst to play a significant role in mitigation and recovery efforts once the attack vector has been identified and the payload contained.
- malware analyst also help to examine and protect against the attack before harm is done.

Job Description and Skills set required

- IDA Pro, WinDbg, OllyDbg, Immunity Debugger
- Strong knowledge of C/C++, Windows API, and Windows OS internals
- Reconstruct unknown file formats & data structures
- Reconstruct unknown TCP/IP protocols
- Understand unpacking, deobfuscation, and anti-debugging techniques
- Python, Perl, Ruby scripting
- Ability to write technical reports

Commonly job responsibilities will include:

- Record malware threats and identify systems to avoid them
- Examine programs and software using analysis programs to identify threats
- Classify malware based on threats and characteristics
- Stay up to date on the latest malware and keep software updated to defend against them
- Write alerts to keep the security team informed
- Help create documentation for security policies
- Understand tools that identify zero-day cyber threats

Need of Malware Analyst

- The global malware analysis market size is expected to grow from USD 3.0 billion in 2019 to USD 11.7 billion in 2024 at a CAGR of 31.0% Source: Secondary Research, Expert Interviews and MarketsandMarkets analysis
- As commerce in the todays world becoming more and more computerized and internet-based, the need for malware analysts continues to rise.
- Every month, new forms of malicious code are deployed across the globe. That trend is not likely to change.
- As there is increase in adoption of IoT & BYOD trend and rise in malware and phishing threats among organizations it drives the growth of the global malware analysis market
- The outbreak of COVID-19 has mandated work from home practice for most of the organizations across the world. Hence there's been an increasing focus on securing remote infrastructure and IP of the respective companies on account of remote service programs from malware attacks.

Demo

InventOnUs

Invent | Optimize | Utilize

We are a global technology consulting and internal audit firm composed of experts specializing in consultancy in domains such as Information Security, Risk and Advisory services. We enable organizations solve problems in finance and transactions, operations, technology, litigation, governance, risk and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East and Africa.

We believe in simplifying the complexity of the business using our deep knowledge and expertise in the corporate sector. We take pride in our ability to provide quality services whether they are an owner-managed business or a large multinational corporation. We are a multi-skilled, multi-disciplined firm, offering clients a wide range of industry-focused business solutions. Investing in our people means our clients get world-class expertise to solve their complex business problems.

About Us

Our Management Team

Hemant Dusane

Hemant is a CEO at InventOnUs. A Cyber Security & IT Risk Management Professional offering 15 years experience in well-known organizations. He lead a highly technical team, incorporating analytical, operational, research & development and vulnerability assessment skills in Information Security Risk management field within the organization. He is an active cyber security evangelist & speaker in various national and international forums. He has won various security awards for overall contribution to Information Risk Management field. He is a CISA, CCISO, PCI-DSS, RSA_DLP, ISO27K LA, ISO20K LA, BS100012:2017 PIMS and GDPR Lead Implementer, MTech Computer Science

Ketan Shah

Ketan is a CTO at InventOnUs. With over 9+ years of experience as Technical, Risk & Compliance expert with a solid reputation for implementing and managing security controls by skillfully evaluating strategic workflow business & organization systems, a team spirit combining technology & project management expertise at a strategic & tactical level to strengthen IT security, support growth & build productivity. His expertise are Network & System Security, Vulnerability Assessment, Penetration Testing, Technical Specification Development & Cloud Security. He is a ECSA, CEH, MCITP, CCNA, ISO27K LA, MCSA certified.

Eswar Muthukrishnan

Eswar is a COO at InventOnUs. He has over 25 years of experience in the IT field having worked in various senior roles like CIO, Vice-President, Director for organizations such as Genpact, BT, Infosys. An information technology specialist with extensive experience in delivering outsourcing solutions to large organizations from US, Europe to Australia. Managed large teams with expertise in all aspects of information technology like data center management, networking, security, as well as management of such activities. An alumni of IIM(Ahmedabad), NIT(Trichy). Eswar is a CISA, PCI-DSS, (CEH),(CISSP)(ISO27K LA), ITIL Manager as well as Six Sigma Green Belt.

Chandan Chourasiya

Chandan is Director-Finance at InventOnUs. He has over 15 years of experience in the fields statutory audit, assurance, internal audit, IT audit, Fraud investigation & taxation. Chandan's expertise is in risk compliance & he specializes in technical system audits, security, internal controls, data analysis, SOX & SSAE 16 Assurance. Chandan was board member of ISACA Pune Chapter and has also served on ISACA HQ committees of like Young Professional (YP) & Communities Committee. He contributed in ISACA's purpose by providing suggestions & planning a framework for YP & Communities Committee. He is a CA, CISA, CIA and CFE.

Q & A

Thank You