

## **Malware Analysis**

### **Executive Summary**

The Malware file analysed is the malware known as Venus Locker. Venus Locker is a dangerous ransomware that encrypts all the files in the user's system and demands a ransom in exchange for the decryption tool and the private key. The malware presents the user with a deadline of 72 hours to pay the ransom by. Upon not meeting this deadline, the malware authors claim that the private key required to decrypt the files will be deleted automatically. The information presented below is a concise representation of the analysis done on the malware.

### **Basic Static Analysis**

The program is not packed as inferred from PeiD. In addition, we can observe that the virtual size and the raw data size of the .text section are roughly the same further confirming that the program is unpacked. It is compiled using Microsoft Visual C# and is written in .NET. The malware was compiled on the 29th of July 2016 at 1:32 AM UTC as seen from PEview and is a Windows GUI application. This particular sample has an MD5 hash of 8675FFB697AD944748E0E24AC1A962CE.

The program's resources can be viewed using Resource Hacker. We observe an icon representing a Lock icon, suggesting that the malware locks files and prevents the user from accessing them. We also see the name of the malware "Venus Locker" referenced in the resources. The resources are presented below.

The program consists of 3 sections. .text, .rsrc, and .reloc sections. The sections and contents are shown below.

On observing the indicators using PESTudio, we see that the program references 3 urls as shown. We investigate further what these urls do in later sections.

The libraries and functions imported are of particular interest. Though the program does not appear to be packed, there only seems to be one dll imported - mscorere.dll which is a Microsoft .NET runtime execution library. Correspondingly, the only function that is referenced is \_CorExeMain which is presumed to be the main function that drives the malware. We assume that the malware imports the rest of its functionality dynamically.

There are also a large number of strings that are of concern. We provide a few important ones. We see a very large number of file extensions. These extensions are found within the strings in two sets containing nothing in common. This suggests that the malware has different functionality depending on the extension of the file selected. We investigate this further later.

We see a number of strings related to cryptography like "System.security.cryptography", "Encoding", "SHA256", "CipherMode" and more further confirming that the program does some sort of encryption. We also see a large number of strings pertaining to certain programs or folders like "Avira", "Internet Explorer", "Adobe", "google" etc. This suggests that the program does some sort of special function for these programs or files belonging to these organizations. We see a number of url's being referenced as well as a tor email "[VenusLocker@mail2tor.com](mailto:VenusLocker@mail2tor.com)" which is most likely the address the victim has to send the ransom bitcoins to.

Of particular interest is one string "OfflineAESKey". This informs us that the program contains some hard coded key value for its AES encryption scheme which provides a point of attack

against the malware for analysts. There are also strings like “RSAkeylength” which could suggest the same for the RSA key used.

Another string is the file name “\U2FsdGVKX1DKeR.vluni”. This is a file that is created when the malware is run and is examined further later.

Finally, we see two strings which can be assumed to be pertaining to the AES key and the RSA key respectively as shown below.

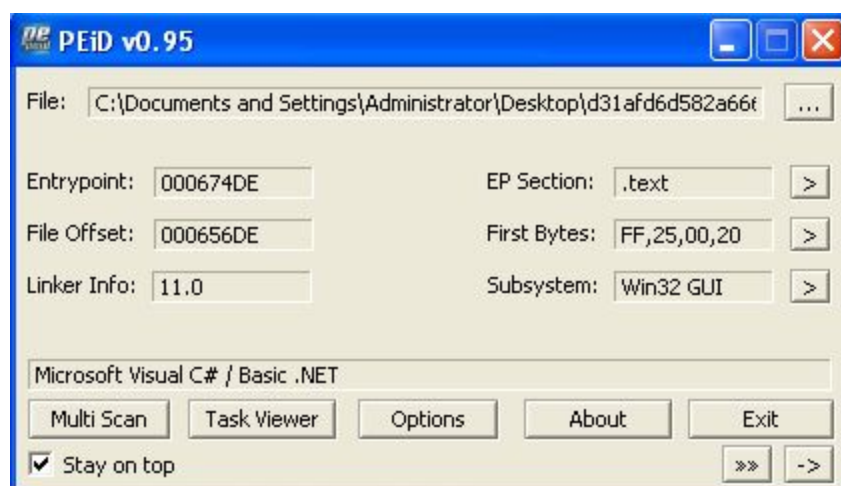


Fig.1 Basic .NET program

00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
00000086	0003	Number of Sections	
00000088	579AB237	Time Date Stamp	2016/07/29 Fri 01:32:39 UTC
0000008C	00000000	Pointer to Symbol Table	
00000090	00000000	Number of Symbols	
00000094	00E0	Size of Optional Header	
00000096	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

Fig.2 Compile date

-----	-----	-----	
000000DC	0002	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI

Fig.3 Windows GUI

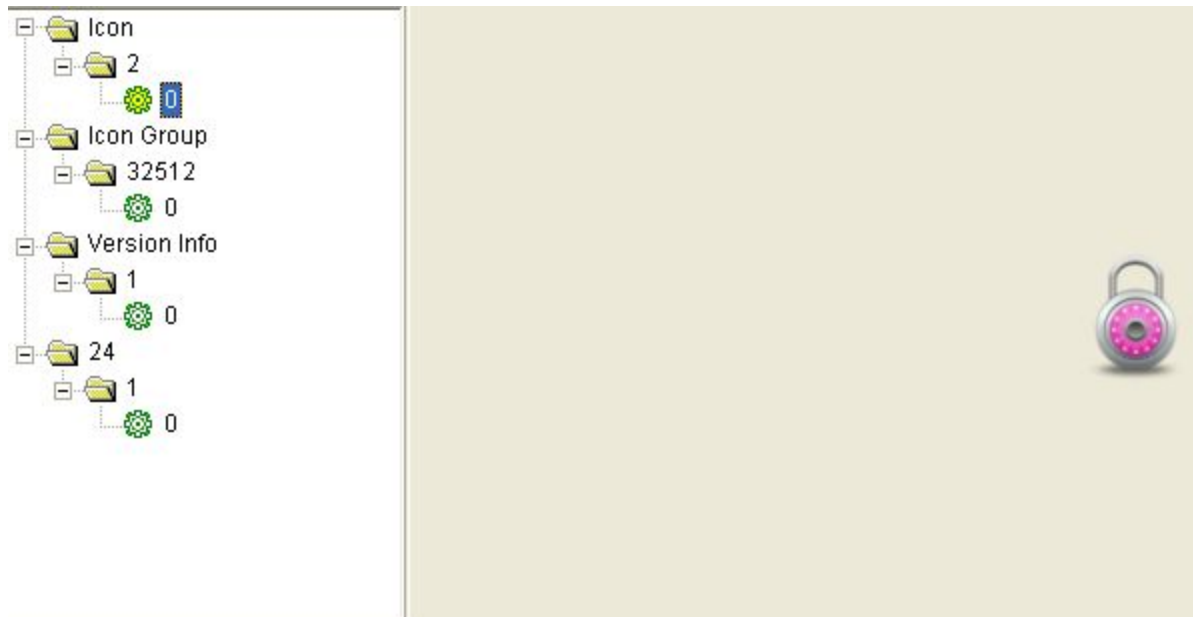


Fig.4 Lock icon resource

MD5	8675FFB697AD944748E0E24AC1A962CE
SHA1	713C2291C8D8D9BE0B7748714130C39268895E6B
Imphash	F34D5F2D4577ED6D9CEEC516C1F5A744
CPU	32-bit
Size (bytes)	439808
File description	n/a
File version	n/a
File date	18:04:2017 - 23:34:26
type	Executable
subsystem	GUI
signature	Microsoft Visual C# / Basic .NET

Fig.5 General Information

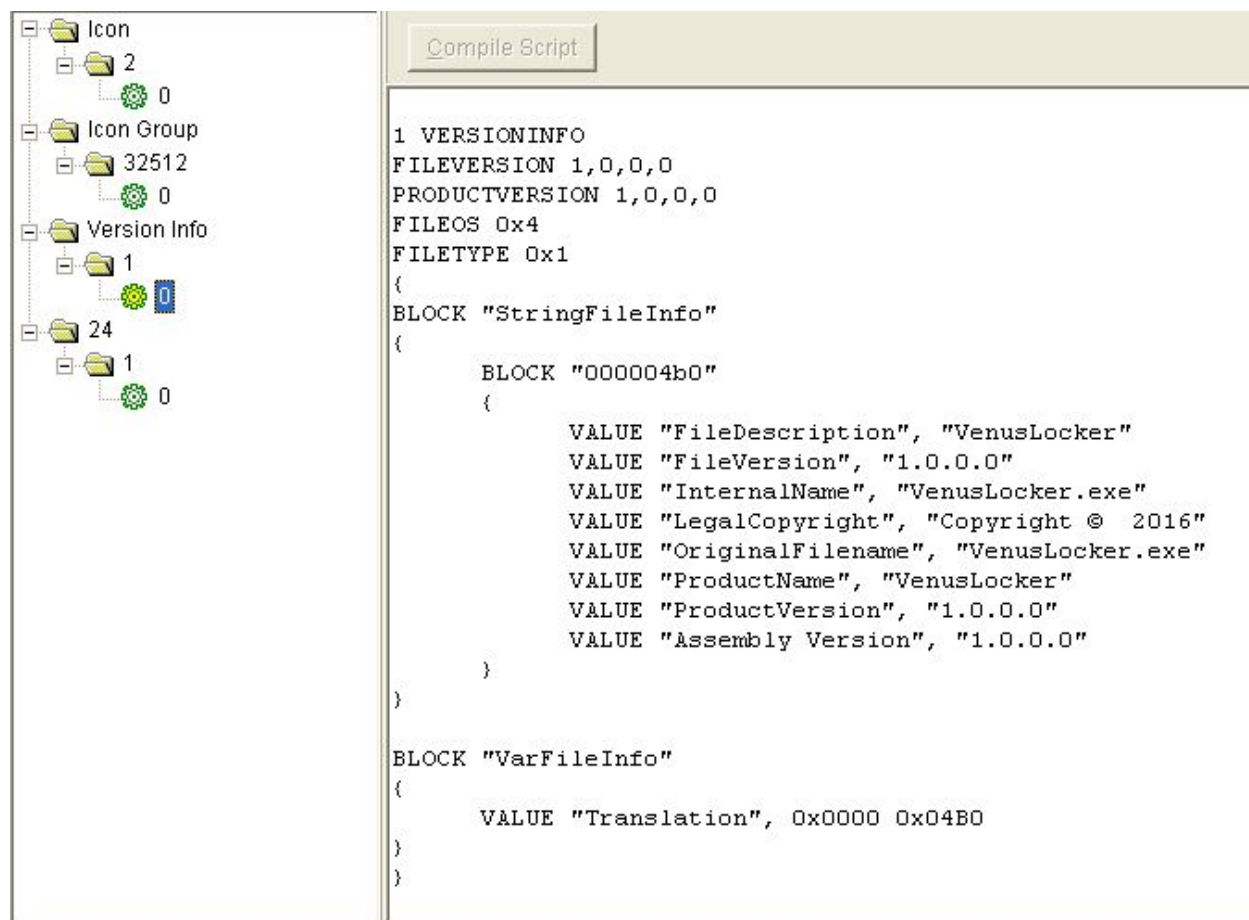


Fig.6 Venus Locker Resource

Property	Value	Value	Value
Name	.text	.rsrc	.reloc
Virtual Size (bytes)	0x000654E4 (414948)	0x00005A80 (23168)	0x0000000C (12)
Virtual Address	0x00002000	0x00068000	0x0006E000
Raw Size (bytes)	0x00065600 (415232)	0x00005C00 (23552)	0x00000200 (512)
Raw Address	0x00000200	0x00065800	0x0006B400
PointerToRelocations	0x00000000	0x00000000	0x00000000
PointerToLinenumbers	0x00000000	0x00000000	0x00000000
NumberOfRelocations	0x00000000	0x00000000	0x00000000
NumberOfLinenumbers	0x00000000	0x00000000	0x00000000
Entry Point	x	-	-
MD5	16AA64375D6731FC9E08...	7F0B337EFF297CD01419...	C0C38DE7859E0878C642...
Cave size (bytes)	0x0000011C (284)	0x00000180 (384)	0x000001F4 (500)
Obfuscated	-	-	-
Blacklisted	-	-	-
Read	x	x	x
Write	-	-	-
Execute	x	-	-
Shared	-	-	-

Fig. 7 Sections

pFile	Raw Data												Value				
00000200	C0	74	06	00	00	00	00	00	48	00	00	00	02	00	05	00	.t.....H.....
00000210	E0	DA	05	00	78	98	00	00	01	00	00	00	22	00	00	06	....x....."
00000220	50	81	00	00	8E	59	05	00	00	00	00	00	00	00	00	00	P....Y.....
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000250	13	30	05	00	5D	1A	00	00	01	00	00	11	02	72	01	00	.0...]. ....r...
00000260	00	70	28	12	00	00	0A	72	15	00	00	70	28	13	00	00	.p(....r...p(....
00000270	0A	7D	10	00	00	04	02	72	41	00	00	70	7D	12	00	00	.}.....rA..p}....
00000280	04	02	1F	2F	8D	2D	00	00	01	0A	06	16	72	43	00	00	.../.-.....rC...
00000290	70	A2	06	17	72	5F	00	00	70	A2	06	18	72	87	00	00	p...r...p...r...
000002A0	70	A2	06	19	72	97	00	00	70	A2	06	1A	72	A9	00	00	p...r...p...r...
000002B0	70	A2	06	1B	72	BB	00	00	70	A2	06	1C	72	D3	00	00	p...r...p...r...
000002C0	70	A2	06	1D	72	DF	00	00	70	A2	06	1E	72	D3	00	00	p...r...p...r...
000002D0	70	A2	06	1F	09	72	E9	00	00	70	A2	06	1F	0A	72	F1	p...r...p...r...
000002E0	00	00	70	A2	06	1F	0B	72	F9	00	00	70	A2	06	1F	0C	..p...r...p....
000002F0	72	07	01	00	70	A2	06	1F	0D	72	13	01	00	70	A2	06	r...p...r...p...
00000300	1F	0E	72	37	01	00	70	A2	06	1F	0F	72	53	01	00	70	...r7..p...rS...p
00000310	A2	06	1F	10	72	7F	01	00	70	A2	06	1F	11	72	B1	01	....r0..p...r...
00000320	00	70	A2	06	1F	12	72	D1	01	00	70	A2	06	1F	13	72	.p...r...p...r...
00000330	F3	01	00	70	A2	06	1F	14	72	0E	02	00	70	A2	06	1F	...n...r...n...

Fig.8 .text section

00065800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	04	00	.....
00065810	03	00	00	00	30	00	00	80	0E	00	00	00	48	00	00	80	....0.....H...
00065820	10	00	00	00	60	00	00	80	18	00	00	00	78	00	00	80	....`.....x....
00065830	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	.....
00065840	02	00	00	00	90	00	00	80	00	00	00	00	00	00	00	00	.....
00065850	00	00	00	00	00	00	01	00	00	7F	00	00	A8	00	00	80	.....0.....
00065860	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	.....
00065870	01	00	00	00	C0	00	00	80	00	00	00	00	00	00	00	00	.....
00065880	00	00	00	00	00	00	01	00	01	00	00	00	D8	00	00	80	.....
00065890	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	.....
000658A0	00	00	00	00	F0	00	00	00	00	00	00	00	00	00	00	00	.....
000658B0	00	00	00	00	00	00	01	00	00	00	00	00	00	01	00	00	.....
000658C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	.....
000658D0	00	00	00	00	10	01	00	00	00	00	00	00	00	00	00	00	.....
000658E0	00	00	00	00	00	00	01	00	00	00	00	00	20	01	00	00	.....
000658F0	F0	83	06	00	88	54	00	00	00	00	00	00	00	00	00	00	....T.....
00065900	78	D8	06	00	14	00	00	00	00	00	00	00	00	00	00	00	x.....
00065910	30	81	06	00	C0	02	00	00	00	00	00	00	00	00	00	00	0... ..
00065920	90	D8	06	00	EA	01	00	00	00	00	00	00	00	00	00	00	.....
00065930	C0	02	34	00	00	00	56	00	53	00	5F	00	56	00	45	00	..4...V.S...V.E.
00065940	52	00	53	00	49	00	4F	00	4E	00	5F	00	49	00	4E	00	R.S.I.O.N...I.N.

Fig.9 .rsrc section



0006B400	00 70 06 00 0C 00 00 00	E0 34 00 00 00 00 00 00	. p . . . . . 4 . . . . .
0006B410	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B420	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B430	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B440	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B450	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B460	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B470	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B480	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B490	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B4F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B500	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B510	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .
0006B520	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	. . . . .

Fig.10 .reloc section

The count (215) of blacklisted strings reached the maximum (30) threshold	1
The time stamp (Year:2016)of the File Header reached the maximum (Year:2015) threshold	1
The time stamp (Year:2016) of the Debug block reached the maximum (Year:2015) threshold	1
The file references a URL (11.0.0.0)	1
The file references a URL (https://158.255.5.153/create.php)	1
The file references a URL (http://ip-api.com/csv?fields=country)	1
The file references a URL (https://158.255.5.153/keysave.php)	1
The file references a URL (http://i.imgur.com/Jk67Lr5.jpg)	1
The file references a URL (https://158.255.5.153/)	1
The file opts for Address Space Layout Randomization (ASLR) as mitigation technique	2
The file checksum (0x00000000) is invalid	2
The manifest identity name (MyApplication.app) is different than the file name (d31afd6d582a666e...	2
The original filename (VenusLocker.exe) is different than the file name (d31afd6d582a666e121a1e1...	2
The debug file name (venuslocker.pdb) is different than the file name (d31afd6d582a666e121a1e1...	2
The file is not signed with a Digital Certificate	2

Fig.11 PEstudio Indicators

Library (1)	Blacklisted (0)	Type	Symbols (1)	Description
mscorlib.dll	-	Implicit	1	Microsoft .NET Runtime Execution Engine

Fig.12 Libraries

Symbol (1)	Blacklisted (0)	Ordinal (0)	Anti-Debug (0)	Library (1)
_CorExeMain	-	-	-	mscorlib.dll

Fig.13 Functions

unicode	4	.text:0...	x	.bit
unicode	4	.text:0...	x	.ini
unicode	4	.text:0...	x	.php
unicode	5	.text:0...	x	.html
unicode	4	.text:0...	x	.css
unicode	4	.text:0...	x	.cpp
unicode	4	.text:0...	x	.log
unicode	5	.text:0...	x	.java
unicode	4	.text:0...	x	.doc
unicode	4	.text:0...	x	.dot
unicode	5	.text:0...	x	.docx
unicode	5	.text:0...	x	.docm
unicode	5	.text:0...	x	.dotm
unicode	4	.text:0...	x	.rtf
unicode	4	.text:0...	x	.wpd
unicode	4	.text:0...	x	.wps
unicode	4	.text:0...	x	.msg
unicode	4	.text:0...	x	.xls
unicode	4	.text:0...	x	.xlt
unicode	5	.text:0...	x	.xlsx
unicode	5	.text:0...	x	.xlsm
unicode	4	.text:0...	x	.xla
unicode	4	.text:0...	x	.xll
unicode	4	.text:0...	x	.xlw
unicode	4	.text:0...	x	.ppt
unicode	4	.text:0...	x	.pot
unicode	4	.text:0...	x	.pps
unicode	5	.text:0...	x	.pptx
unicode	5	.text:0...	x	.pptm
unicode	5	.text:0...	x	.ppsx
unicode	5	.text:0...	x	.ppsm
unicode	6	.text:0...	x	.class
unicode	4	.text:0...	x	.jar
unicode	4	.text:0...	x	.csv
unicode	4	.text:0...	x	.xml
unicode	4	.text:0...	x	.dwg
unicode	4	.text:0...	x	.asp
unicode	4	.text:0...	x	.asf
unicode	4	.text:0...	x	.pdf
unicode	4	.text:0...	x	.mp3

Fig.14.1 File extension set 1

unicode	4	.text:0...	x	.jpg
unicode	5	.text:0...	x	.jpeg
unicode	4	.text:0...	x	.rar
unicode	4	.text:0...	x	.zip
unicode	4	.text:0...	x	.psd
unicode	4	.text:0...	x	.tif
unicode	4	.text:0...	x	.wma
unicode	4	.text:0...	x	.gif
unicode	4	.text:0...	x	.bmp
unicode	4	.text:0...	x	.eps
unicode	4	.text:0...	x	.png
unicode	4	.text:0...	x	.tar
unicode	4	.text:0...	x	.cdr
unicode	4	.text:0...	x	.wmv
unicode	4	.text:0...	x	.avi
unicode	4	.text:0...	x	.mp4
unicode	4	.text:0...	x	.pdd
unicode	6	.text:0...	x	.acddb
unicode	4	.text:0...	x	.raw
unicode	4	.text:0...	x	.bik
unicode	4	.text:0...	x	.flv
unicode	4	.text:0...	x	.swf
unicode	4	.text:0...	x	.dng
unicode	4	.text:0...	x	.mag
unicode	4	.text:0...	x	.msp
unicode	4	.text:0...	x	.odc
unicode	4	.text:0...	x	.mlx
unicode	5	.text:0...	x	.mbox
unicode	4	.text:0...	x	.odm
unicode	4	.text:0...	x	.oft
unicode	4	.text:0...	x	.wbk
unicode	4	.text:0...	x	.wsh
unicode	4	.text:0...	x	.arc
unicode	4	.text:0...	x	.arj
unicode	4	.text:0...	x	.pak
unicode	4	.text:0...	x	.sfx
unicode	5	.text:0...	x	.zipx
unicode	5	.text:0...	x	.indd
unicode	4	.text:0...	x	.cer
unicode	4	.text:0...	x	.crt

Fig.14.2 File extension set 1

unicode	4	.text:0...	x	.htm
unicode	4	.text:0...	x	.url
unicode	4	.text:0...	x	.big
unicode	4	.text:0...	x	.lwd
unicode	4	.text:0...	x	.lxl
unicode	4	.text:0...	x	.map
unicode	4	.text:0...	x	.sav
unicode	4	.text:0...	x	.vtf
unicode	4	.text:0...	x	.w3x
unicode	4	.text:0...	x	.mdf
unicode	4	.text:0...	x	.nrg
unicode	4	.text:0...	x	.bkf
unicode	4	.text:0...	x	.ade
unicode	4	.text:0...	x	.dex
unicode	4	.text:0...	x	.dif
unicode	5	.text:0...	x	.itdb
unicode	4	.text:0...	x	.itl
unicode	4	.text:0...	x	.mdn
unicode	4	.text:0...	x	.odp
unicode	4	.text:0...	x	.ods
unicode	4	.text:0...	x	.qdf
unicode	4	.text:0...	x	.sdb
unicode	4	.text:0...	x	.sql
unicode	4	.text:0...	x	.xlc
unicode	4	.text:0...	x	.cap
unicode	4	.text:0...	x	.dsp
unicode	4	.text:0...	x	.jav
unicode	5	.text:0...	x	.rsrc
unicode	4	.text:0...	x	.xlv
unicode	4	.text:0...	x	.cfg
unicode	4	.text:0...	x	.bak
unicode	4	.text:0...	x	.odt
unicode	4	.text:0...	x	.pst
unicode	4	.text:0...	x	.mpg
unicode	5	.text:0...	x	.mpeg
unicode	4	.text:0...	x	.odb
unicode	4	.text:0...	x	.xlk
unicode	4	.text:0...	x	.mdb
unicode	4	.text:0...	x	.dxg
unicode	4	.text:0...	x	.wb2

Fig.15.1 File Extension set 2

unicode	4	.text:0...	x	.dbf
unicode	4	.text:0...	x	.3fr
unicode	4	.text:0...	x	.arw
unicode	4	.text:0...	x	.srf
unicode	4	.text:0...	x	.sr2
unicode	4	.text:0...	x	.bay
unicode	4	.text:0...	x	.crw
unicode	4	.text:0...	x	.cr2
unicode	4	.text:0...	x	.dcr
unicode	4	.text:0...	x	.kdc
unicode	4	.text:0...	x	.erf
unicode	4	.text:0...	x	.mef
unicode	4	.text:0...	x	.nrw
unicode	4	.text:0...	x	.orf
unicode	4	.text:0...	x	.raf
unicode	4	.text:0...	x	.rwl
unicode	4	.text:0...	x	.rw2
unicode	4	.text:0...	x	.r3d
unicode	4	.text:0...	x	.ptx
unicode	4	.text:0...	x	.pef
unicode	4	.text:0...	x	.srw
unicode	4	.text:0...	x	.x3f
unicode	4	.text:0...	x	.der
unicode	4	.text:0...	x	.pem
unicode	4	.text:0...	x	.pfx
unicode	4	.text:0...	x	.p12
unicode	4	.text:0...	x	.p7b
unicode	4	.text:0...	x	.p7c
unicode	5	.text:0...	x	.jiff
unicode	4	.text:0...	x	.pdb
unicode	4	.text:0...	x	.dat
unicode	5	.text:0...	x	.idml
unicode	4	.text:0...	x	.svg

Fig.15.2 File Extension set 2



ascii	6	?:0x017E	x	`.rsrc
ascii	17	.text:0...	x	Adobe ImageReadyq
ascii	4	.text:0...	x	1Z.H
ascii	4	.text:0...	x	IO.H
ascii	15	.text:0...	x	VenusLocker.exe
ascii	7	.text:0...	x	Program
ascii	8	.text:0...	x	Settings
ascii	6	.text:0...	x	System
ascii	6	.text:0...	x	Source
ascii	5	.text:0...	x	Email
ascii	20	.text:0...	x	SystemParametersInfo
ascii	28	.text:0...	x	System.Security.Cryptography
ascii	7	.text:0...	x	Default
ascii	6	.text:0...	x	sender
ascii	30	.text:0...	x	System.Runtime.InteropServices
ascii	17	.text:0...	x	System.Reflection
ascii	31	.text:0...	x	System.Runtime.CompilerServices
ascii	10	.text:0...	x	user32.dll
ascii	10	.text:0...	x	System.Net
ascii	15	.text:0...	x	get_MachineName
ascii	8	.text:0...	x	Encoding
ascii	11	.text:0...	x	ComputeHash
ascii	6	.text:0...	x	SHA256
ascii	14	.text:0...	x	RuntimeHelpers
ascii	12	.text:0...	x	MemoryStream
ascii	10	.text:0...	x	CipherMode
ascii	11	.text:0...	x	PaddingMode
ascii	12	.text:0...	x	DownloadFile
ascii	7	.text:0...	x	Process
ascii	5	.text:0...	x	Start
ascii	8	.text:0...	x	11.0.0.0
ascii	107	.text:0...	x	c:\Users\Hacker\Documents\Visual Studio 2012\Projects\VenusLockerV2\VenusLocker\obj\Release\...
ascii	11	.text:0...	x	mscorlib.dll

Fig.16.1 Strings

unicode	5	.text:0...	x	Avira
unicode	17	.text:0...	x	Internet Explorer
unicode	13	.text:0...	x	Microsoft.NET
unicode	10	.text:0...	x	Windows NT
unicode	5	.text:0...	x	Adobe
unicode	14	.text:0...	x	AVAST Software
unicode	8	.text:0...	x	CCleaner

Fig.16.2 Strings

unicode	8	.text:0...	x	username
unicode	5	.text:0...	x	Vista
unicode	4	.text:0...	x	2003
unicode	4	.text:0...	x	2000
unicode	32	.text:0...	x	https://158.255.5.153/create.php
unicode	4	.text:0...	x	POST
unicode	36	.text:0...	x	http://ip-api.com/csv?fields=country
unicode	33	.text:0...	x	https://158.255.5.153/keysave.php
unicode	24	.text:0...	x	VenusLocker@mail2tor.com
unicode	6	.text:0...	x	bq.jpg
unicode	30	.text:0...	x	http://i.imgur.com/3k67Lr5.jpg
unicode	19	.text:0...	x	\\Desktop\ReadMe.txt
unicode	12	.text:0...	x	CoinCafe.com
unicode	21	.text:0...	x	HowToBuy Bitcoins.info
unicode	22	.text:0...	x	https://158.255.5.153/
unicode	11	.text:0...	x	keysave.php
unicode	36	.text:0...	x	http://ip-api.com/csv?fields=country
unicode	24	.text:0...	x	VenusLocker@mail2tor.com
unicode	15	.text:0...	x	VenusLocker.exe
unicode	15	.text:0...	x	VenusLocker.exe

Fig.16.3 Strings

ascii	11	.text:0...	-	VenusLocker
ascii	4	.text:0...	-	Mode
ascii	9	.text:0...	-	Resources
ascii	22	.text:0...	-	VenusLocker.Properties
ascii	20	.text:0...	-	System.Windows.Forms
ascii	4	.text:0...	-	Form
ascii	8	.text:0...	-	mscorlib
ascii	4	.text:0...	-	Enum
ascii	6	.text:0...	-	Object
ascii	20	.text:0...	-	System.Configuration
ascii	23	.text:0...	-	ApplicationSettingsBase
ascii	7	.text:0...	-	Expired
ascii	9	.text:0...	-	ServerUrl
ascii	16	.text:0...	-	ServerInfoSubmit
ascii	13	.text:0...	-	ServerKeySave
ascii	13	.text:0...	-	BackgroundUrl
ascii	14	.text:0...	-	IPAPIServerUrl
ascii	19	.text:0...	-	BTCReceivingAddress
ascii	13	.text:0...	-	OfflineAESKey
ascii	14	.text:0...	-	EncryptedBytes
ascii	17	.text:0...	-	AESPasswordLength
ascii	10	.text:0...	-	RSAPublicKeySize
ascii	6	.text:0...	-	isOAEP
ascii	15	.text:0...	-	RSAPublicKeyXML
ascii	13	.text:0...	-	SingletonPath
ascii	8	.text:0...	-	FirstRun
ascii	10	.text:0...	-	PersonalID
ascii	26	.text:0...	-	System.Collections.Generic
ascii	13	.text:0...	-	ICollection`1
ascii	13	.text:0...	-	ExcludeFolder
ascii	18	.text:0...	-	FullCryptExtension
ascii	11	.text:0...	-	ValidExtension
ascii	5	.text:0...	-	.ctor
ascii	9	.text:0...	-	EventArgs
ascii	13	.text:0...	-	MainForm_Load
ascii	14	.text:0...	-	VenusLockerRun
ascii	8	.text:0...	-	SendInfo
ascii	11	.text:0...	-	IP2Location
ascii	14	.text:0...	-	CreatePassword
ascii	24	.text:0...	-	RNGCryptoServiceProvider

Fig.16.4 Strings

ascii	6	.text:0...	-	GetInt
ascii	15	.text:0...	-	Disk_Encryption
ascii	22	.text:0...	-	CurrentPath_Encryption
ascii	9	.text:0...	-	System.IO
ascii	8	.text:0...	-	FileInfo
ascii	15	.text:0...	-	File_Encryption
ascii	11	.text:0...	-	AES_Encrypt
ascii	19	.text:0...	-	AESKeyEncryptWithRS
ascii	7	.text:0...	-	SendKey
ascii	6	.text:0...	-	ShowUI
ascii	12	.text:0...	-	SetWallPaper
ascii	14	.text:0...	-	MessageCreator
ascii	45	.text:0...	-	System.Security.Cryptography.X509Certificates
ascii	15	.text:0...	-	X509Certificate
ascii	9	.text:0...	-	X509Chain
ascii	19	.text:0...	-	System.Net.Security
ascii	15	.text:0...	-	SslPolicyErrors
ascii	25	.text:0...	-	ValidateRemoteCertificate
ascii	8	.text:0...	-	TimeSpan
ascii	10	.text:0...	-	Timer_Tick
ascii	29	.text:0...	-	LinkLabelLinkClickedEventArgs
ascii	20	.text:0...	-	HomePage_LinkClicked
ascii	29	.text:0...	-	GetStartLinkLabel_LinkClicked
ascii	31	.text:0...	-	BlockchainLinkLabel_LinkClicked
ascii	34	.text:0...	-	LocalBitcoinLinkLabel_LinkClicked
ascii	29	.text:0...	-	CoinCafeLinkLabel_LinkClicked
ascii	30	.text:0...	-	BTCDirectLinkLabel_LinkClicked
ascii	24	.text:0...	-	CExLinkLabel_LinkClicked
ascii	29	.text:0...	-	CoinMamaLinkLabel_LinkClicked
ascii	29	.text:0...	-	HowToBuyLinkLabel_LinkClicked
ascii	33	.text:0...	-	PerfectMoneyLinkLabel_LinkClicked
ascii	30	.text:0...	-	PMBitcoinLinkLabel_LinkClicked

Fig.16.5 Strings

ascii	15	.text:0...	-	WhatHappenLabel
ascii	17	.text:0...	-	HowToDecryptLabel
ascii	13	.text:0...	-	HowToPayLabel

Fig.16.6 Strings

unicode	21	.text:0...	-	\U2FsdGVkX1DKeR.vluni
---------	----	------------	---	-----------------------

Fig.16.7 Strings

unicode	6	.text:0...	-	Google
unicode	5	.text:0...	-	Intel
unicode	13	.text:0...	-	Kaspersky Lab
unicode	21	.text:0...	-	Microsoft Bing Pinyin
unicode	24	.text:0...	-	Microsoft Chart Controls
unicode	15	.text:0...	-	Microsoft Games
unicode	16	.text:0...	-	Microsoft Office
unicode	12	.text:0...	-	MicrosoftBAF
unicode	7	.text:0...	-	MSBuild
unicode	12	.text:0...	-	QQMailPlugin
unicode	7	.text:0...	-	Realtek
unicode	5	.text:0...	-	Skype
unicode	20	.text:0...	-	Reference Assemblies
unicode	7	.text:0...	-	Tencent
unicode	11	.text:0...	-	USB Camera2
unicode	6	.text:0...	-	WinRAR
unicode	15	.text:0...	-	Windows Sidebar
unicode	24	.text:0...	-	Windows Portable Devices
unicode	20	.text:0...	-	Windows Photo Viewer
unicode	20	.text:0...	-	Windows Media Player
unicode	12	.text:0...	-	Windows Mail
unicode	18	.text:0...	-	NVIDIA Corporation
unicode	5	.text:0...	-	IObit
unicode	9	.text:0...	-	VirtualDJ
unicode	10	.text:0...	-	TeamViewer
unicode	1	.text:0...	-	java
unicode	6	.text:0...	-	Yahoo!

Fig.16.8 Strings

unicode	32	.text:0...	-	BGORMkj&v=u1X002hOybNdRvzb9SGGnm
unicode	1	.text:0...	-	NULL
unicode	6	.text:0...	-	pname
unicode	7	.text:0...	-	unknown
unicode	1	.text:0...	-	lang
unicode	1	.text:0...	-	time
unicode	5	.text:0...	-	loads
unicode	6	.text:0...	-	userid
unicode	524	.text:0...	-	<RSAKeyValue><Modulus>laQ/NdkbwsWz2zVMG4MaRaL7/t1krRdDHURawFCEUlgMbkWY9MK<mq1TFC6dpLNk2cj6sezkg9c38YaBRg33BF5PaHtZW4Og+JP9W...
unicode	524	.text:0...	-	YrCT1S3+wwlRSfajp1FNe1CNW78BtGxKqGgz/xCkuk3QFGCufw1fMyQj/dUJ22dR0hNKfpRCI9v2yN2XqdVjXapWnpDVGaIP8zTeQ==</Modulus><Exponent>...
unicode	34	.text:0...	-	1Dj9YnMicNgakuyzkynngu7n821tvW6QD

Fig.16.9 Strings

## Basic Dynamic Analysis

Upon executing Venus Locker, It creates a file U2FsdGVKX1DKeR.vluni at C:\Users\current user\. The actual contents of this file is unknown and encrypted however we assume that this file is used as a way of ensuring persistence and notifying multiple instances of the malware that the system is already infected. This assumption is made as the malware does not execute if it is already running on the system.

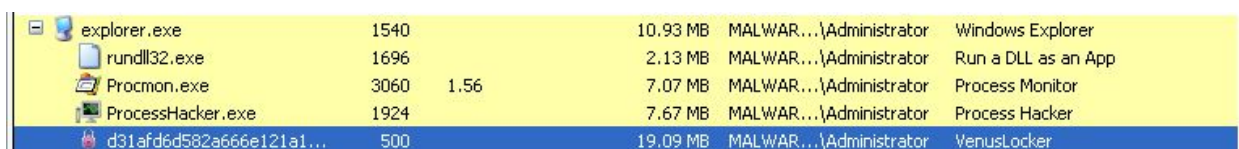
During its execution, Venus Locker slowly starts encrypting files as can be seen below. It creates 2 different encrypted files - .Venusf files or .Venusp files. As previously mentioned, we saw that the malware has 2 sets of file extensions that are to be encrypted if found. We can correlate these 2 findings and establish that Venus Locker encrypts one set of file extensions into .Venusf files and the other set of file extensions into .Venusp files. There do not seem to be any significant structural differences between both files. However, it is interesting to note that Venus Locker does not prevent using any of the applications that have been encrypted and we can still make use of their functionality. Another subject of note is that Venus Locker does not encrypt some files. We assume this corresponds to those applications that we previously saw in the strings section. Once the program has completed its encryption process, It launches a GUI explaining to the user that his files have been encrypted. It gives him a deadline of 72 hours after which the private key needed to decrypt his files will be deleted. It also provides a number of ways to purchase bitcoins and prompts the user to pay the ransom.

Venus Locker also seems to execute a method to change the user's wallpaper as shown. While during analysis, the default Windows XP wallpaper was only removed, we believe that the malware attempts to download an image from the url <http://i.imgur.com/JK67LrS.jpg> mentioned earlier and set this image as the wallpaper, which in this case it failed to do so due to lack of connectivity.

Venus Locker does communicate with a command and control server located at <https://158.255.5.153>. The other url that the malware contacts is <http://ip-api.com/csv?fields=country> which is a service used to collect intelligence about the victim's machine like external ip address etc. We can correlate the two and presume that the malware reports infected victim data to the CnC server.

The malware as previously mentioned uses the AES encryption scheme along with an RSA scheme to encrypt the AES key. It dynamically loads a lot of dlls as can be seen using procmon of which one in particular is the rsaenh.dll encryption library. While it does not set an autorun registry value, it adds a prefetch file to the registry as shown below.

Finally, the malware has some date checking mechanism wherein it only executes its functionality thread if the date is not beyond the 30th of August 2016. If the system date has exceeded this point, the process is instantly terminated while if it is before, the malware proceeds along its main thread.



explorer.exe	1540		10.93 MB	MALWAR...\Administrator	Windows Explorer
rundll32.exe	1696		2.13 MB	MALWAR...\Administrator	Run a DLL as an App
Procmon.exe	3060	1.56	7.07 MB	MALWAR...\Administrator	Process Monitor
ProcessHacker.exe	1924		7.67 MB	MALWAR...\Administrator	Process Hacker
d31afd6d582a666e121a1...	500		19.09 MB	MALWAR...\Administrator	VenusLocker

Fig.17 Process running







-----  
Files [attributes?] modified:11  
-----

C:\Documents and Settings\Administrator\ntuser.dat.LOG  
C:\WINDOWS\Prefetch\APATEDNS.EXE-3AE1E42D.pf  
C:\WINDOWS\Prefetch\D31AFD6D582A666E121A1E1DF8BC1-097C0992.pf  
C:\WINDOWS\Prefetch\LOGON.SCR-151EFAEA.pf  
C:\WINDOWS\Prefetch\PROCEXP.EXE-37D9F3A4.pf  
C:\WINDOWS\Prefetch\PROCMON.EXE-374C12E7.pf  
C:\WINDOWS\Prefetch\WMIPRVSE.EXE-28F301A9.pf  
C:\WINDOWS\system32\config\software.LOG  
C:\WINDOWS\system32\config\system.LOG  
C:\WINDOWS\system32\wbem\Logs\wbemcore.log  
C:\WINDOWS\system32\wbem\Logs\wmiprov.log

Fig.20 Prefetch file added

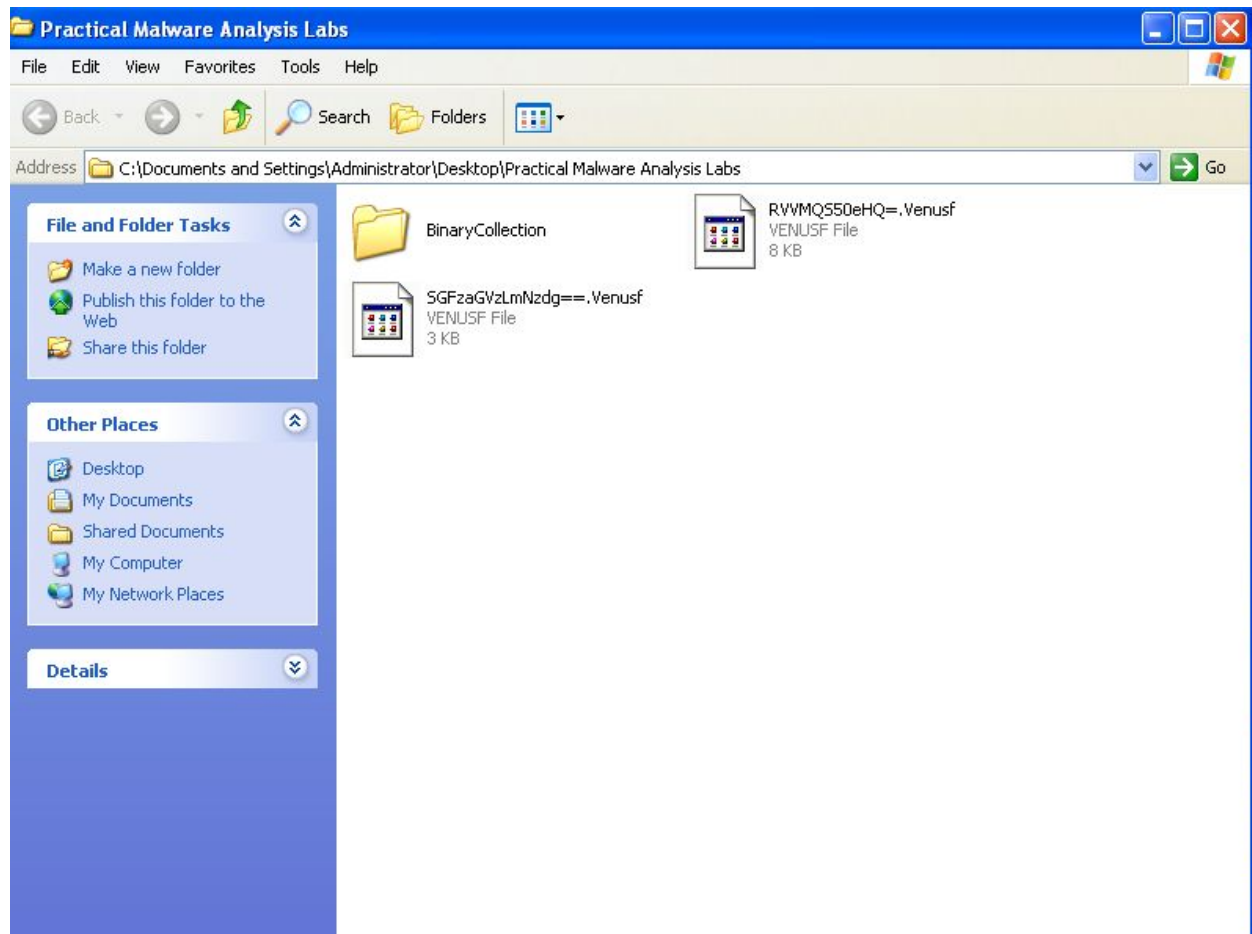


Fig.21 Encrypted files



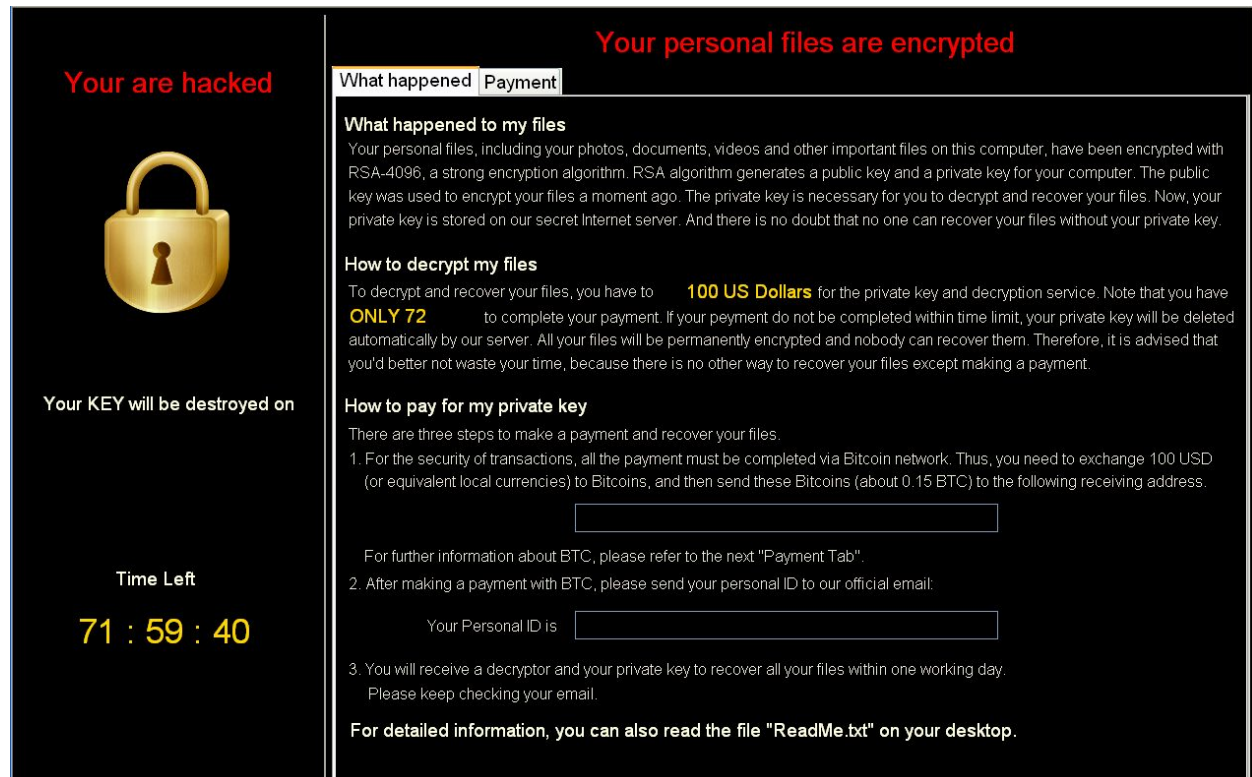


Fig.24.1 GUI

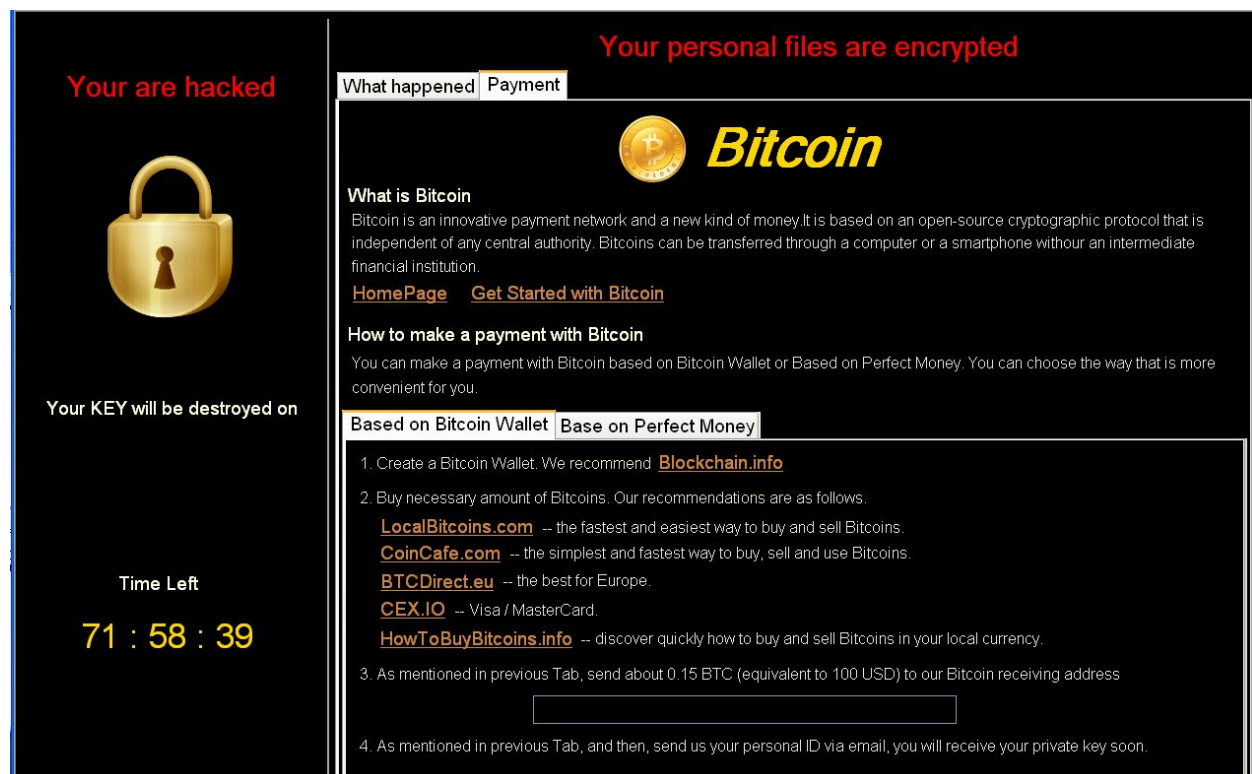


Fig.24.2 GUI

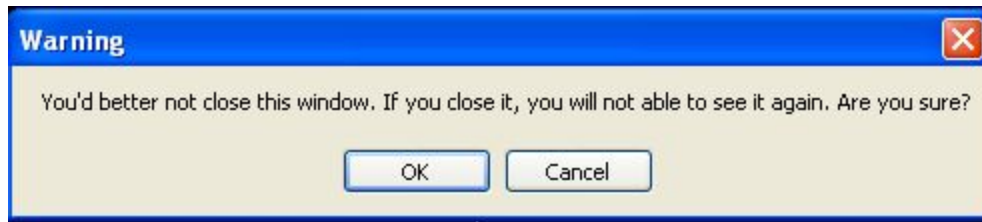


Fig.24.3 GUI



Fig.25 Wallpaper changed

### **Indicators of Compromise**

Venus Locker shows a large number of host and network based indicators.

The network activity can be used as an indicator. If the program attempts to contact the url <https://158.255.5.153> or <http://ip-api.com/csv?fields=country> then it can be used as a strong indicator of compromise. The wallpaper image url <http://i.imgur.com/JK67LrS.jpg> can also be used as another network based indicator.

The malware initially creates a file U2FsdGVKX1DKeR.vluni at C:\Users\current user\. This can be used as a strong host based indicator of compromise. The prefetch registry file can also be used as another indicator of compromise.

### **Conclusion**

Venus Locker is a dangerous albeit basic ransomware that is hard to mitigate once activated, hence prevention is definitely a critical priority. Periodic backup of system files can help by facilitating system formats followed by system restores.