

# Malware Analysis

## Executive Summary

The malware sample.exe is a ransomware called cryptolocker. It functions by encrypting all the files present in the system drives and prompts the user to provide monetary compensation if he requires decryption. The malware attempts to contact a large number of command and control servers using a ‘Domain Generation Algorithm’ in the hopes of reaching out to an active server. Once this connection is established, the server generates a public-private key pair which the malware then uses to encrypt the user’s files. While the malware is primarily distributed via the Gameover Zeus botnet, it is also found in spam emails as attachments. 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. The Malware was compiled on the 26th of November 2013 at 7:11 PM as observed from PEStudio and it is a windows GUI application. This particular sample has an MD5 hash of 8466505F0F110825420BEAC9CE551A29.

The program’s resources (provided below) allow us to identify it’s working in closer detail. A few window icons and images are found which establish the malware as a GUI program.

Furthermore, on analysing the text resources, the program informs the user that his files are encrypted and that he must pay a particular amount to a certain mentioned virtual address in order to get them decrypted. This further confirms our previous statement that the malware is a ransomware called Cryptolocker. A few images can be found pertaining to payment options that the user can use to make the payment like Ukash, bitcoin etc. The program sections and contents are provided below.

On analysing the imports, the program appears to import a large number of http modules implying that the malware attempts to make http connections to a certain server to send or receive data. Another set of libraries imported are crypto libraries used in the encryption and decryption processes. We also observe that there are a few functions used to create, modify and delete registry keys which can potentially be harmful. A few suspicious imports are provided below.

There are also a large number of strings that are of concern. We provide a few important ones. “Microsoft enhanced RSA and AES cryptographic provider”, “Microsoft enhanced cryptographic provider v1.0”, “CryptStringtoBinary”, “CryptDecodeObjectEx” and “CryptImportPublicKeyInfo” are all related to cryptographic schemes used by the Malware. We also see a number of file format strings like “\*.p7c”, “\*.orf” and “\*.pef”. The malware encrypts all files with these formats on the user’s drives. There are around 50 such file formats. A large number of HTTP related strings can also be seen like “WinHttpReceiveResponse”, “WinHttpSendRequest”, “WinHttpWriteData” and “WinHttpReadData”. An IP address is also seen, “184.164.136.134” which is assumed to be the initial Command and Control Server that the malware tries to contact before running its DGA. A few other strings of importance are “Software\Microsoft\Windows\CurrentVersion\Run” and “Software\Cryptolocker”. The former is a registry key that is updated to add the malware to a list of autorun programs to run on each startup while the latter is the name of the malware itself. We delve deeper into these findings in

the upcoming sections.

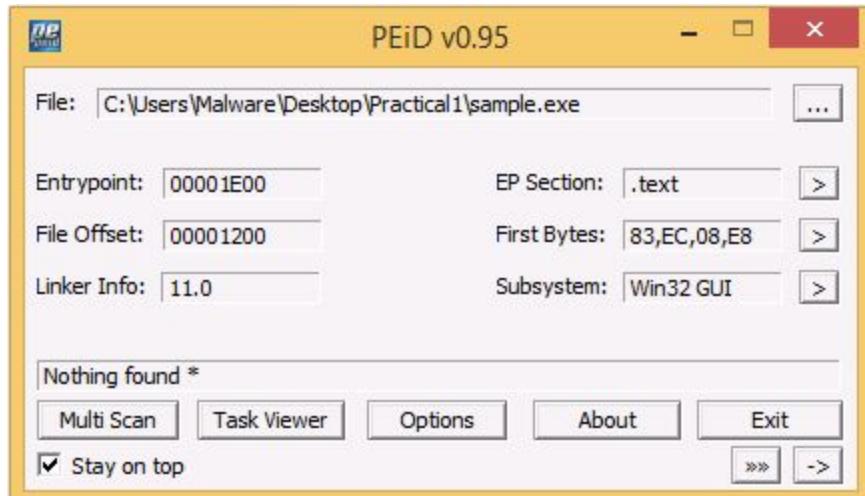


Fig.1 Unpacked program

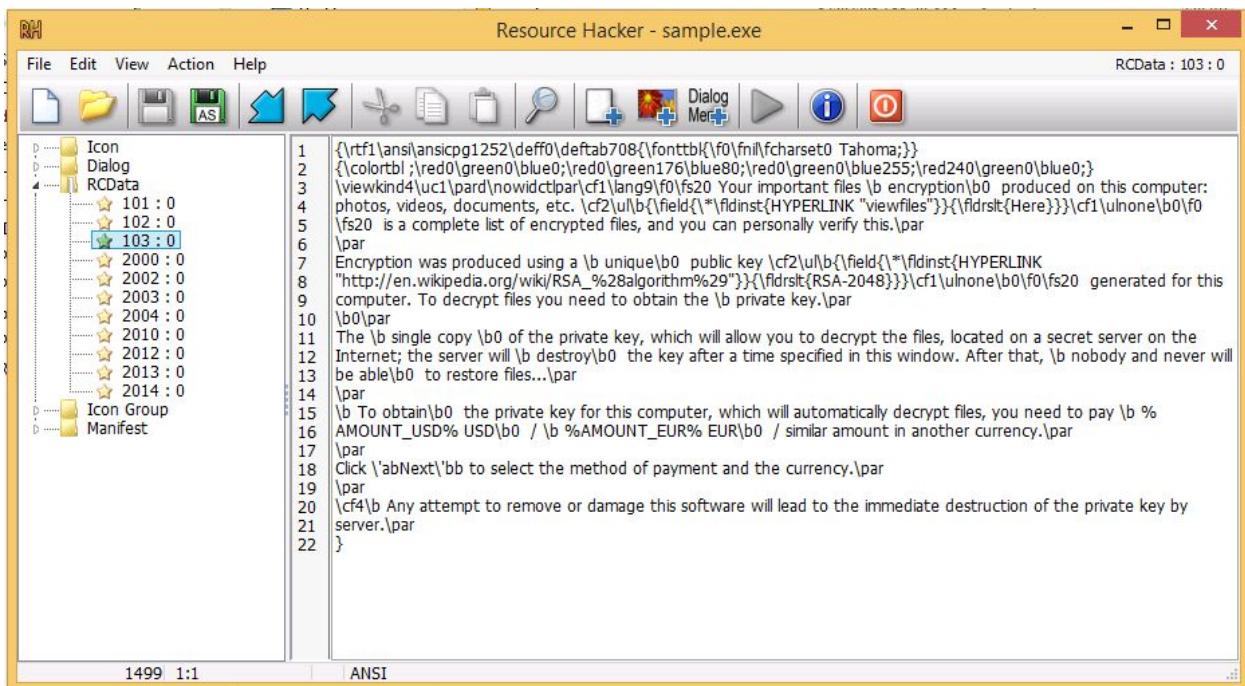


Fig.2 Text Resources

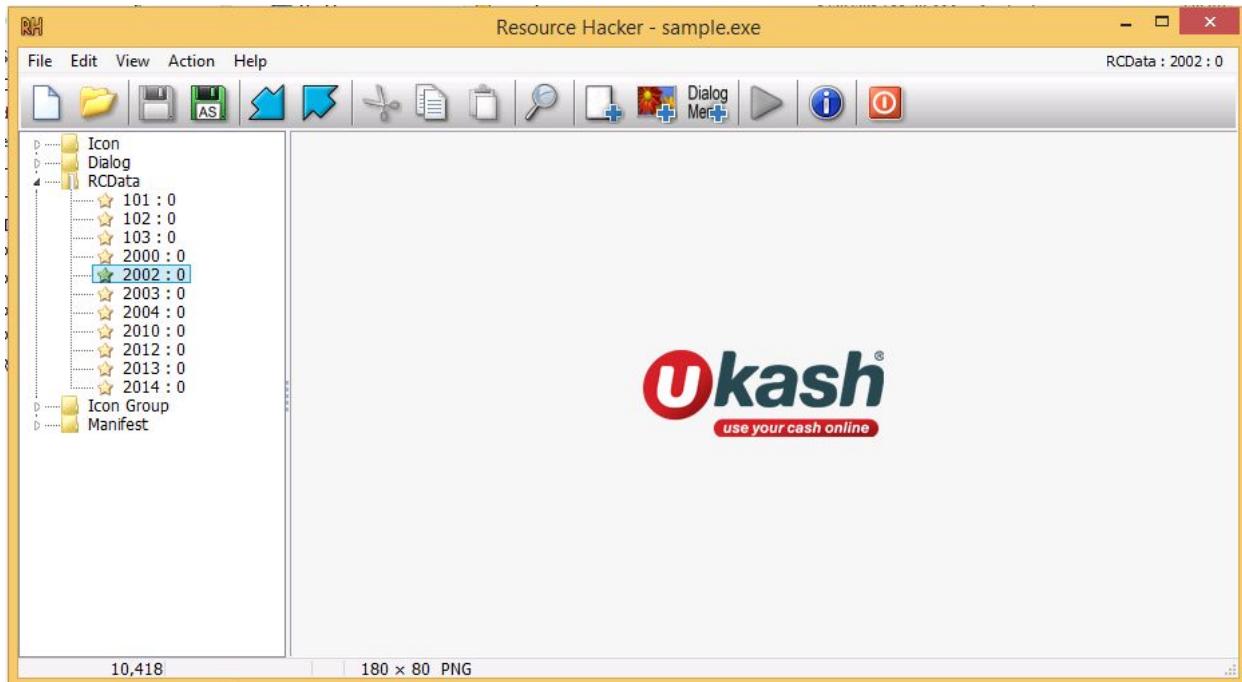


Fig.3 Payment option

pestudio 8.55 - Malware Initial Assessment - www.winitor.com	
File	Help
c:\users\malware\Desktop\pr	property value
indicators (wait..)	md5 8466505F0F110825420BEAC9CE551A29
virustotal (offline)	sha1 D369DAE745A501B866888494A8BF15A32AB5570B
dos-stub (176 bytes)	imphash n/a
file-header (20 bytes)	cpu 32-bit
optional-header (224 bytes)	size 346112
directories (4/15)	entropy 7.718
sections (5)	description n/a
libraries (3/14)	version n/a
imports (106/259)	date 26:11:2013 - 19:11:00
exports (n/a)	type executable
exceptions (n/a)	subsystem GUI
tls-callbacks (n/a)	signature n/a
resources (Rich Text)	
abc strings (217/4171)	
debug (n/a)	
manifest (invoker)	
1.0 version (n/a)	
certificate (n/a)	
overlay (n/a)	

Fig.4 Malware information

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

File	Help				
c:\users\malware\Desktop\prj <span style="color: #0070C0;">[+]</span> indicators (9/16) <span style="color: #0070C0;">[+]</span> virustotal (offline) <span style="color: #0070C0;">[-]</span> dos-stub (176 bytes) <span style="color: #0070C0;">[-]</span> file-header (20 bytes) <span style="color: #0070C0;">[-]</span> optional-header (224 bytes) <span style="color: #0070C0;">[-]</span> directories (4/15) <span style="color: #0070C0;">[+]</span> sections (5) <span style="color: #0070C0;">[-]</span> libraries (3/14) <span style="color: #0070C0;">[-]</span> imports (106/259) <span style="color: #0070C0;">[-]</span> exports (n/a) <span style="color: #0070C0;">[-]</span> exceptions (n/a) <span style="color: #0070C0;">[-]</span> tls-callbacks (n/a) <span style="color: #0070C0;">[+]</span> resources (Rich Text) <span style="color: #0070C0;">[-]</span> strings (217/4171) <span style="color: #0070C0;">[-]</span> debug (n/a) <span style="color: #0070C0;">[+]</span> manifest (invoker) <span style="color: #0070C0;">[-]</span> version (n/a) <span style="color: #0070C0;">[-]</span> certificate (n/a) <span style="color: #0070C0;">[-]</span> overlay (n/a)					
property	value	value	value	value	value
name	.text	.rdata	.data	.rsrc	.reloc
virtual-size	0x0000FA90 (64144)	0x000045E8 (17896)	0x0000F24 (3876)	0x0003DF78 (253816)	0x00001F3C (7996)
virtual-address	0x00001000	0x00011000	0x00016000	0x00017000	0x00055000
raw-size	0x0000FC00 (64512)	0x00004600 (17920)	0x00000200 (512)	0x0003E000 (253952)	0x00002000 (8192)
raw-data	0x00000400	0x00010000	0x00014600	0x00014800	0x00052800
PointerToRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
PointerToLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
md5	E2EDDCBF3691B5D953...	8AD708C60F15D409737...	C14DF587968AE58C77D...	1A9E9ADDCCDADC2A7E...	60324B2F4248EF2C2290...
cave	0x000000170 (368)	0x00000018 (24)	0x00000000 (0)	0x00000088 (136)	0x000000C4 (196)
entropy	6.343	4.872	2.096	7.966	4.893
entry-point	x	-	-	-	-
obfuscated	-	-	-	-	-
blacklisted	-	-	-	-	-
readable	x	x	x	x	x
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
cachable	x	x	x	x	x

Fig.5 Program Sections

## Fig 6 Section Contents

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

symbol (259)	blacklisted (106)	anonymous (3)	anti-debug (1)	library (14)
PathFindFileNameW	x	-	-	shlwapi.dll
PathRemoveFileSpecW	x	-	-	shlwapi.dll
AlphaBlend	x	-	-	msimg32.dll
WinHttpConnect	x	-	-	winhttp.dll
WinHttpCloseHandle	x	-	-	winhttp.dll
WinHttpQueryHeaders	x	-	-	winhttp.dll
WinHttpWriteData	x	-	-	winhttp.dll
WinHttpOpenRequest	x	-	-	winhttp.dll
WinHttpReadData	x	-	-	winhttp.dll
WinHttpAddRequest	x	-	-	winhttp.dll
WinHttpSendRequest	x	-	-	winhttp.dll
WinHttpReceiveResponse	x	-	-	winhttp.dll
WinHttpOpen	x	-	-	winhttp.dll
ColInitializeEx	x	-	-	ole32.dll
CoUninitialize	x	-	-	ole32.dll
StringFromGUID2	x	-	-	ole32.dll
CryptImportPublickey	x	-	-	crypt32.dll
CryptStringToBinaryA	x	-	-	crypt32.dll
CryptDecodeObjectEx	x	-	-	crypt32.dll
_except_handler3	-	-	-	msvcr3.dll
memcpv	-	-	-	msvcr3.dll

Fig.7 Http Imports

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

symbol (259)	blacklisted (106)	anonymous (3)	anti-debug (1)	library (14)
ReplyMessage	x	-	-	user32.dll
CryptAcquireContextW	x	-	-	advapi32.dll
RegSetValueExW	x	-	-	advapi32.dll
RegEnumKeyExW	x	-	-	advapi32.dll
RegFlushKey	x	-	-	advapi32.dll
CryptSetKeyParam	x	-	-	advapi32.dll
CryptGetKeyParam	x	-	-	advapi32.dll
CryptReleaseContext	x	-	-	advapi32.dll
CryptImportKey	x	-	-	advapi32.dll
CryptEncrypt	x	-	-	advapi32.dll
CryptGenKey	x	-	-	advapi32.dll
CryptDestroyKey	x	-	-	advapi32.dll
CryptDecrypt	x	-	-	advapi32.dll
CryptGetHashParam	x	-	-	advapi32.dll
CryptCreateHash	x	-	-	advapi32.dll
CryptDestroyHash	x	-	-	advapi32.dll
CryptHashData	x	-	-	advapi32.dll
RegCreateKeyExW	x	-	-	advapi32.dll
CryptExportKey	x	-	-	advapi32.dll
RegDeleteKeyW	x	-	-	advapi32.dll
ReqDeleteValueW	x	-	-	advapi32.dll

Fig.8 Crypto and Registry Imports

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

symbol (259)	blacklisted (106)	anonymous (3)	anti-debug (1)	library (14)
SizeofResource	x	-	-	kernel32.dll
LockResource	x	-	-	kernel32.dll
CreateProcessW	x	-	-	kernel32.dll
SetFilePointerEx	x	-	-	kernel32.dll
FindNextFileW	x	-	-	kernel32.dll
GetCurrentThreadId	x	-	-	kernel32.dll
GetProcessHeap	x	-	-	kernel32.dll
GetEnvironmentVaria...	x	-	-	kernel32.dll
CopyFileExW	x	-	-	kernel32.dll
FindClose	x	-	-	kernel32.dll
FindFirstFileW	x	-	-	kernel32.dll
<b>DeleteFileW</b>	<b>x</b>	<b>-</b>	<b>-</b>	<b>kernel32.dll</b>
SetLastError	x	-	-	kernel32.dll
FlushFileBuffers	x	-	-	kernel32.dll
WriteFile	x	-	-	kernel32.dll
SetFileTime	x	-	-	kernel32.dll
ResumeThread	x	-	-	kernel32.dll
QueryPerformanceC...	x	-	-	kernel32.dll
SetFileAttributesW	x	-	-	kernel32.dll
GetFileAttributesW	x	-	-	kernel32.dll
Sleep	x	-	-	kernel32.dll

Fig.9 Delete Imports

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

symbol (259)	blacklisted (106)	anonymous (3)	anti-debug (1)	library (14)
GetFileTime	-	-	-	kernel32.dll
GetFileSizeEx	-	-	-	kernel32.dll
ReadFile	-	-	-	kernel32.dll
EnterCriticalSection	-	-	-	kernel32.dll
LeaveCriticalSection	-	-	-	kernel32.dll
InitializeCriticalSection	-	-	-	kernel32.dll
<b>CreateFileW</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>kernel32.dll</b>
ExpandEnvironmentS...	-	-	-	kernel32.dll
WaitForMultipleObje...	-	-	-	kernel32.dll
ResetEvent	-	-	-	kernel32.dll
LocalFree	-	-	-	kernel32.dll
CloseHandle	-	-	-	kernel32.dll
GetLastError	-	-	-	kernel32.dll
GetHandleInformation	-	-	-	kernel32.dll
SetEvent	-	-	-	kernel32.dll
WaitForSingleObject	-	-	-	kernel32.dll
MessageBoxIndirectW	-	-	-	user32.dll
ClientToScreen	-	-	-	user32.dll
GetWindowLongW	-	-	-	user32.dll
GetClassNameW	-	-	-	user32.dll
GetCaretPos	-	-	-	user32.dll

Fig.10 Create Imports

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

type	size	location	blacklisted (217)	item (4171)
unicode	4	-	-	Name
unicode	8	-	-	Location
unicode	7	-	-	s/home/
unicode	4	-	-	name
unicode	5	-	-	group
unicode	6	-	-	method
unicode	4	-	-	code
unicode	6	-	-	amount
unicode	4	-	-	@com
unicode	5	-	-	co.uk
unicode	4	-	-	info
unicode	5	-	-	@/w%p
unicode	9	-	-	PublicKey
unicode	10	-	-	PrivateKey
unicode	11	-	-	VersionInfo
unicode	21	-	-	Software\CryptoLocker
unicode	27	-	-	Software\CryptoLocker\Files
unicode	6	-	-	Tahoma
unicode	11	-	-	RICHEDIT50W
unicode	6	-	-	Tahoma
unicode	11	-	-	RICHEDIT50W
unicode	6	-	-	Tahoma
unicode	6	-	-	Tahoma
unicode	17	-	-	msctls_progress32
unicode	6	-	-	Tahoma
unicode	13	-	-	SysListView32

Fig.11 CryptoLocker String

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

type	size	location	blacklisted (217)	item (4171)
unicode	5	-	x	*.x3f
unicode	5	-	x	*.der
unicode	5	-	x	*.cer
unicode	5	-	x	*. crt
unicode	5	-	x	*. pem
unicode	5	-	x	*. pfx
unicode	5	-	x	*. p12
unicode	5	-	x	*. p7b
unicode	5	-	x	*. p7c
unicode	9	-	x	@.tmp.tmp
unicode	53	-	x	Microsoft Enhanced RSA and AES Cryptographic Provider
unicode	46	-	x	Microsoft Enhanced Cryptographic Provider v1.0
unicode	13	-	x	@Msftedit.dll
unicode	11	-	x	@urlmon.dll
unicode	4	-	x	POST
unicode	8	-	x	HTTP/1.1
unicode	13	-	x	Wadvapi32.dll
unicode	8	-	x	moneypak
unicode	7	-	x	ComSpec
unicode	4	-	x	.bat
unicode	4	-	x	.exe
unicode	10	-	x	Select all
unicode	34	-	x	Your personal files are encrypted!
unicode	45	-	x	Software\Microsoft\Windows\CurrentVersion\Run
ascii	40	-	-	!This program cannot be run in DOS mode.
ascii	4	-	-	Rich

Fig.12 Important Strings

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

	type	size	location	blacklisted (217)	item (4171)
...	unicode	5	-	x	*.3fr
... indicators (9/16)	unicode	5	-	x	*.aw
... virustotal (offline)	unicode	5	-	x	*.srf
... dos-stub (176 bytes)	unicode	5	-	x	*.sr2
... file-header (20 bytes)	unicode	5	-	x	*.bay
... optional-header (224 byte)	unicode	5	-	x	*.cnv
... directories (4/15)	unicode	5	-	x	*.cr2
... sections (5)	unicode	5	-	x	*.dcr
... libraries (3/14)	unicode	5	-	x	*.kdc
... imports (106/259)	unicode	5	-	x	*.erf
... exports (n/a)	unicode	5	-	x	*.mef
... exceptions (n/a)	unicode	5	-	x	*.nrv
... tls-callbacks (n/a)	unicode	5	-	x	*.orf
resources (Rich Text)	unicode	5	-	x	*.raf
abc strings (217/4171)	unicode	5	-	x	*.raw
debug (n/a)	unicode	5	-	x	*.rwl
manifest (invoker)	unicode	5	-	x	*.rw2
version (n/a)	unicode	5	-	x	*.r3d
certificate (n/a)	unicode	5	-	x	*.ptx
overlay (n/a)	unicode	5	-	x	*.pef
	unicode	5	-	x	*.srw
	unicode	5	-	x	*.x3f
	unicode	5	-	x	*.der
	unicode	5	-	x	*.cer
	unicode	5	-	x	*.crt
	unicode	5	-	x	*.pem
	unicode	5	-	x	*.pfx
	unicode	5	-	x	*.p12
	unicode	5	-	x	*.p7b
	unicode	5	-	x	*.p7c
	unicode	9	-	x	@.tmp.tmp

Fig.13 File types

pestudio 8.55 - Malware Initial Assessment - www.winito.com

	type	size	location	blacklisted (217)	item (4171)
... \ indicators (9/16)	ascii	13	-	x	RegSetValueEx
... \ virustotal (offline)	ascii	14	-	x	ShellExecuteEx
... \ dos-stub (176 bytes)	ascii	17	-	x	CommandLineToArgv
... \ file-header (20 bytes)	ascii	11	-	x	UxTheme.dll
... \ optional-header (224 bytes)	ascii	16	-	x	PathFindFileName
... \ directories (4/15)	ascii	18	-	x	PathRemoveFileSpec
... \ sections (5)	ascii	11	-	x	MSIMG32.dll
... \ libraries (3/14)	ascii	22	-	x	WinHttpReceiveResponse
... \ imports (106/259)	ascii	18	-	x	WinHttpSendRequest
... \ exports (n/a)	ascii	16	-	x	WinHttpWriteData
... \ exceptions (n/a)	ascii	14	-	x	WinHttpConnect
... \ tls-callbacks (n/a)	ascii	18	-	x	WinHttpCloseHandle
... \ resources (Rich Text)	ascii	19	-	x	WinHttpQueryHeaders
abc \ strings (217/4171)	ascii	11	-	x	WinHttpOpen
... \ debug (n/a)	ascii	18	-	x	WinHttpOpenRequest
... \ manifest (invoker)	ascii	15	-	x	WinHttpReadData
... \ version (n/a)	ascii	24	-	x	WinHttpAddRequestHeaders
... \ certificate (n/a)	ascii	11	-	x	WINHTTP.dll
... \ overlay (n/a)	ascii	11	-	x	gdplus.dll
	ascii	15	-	x	StringFromGUID2
	ascii	13	-	x	CoTaskMemFree
	ascii	14	-	x	CoUninitialize
	ascii	14	-	x	CoInitializeEx
	ascii	11	-	x	CRYPT32.dll
	ascii	5	-	x	^% .c
	ascii	5	-	x	EDE.Z
	unicode	15	-	x	184.164.136.134
	unicode	5	-	x	*.odt
	unicode	5	-	x	*.ods
	unicode	5	-	x	*.odp
	unicode	5	-	x	*.odm

Fig.14 Http and IP

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

type	size	location	blacklisted (217)	item (4171)
ascii	13	-	x	FlashWindowEx
ascii	11	-	x	PostMessage
ascii	14	-	x	CryptExportKey
ascii	19	-	x	CryptAcquireContext
ascii	16	-	x	CryptSetKeyParam
ascii	16	-	x	CryptGetKeyParam
ascii	19	-	x	CryptReleaseContext
ascii	14	-	x	CryptImportKey
ascii	12	-	x	CryptEncrypt
ascii	11	-	x	CryptGenKey
ascii	15	-	x	CryptDestroyKey
ascii	12	-	x	CryptDecrypt
ascii	17	-	x	CryptGetHashParam
ascii	15	-	x	CryptCreateHash
ascii	16	-	x	CryptDestroyHash
ascii	13	-	x	CryptHashData
ascii	14	-	x	RegCreateKeyEx
ascii	11	-	x	RegCloseKey
ascii	15	-	x	RegQueryValueEx
ascii	15	-	x	RegQueryInfoKey
ascii	12	-	x	RegDeleteKey
ascii	14	-	x	RegDeleteValue
ascii	12	-	x	RegEnumValue
ascii	12	-	x	RegOpenKeyEx
ascii	11	-	x	RegFlushKey
ascii	12	-	x	RegEnumKeyEx
ascii	13	-	x	RegSetValueEx
ascii	14	-	x	ShellExecuteEx
ascii	17	-	x	CommandLineToArgv
ascii	11	-	x	UxTheme.dll
ascii	16	-	x	PathFindFileName

Fig.15 Crypto and Registry Strings

pestudio 8.55 - Malware Initial Assessment - www.winitor.com

type	size	location	blacklisted (217)	item (4171)
ascii	14	-	-	GdipCloneImage
ascii	14	-	-	GdipPlusStartup
ascii	15	-	-	GdipDeleteBrush
ascii	14	-	-	GdipCloneBrush
ascii	25	-	-	GdipCreateFontFromLogfont
ascii	28	-	-	GdipSetStringFormatLineAlign
ascii	14	-	-	GdipDeleteFont
ascii	18	-	-	GdipDeleteGraphics
ascii	18	-	-	GdipDrawImageRect
ascii	24	-	-	GdipSetStringFormatAlign
ascii	19	-	-	GdipCreateSolidFill
ascii	14	-	-	GdipDrawString
ascii	17	-	-	GdipCreateFromHDC
ascii	31	-	-	GdipSetStringFormatHotkeyPrefix
ascii	22	-	-	GdipCreateStringFormat
ascii	22	-	-	GdipDeleteStringFormat
ascii	20	-	-	GdipCreateFontFromDC
ascii	18	-	-	GdipGetImageHeight
ascii	17	-	-	GdipGetImageWidth
ascii	9	-	-	ole32.dll
ascii	19	-	-	CryptStringToBinary
ascii	19	-	-	CryptDecodeObjectEx
ascii	24	-	-	CryptImportPublicKeyInfo
ascii	16	-	-	_except_handler3
ascii	6	-	-	memcpy
ascii	6	-	-	memset

Fig.16 Crypto Strings

pestudio 8.55 - Malware Initial Assessment - www.winitor.com				
	type	size	location	blacklisted (217) item (4171)
c:\users\malware\Desktop\pr...	unicode	7	-	@Tahoma
└ indicators (9/16)	unicode	14	-	@I'll be back!
└ virustotal (offline)	unicode	10	-	MainWindow
└ dos-stub (176 bytes)	unicode	10	-	@300 USD
└ file-header (20 bytes)	unicode	9	-	300 EUR
└ optional-header (224 bytes)	unicode	9	-	300 AUD
└ directories (4/15)	unicode	9	-	600 BRL
└ sections (5)	unicode	9	-	300 CAD
└ libraries (3/14)	unicode	9	-	6000 CZK
└ imports (106/259)	unicode	9	-	3000 DKK
└ exports (n/a)	unicode	9	-	300 GBP
└ exceptions (n/a)	unicode	9	-	3000 MXN
└ tls-callbacks (n/a)	unicode	9	-	4500 NOK
└ resources (Rich Text)	unicode	9	-	600 NZD
└ strings (217/4171)	unicode	9	-	1500 PLN
└ debug (n/a)	unicode	9	-	600 RON
└ manifest (invoker)	unicode	9	-	4500 SEK
└ version (n/a)	unicode	9	-	2 BTC
└ certificate (n/a)	unicode	5	-	ukash
└ overlay (n/a)	unicode	5	-	cashu
	unicode	7	-	bitcoin
	unicode	11	-	Courier New
	unicode	8	-	Explorer
	unicode	7	-	explore
	unicode	9	-	@echo off
	unicode	7	-	:Repeat

Fig.17 Currencies and amount

## Basic Dynamic Analysis

Cryptolocker when it is first run, hides its presence from the user by creating a secondary executable and then deleting the initial executable file from the system. The secondary executable is hidden in the system and the typical user is not aware of its existence until it becomes active. The malware creates the secondary file in either \AppData or \LocalAppData as shown below. The malware initially keeps pinging a large number of command and control servers in the hopes of establishing a connection with an active one. It supposedly gets the list of urls to attempt connection to from its Domain Generation Algorithm (DGA). Once it successfully establishes an HTTP connection to one of these C2 servers, it then identifies itself to the server which generates a Public-Private key pair for use by it. The malware then becomes active and encrypts the user's files using the public key and holds the private key for a limited amount of time for ransom.

Cryptolocker also creates an autorun registry key shown below as "HKU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"CryptoLocker" : <filepath>" to ensure persistence of the malware across reboots. The malware also stores configuration data in "HKU\SOFTWARE\CryptoLocker" like the public key received from the C2 server.

It is also observed that the executable files use a random filename of 32 characters like {7EFA68C6-086B-43E1-A2D2-55A113531240}.

From the dynamic analysis, we see that the DGA produces a large number of domain names across seven possible Top-Level-Domains: net, biz, com, org, info, ru and co.uk. The domain names generated are 15 alphabetical characters long and are provided below. This is possibly due to the frequent shift of the C2 domains used by malware hosts to avoid detection or compromise. Further aspects of the malware are discussed in the following sections.

Process Hacker [WIN-KANAJBRNOSV\Malware]

Name	PID	CPU	I/O total ...	Private b...	User name	Description
svchost.exe	868			6.08 MB		Host Process for Windows Ser...
svchost.exe	964	0.13	168 B/s	5.27 MB		Host Process for Windows Ser...
spoolsv.exe	1056			5.15 MB		Spooler SubSystem App
svchost.exe	1096			9.57 MB		Host Process for Windows Ser...
VGAuthService.exe	1292			3.05 MB		VMware Guest Authentication...
vm vmtoolsd.exe	1328	0.08		5.98 MB		VMware Tools Core Service
MsMpEng.exe	1356			72.58 MB		Antimalware Service Executable
svchost.exe	1748			872 kB		Host Process for Windows Ser...
msdtc.exe	952			1.9 MB		Microsoft Distributed Transac...
SearchIndexer.exe	2116			15.52 MB		Microsoft Windows Search In...
svchost.exe	2696			1.2 MB		Host Process for Windows Ser...
lsass.exe	516			2.46 MB		Local Security Authority Proce...
csrss.exe	424			1.56 MB		Client Server Runtime Process
winlogon.exe	452			1.06 MB		Windows Logon Application
dwm.exe	680	0.23		64.23 MB		Desktop Window Manager
explorer.exe	2476	0.08		37.54 MB	WIN-KANAJ...\\Malware	Windows Explorer
vm vmtoolsd.exe	3060	0.13		2.7 MB	WIN-KANAJ...\\Malware	VMware Tools Core Service
Procmon.exe	3484			1.23 MB	WIN-KANAJ...\\Malware	Process Monitor
Procmon.exe	2608			4.83 MB	WIN-KANAJ...\\Malware	Process Monitor
ProcessHacker.exe	2816	1.42		6.81 MB	WIN-KANAJ...\\Malware	Process Hacker
regshot.exe	2828			92.74 MB	WIN-KANAJ...\\Malware	Regshot
{252C7B1F-0437-1206-001F...}	2952	0.91	460 B/s	1.97 MB	WIN-KANAJ...\\Malware	
{252C7B1F-0437-1206-0...}	2772			880 kB	WIN-KANAJ...\\Malware	

Fig.18.1 Subprocess running under main process

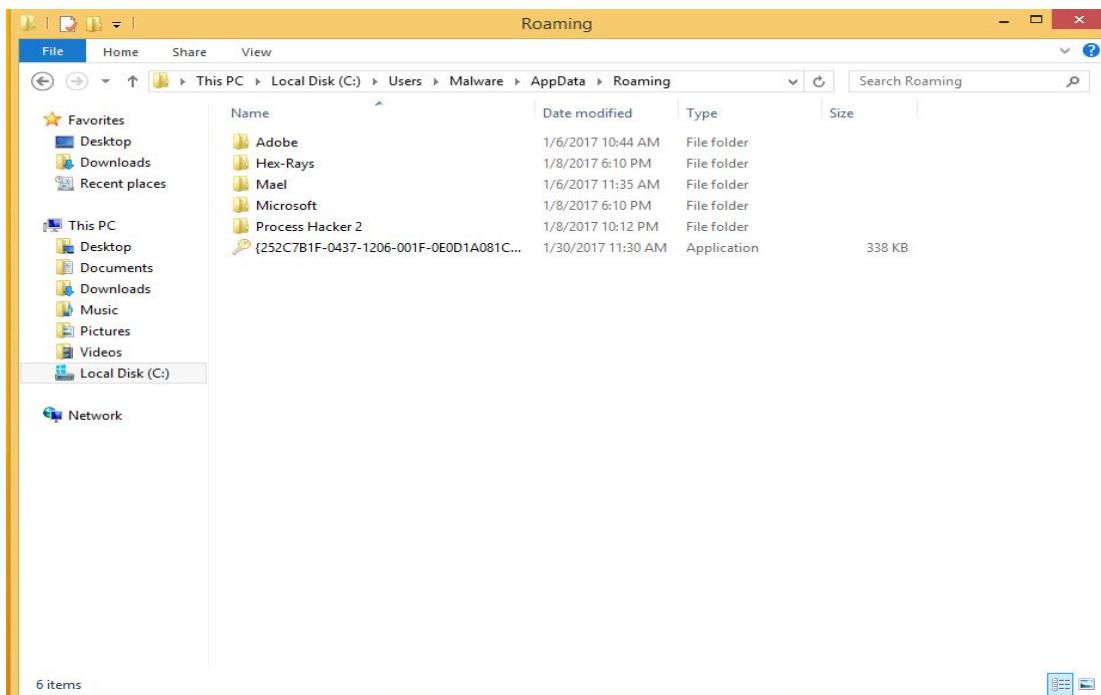


Fig.18.2 Hidden secondary executable

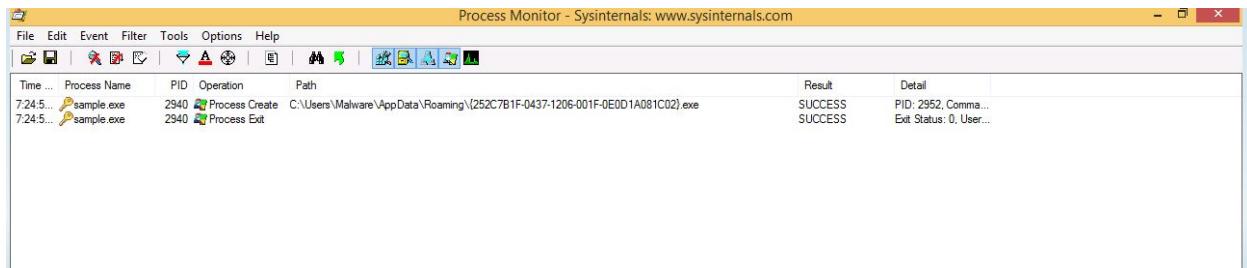


Fig.19 Creation of secondary executable and deletion of first executable

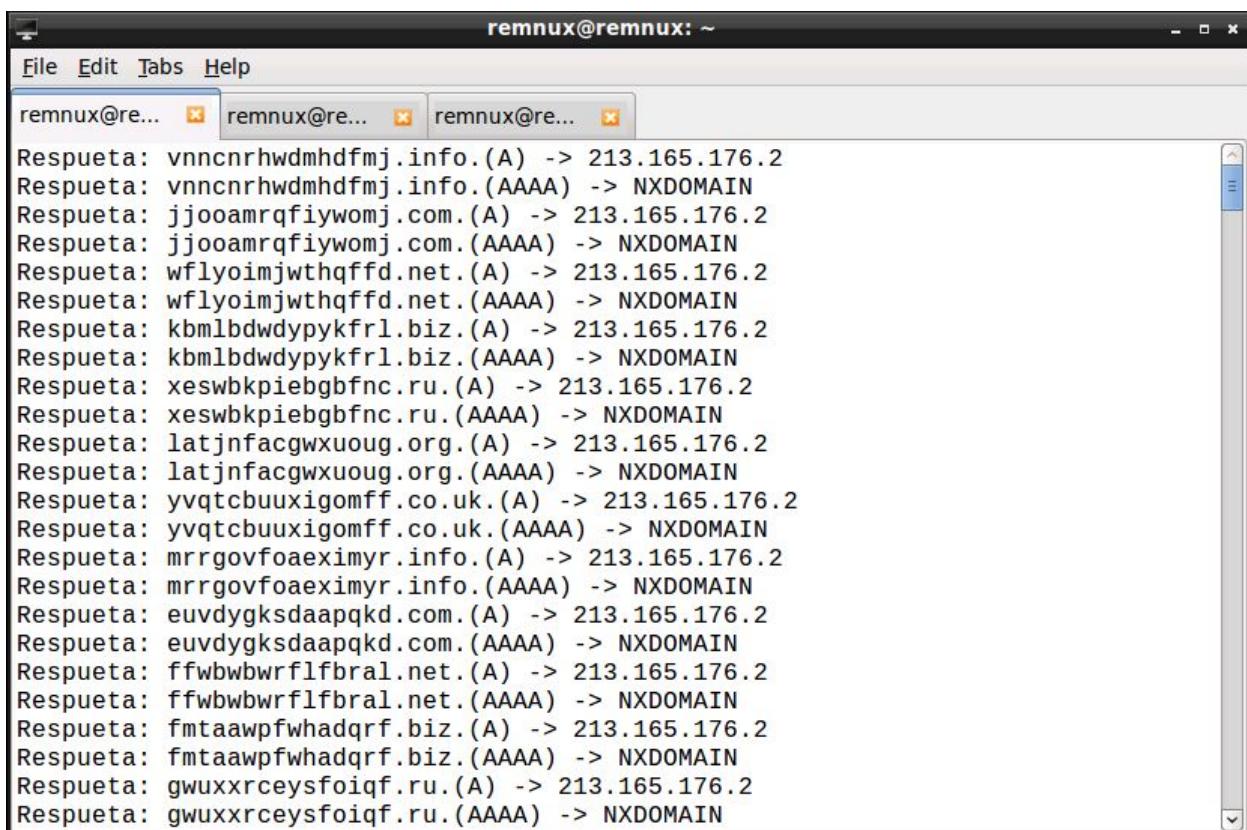


Fig.20 Attempting connection to urls generated by DGA

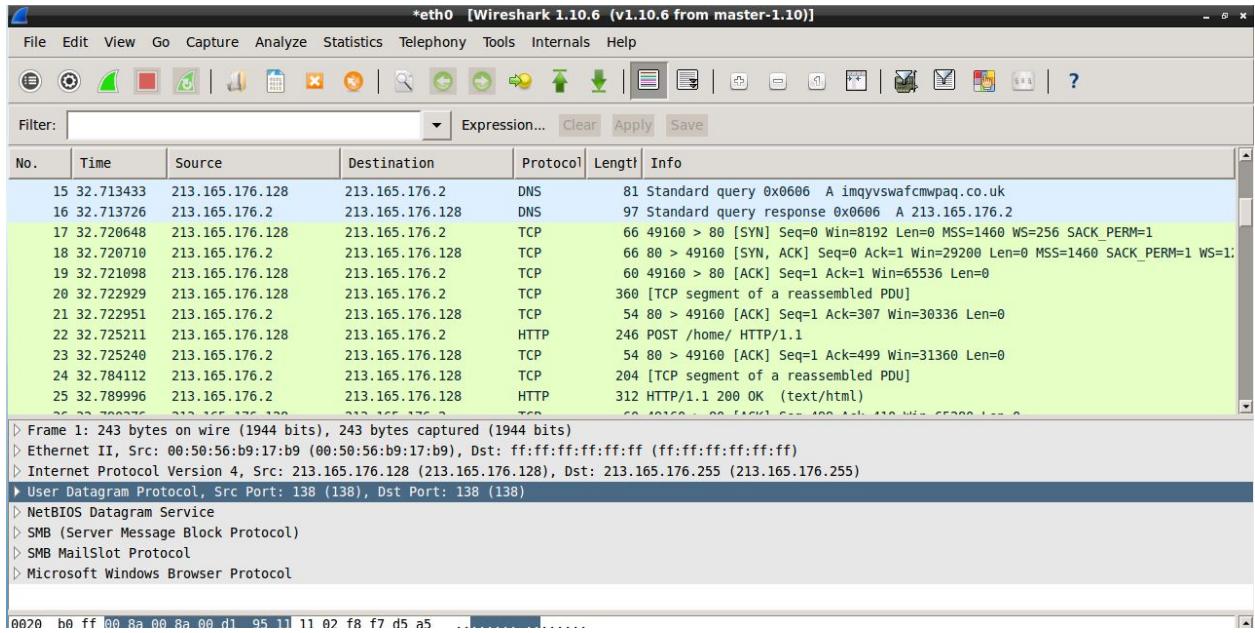


Fig.21 Attempion TCP and HTTP connection to the url.

```
Regshot 1.8.3-beta1VS
Comments:
Datetime:2017/2/20 12:21:40 , 2017/2/20 12:36:49
Computer:WIN-KANAJBRNOSV , WIN-KANAJBRNOSV
Username:Malware , Malware

-----
Keys added:7
-----
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Modules\GlobalSettings\Sizer
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\PrimaryProperties
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\PrimaryProperties\UnindexedLocations
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\Inherit
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\Inherit
```

Fig.22 Registry keys added

```

Values added:31
-----
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Modules\GlobalSettings\Sizer\PageSpaceControlsizer: A0
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\PrimaryProperties\UnindexedLocations\SearchOnly
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences\AutoWildCard: 0x00000001
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences\EnableNaturalQuerySyntax: 0x00000000
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences\WholeFileSystem: 0x00000000
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences\SystemFolders: 0x00000001
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences\ArchivedFiles: 0x00000000
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker: "C:\Users\Malware\AppData\Roaming\{252C781F-0
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{7EFA68C6-086B-43E1-A2D2-55A113531240}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{F81E9010-6E44-11CE-A7FF-00AA003CA9F6}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{1F2E5C40-9550-11CE-99D2-00AA006E086C}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{A47DE0A0-AD25-11D0-98A8-0000361B1803}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{596AB062-B4D2-4215-9F74-E9109B0A1813}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ECDF5F43-45CC-11CE-B9BF-0080C87CDBA6}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{748F5920-B42A-42A0-1069-A2E4-00002B30309D}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{748F5920-FB24-4D09-B360-BAF6F199A0D6}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{0E32D9F9-10F8-4B90-8B24-826B079084D0}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{69375D35-B310-40FD-A7D0-9548E10BC3B5}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{35A5E985-12E6-46EE-B385-E887F394FB0}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{9C07355E-C50A-45D2-B4A3-0A8235F8847F}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{BBB93890-CB46-4855-ADA6-4570E7342B3C}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{C139C040-532D-451B-80CA-44D1F0839D2A}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{E2765AC3-564C-40F9-AC12-CD393FBAA0F}
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\{C:\Users\Malwar
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\MuiCache\18\52C6487E@zipfldr.dll,-10530: "Zip"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\MuiCache\18\52C6487E@explorerframe.dll,-14418: "Fax"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\FolderType: "Generic"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\MuiCache\18\52C6487E@zipfldr.dll,-10530: "Zip"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\MuiCache\18\52C6487E@explorerframe.dll,-14418: "Fax"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\FolderType: "Generic"

```

Fig.23 Registry values added

```

File Edit Format View Help
-res_0000 - Notepad
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\{C:\Users\Malwar
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\MuiCache\18\52C6487E@zipfldr.dll,-10530: "Zip"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\MuiCache\18\52C6487E@explorerframe.dll,-14418: "Fax"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\FolderType: "Generic"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\MuiCache\18\52C6487E@zipfldr.dll,-10530: "Zip"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\MuiCache\18\52C6487E@explorerframe.dll,-14418: "Fax"
HKU\S-1-5-21-2312279452-2117245222-1845265772-1001 Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\118\Shell\FolderType: "Generic"

Values modified:20
-----
HKLMSOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter: 31 00 31 38 34 37 00 32 00 53 79 73 74 65 60 00 34 00 4D 65 60 6F 72 79 00 36 00 25 2
2F 73 65 63 00 33 36 00 43 61 63 68 65 20 46 61 75 6C 74 73 2F 73 65 63 00 33 38 00 44 65 6D 61 6E 64 20 5A 65 72 6F 20 46 61 75 6C 74 73 2F 73 65 63 00 34
9 74 65 73 00 37 30 00 53 79 73 74 65 60 20 43 6F 64 65 20 52 65 73 69 64 65 6E 74 20 42 79 74 65 73 00 37 32 00 53 79 73 74 65 6D 20 44 72 69 76 65 72 50 5
38 00 58 69 6E 26 52 65 61 64 73 2F 73 65 63 00 31 30 00 53 79 66 63 20 50 69 6E 26 52 65 61 64 73 2F 73 65 63 00 31 30 00 41 73 79 6E 63 20 50 69 6E
3 65 63 00 31 33 30 00 46 61 73 74 20 52 65 61 64 20 52 65 73 6F 75 72 63 65 20 4D 69 73 73 65 72 63 65 00 31 33 32 00 46 61 73 74 20 52 65 61 64 20 4
72 76 65 72 2F 73 65 63 00 31 35 38 00 45 6F 75 60 65 72 61 74 69 66 6E 73 20 44 6F 60 61 69 66 2F 73 65 63 00 31 36 30 00 45 6E 75 60 65 72 61 74 69 6E
3 65 63 00 31 33 30 00 46 61 73 74 20 52 65 61 64 20 52 65 73 6F 75 72 63 65 20 4D 69 73 73 65 63 00 31 33 32 00 46 61 73 74 20 52 65 61 64 20 4
1 67 65 20 46 69 6C 65 20 42 79 74 65 73 00 31 38 36 00 50 72 69 76 61 74 65 20 42 79 74 65 73 00 31 38 38 00 41 6E 6E 6F 75 65 63 65 60 65 6E 74 73 20 54 6
65 61 64 20 42 79 74 65 73 2F 73 65 63 00 32 32 00 44 69 73 68 20 57 72 69 74 65 20 42 79 74 65 73 2F 73 65 63 00 32 32 34 00 41 76 67 2E 20 44 69 73 6B
3 00 32 35 36 00 46 75 74 65 76 63 00 32 35 38 00 53 65 63 74 69 66 6E 73 00 32 36 30 00 46 62 64 65 63 74 73 00 32 36 32 00 52 65 64 69 72 65 63 74 6F 7
65 2F 73 65 63 00 32 38 00 57 72 69 74 65 20 42 79 74 65 73 20 46 77 6F 72 6B 2F 73 65 63 00 32 38 00 52 65 61 64 20 4F 76 65 72 61 74 69 6E 6
2 72 6F 72 73 73 65 63 00 33 31 34 00 53 65 72 76 65 72 20 53 65 73 69 6F 6E 73 00 33 31 36 00 53 65 72 76 65 72 20 52 65 63 66 6F 6E 66 65 63 74 73 00 3
6F 67 6F 6E 00 33 35 30 00 45 72 72 6F 72 73 20 41 63 63 65 73 73 20 50 65 72 6D 69 73 69 6F 6E 73 00 33 35 32 00 45 72 72 6F 72 73 20 47 72 61 6E 74 65
C 69 6E 6B 20 4E 65 74 42 49 4F 53 00 34 38 00 58 61 63 68 65 74 73 2F 73 65 63 00 34 38 00 43 6F 6E 74 65 78 74 20 42 6C 6F 63 68 73 20 51 75 65 7 6
34 33 30 00 46 61 69 6C 75 72 65 73 20 52 65 73 6F 6D 6F 74 65 00 34 33 32 00 46 61 69 6C 75 72 65 73 20 52 65 73 6F 75 72 63 65 20 4C
9 74 65 73 20 53 65 6E 74 2F 73 65 63 00 34 36 00 46 72 61 60 65 73 20 52 65 63 65 69 76 65 64 2F 73 65 63 00 34 36 00 46 72 61 60 65 20 42 79 74 65 7
69 6E 6B 20 53 58 00 34 39 32 00 4E 65 74 42 45 55 49 00 34 39 34 00 4E 65 74 42 45 55 49 00 20 52 65 73 6F 75 72 63 65 00 34 39 36 00 55 73 65 64 20 4D 61
3 32 00 58 61 63 68 65 74 73 20 52 65 63 65 69 76 65 64 20 55 6E 6B 6F 77 6E 00 35 33 36 00 58 61 63 68 65 74 73 28 53 65 6E 74 20 55 6E 69 63 61 73 74 2
67 62 61 63 73 20 52 65 63 65 69 76 65 64 00 35 36 32 00 44 61 74 61 67 62 61 6D 20 52 65 63 65 69 76 65 64 20 44 65 6C 66
5 63 65 69 76 65 64 2F 73 65 63 00 35 38 00 40 65 73 73 61 67 65 73 20 52 65 63 65 69 76 65 64 20 45 72 72 6F 72 73 00 35 39 30 00 52 65 63 65 69 76 65 6
73 68 20 52 65 70 6C 79 00 36 31 32 00 4D 65 73 73 61 67 65 73 20 53 65 6E 74 2F 73 65 63 00 36 31 34 00 4D 65 73 73 61 67 65 73 20 4F 75 74 62 6F 75 65 6E 64
0 36 34 30 00 53 65 67 68 65 6E 74 73 2F 73 65 63 00 36 34 32 00 43 6F 6E 65 63 74 69 6F 6E 73 20 45 73 74 61 62 6C 69 73 68 65 64 00 36 34 30 00 43 6F 6
74 6F 72 61 67 65 20 55 66 69 74 00 36 37 32 00 43 6C 6F 63 61 74 69 6F 6E 20 46 61 69 6C 75 72 65 73 00 36 37 34 00 53 79 73 74 65 6D 20 55 70 20 54 69
5 73 61 67 65 00 37 30 00 25 20 55 73 61 67 65 20 58 65 61 68 00 37 30 36 00 53 74 61 72 74 20 41 64 64 72 65 73 73 00 37 30 38 00 55 73 65 72 20 50 43 0
4F 6E 6C 79 00 37 33 30 00 52 65 73 65 72 65 64 20 53 70 61 63 65 20 52 65 61 64 2F 57 72 69 74 65 00 37 33 32 00 52 65 73 65 72 65 64 20 53 70 61 63
1 73 73 69 67 6E 65 64 20 53 70 61 63 65 20 45 78 65 63 75 74 61 62 6C 65 00 37 35 34 00 55 6E 61 73 73 69 67 6E 65 64 20 53 70 61 63 65 20 45 78 65 63 20 5
```

Fig.24 Registry Values modified

### **Further Static and Dynamic analysis**

The Malware Cryptolocker, uses cryptographic libraries provided by Microsoft's CryptoAPI. It uses the "Microsoft Enhanced RSA and AES Cryptographic Provider" to create keys and to encrypt data. It is seen using IDA that the malware calls 'CryptAcquireContextW' which sets configuration data like flags and context for use by the encryption and decryption functions. The malware receives the public key to use in the encryption process from the C2 server that it establishes an HTTP connection with, which it stores in the "HKU\SOFTWARE\Cryptolocker" registry key. Once the environment is set, the program calls 'CryptEncrypt' (as shown below) to encrypt the data.

The same functionality works in reverse where the malware upon receiving payment from the user, obtains the private key from the C2 server which it stores in the same registry key.

Afterwards, it makes a call to the 'CryptDecrypt' function to decrypt the user's files and return them to him.

The malware initially begins the entire encryption process by calculating the free space available for use in each drive as shown below. Once this is obtained, it makes a call to 'GetLogicalDrives' which obtains a list of all the drives on the system. Further, the 'GetDriveTypeW' function determines whether the drives are local or network based. These drives are then chosen for encryption and the files inside them that match the previously mentioned file formats are listed. The files are finally encrypted using the keys obtained from the C2 server and written back to disc. The encrypted files can only be recovered by using the private key held by the C2 server for ransom.

Furthermore, the malware appears to use command line arguments which it converts to an array of pointers to the arguments for use by the program as shown below. It is assumed that the command line arguments pertain to the GUI properties like language used, currency etc. On investigating deeper into the malware using IDA, we see further evidence for our previous claims by seeing implementations for the different currencies and prices. Certain code is also seen that creates a new executable file using 'WriteFile' and deletes the existing file using 'DeleteFileW'. We assume this corresponds to the malware hiding its presence by deleting itself and creating a secondary executable for its functioning.

Finally, we also witness a lot of HTTP implementations as shown below. 'WinHttpOpenRequest' and 'WinHttpAddRequestHeaders' opens an HTTP request and modifies the package headers. Once this is done a 'WinHttpSendRequest' launches the request to the target domain. 'WinHttpWriteData' and 'WinHttpReceiveResponse' handle the response received from the domain. This adds further evidence to our initial statement that the malware receives the public-private key pair from the C2 server it connects to.

Function name

```

f sub_404420
f sub_404620
f sub_404690
f sub_4046C0
f sub_404720
f sub_4047C0
f sub_4048A0
f sub_4048F0
f sub_404960
f sub_404A50
f sub_404AC0
f sub_404BA0
f sub_404C90
f sub_404D10
f sub_404D60
f sub_404E00
f sub_404E50
< f sub_404620

```

Line 53 of 321

Graph overview

```

loc_404642:
push 0F0000040h ; dwFlags
push 18h ; dwProvType
push offset szProvider ; "Microsoft Enhanced RSA and AES Cryptogr"...
push 0 ; szContainer
push esi ; phProv
call ds:CryptAcquireContextW
test eax, eax
jnz short loc_40467E

loc_404667:
push 0F0000040h ; dwFlags
push 18h ; dwProvType
push offset aMicrosoftEnh_1 ; "Microsoft Enhanced RSA and AES Cryptogr"
push 0 ; szContainer
push esi ; phProv
call ds:CryptAcquireContextW
test eax, eax
jnz short loc_40467E

```

100.00% (76,225) (248,174) 00003A20 00404620: sub 404620 (Synchronized with Hex View-1)

Fig.25 Setting environment for cryptographic libraries

Function name

```

f sub_404420
f sub_404620
f sub_404690
f sub_4046C0
f sub_404720
f sub_4047C0
f sub_4048A0
f sub_4048F0
f sub_404960
f sub_404A50
f sub_404AC0
f sub_404BA0
f sub_404C90
f sub_404D10
f sub_404D60
f sub_404E00
f sub_404E50
< f sub_404620

```

Line 53 of 321

Graph overview

```

Src= dword ptr 0
pdwDataLen= dword ptr 0Ch
arg_8= dword ptr 10h

push ebp
mov ebp, esp
push ecx
mov eax, ecx
push ebx
cmp dword ptr [eax], 1
mov ebx, [ebp+pdwDataLen]
push esi
mov [ebp+var_4], eax
ja short loc_40499A

loc_40499A:
push 0 ; dwBufLen
lea ecx, [ebp+pdwDataLen]
push ecx ; pdwDataLen
push 0 ; pbData
push 0 ; dwFlags
push 1 ; Final
push 0 ; hHash
push dword ptr [eax+8] ; hKey
mov [ebp+pdwDataLen], ebx
call ds:CryptEncrypt
mov esi, [ebp+pdwDataLen]
or ecx, 0FFFFFFFh
test eax, eax
cmovz esi, ecx
jmp short loc_40499C

```

100.00% (-129,126) (292,427) 00003D60 00404960: sub\_404960 (Synchronized with Hex View)

Fig.26 Encryption using CryptEncrypt

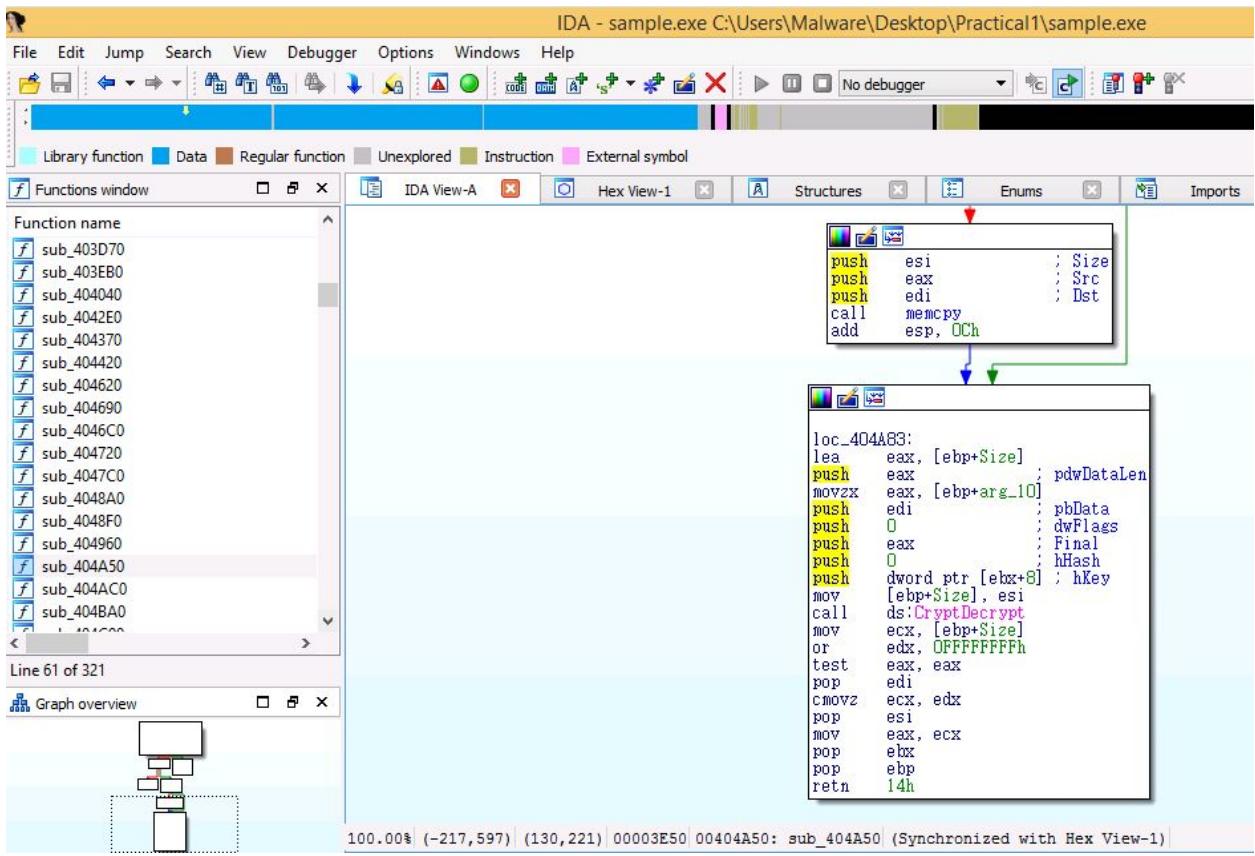


Fig.27 Decryption using CryptDecrypt

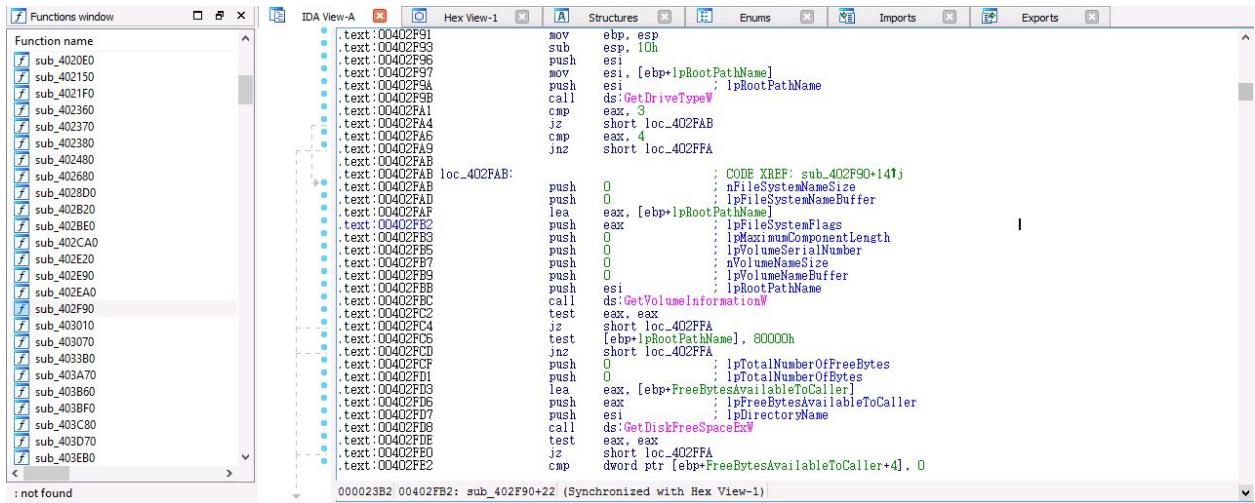


Fig.28.1 Acquiring Free Space

Function name

```

and    esp, 0FFFFFFF8h
sub   esp, 334h
push  ebx
push  esi
mov   esi, ecx
push  edi
mov   [esp+340h+Handles], esi
call  ds:GetLogicalDrives
xor   bl, bl
mov   edx, eax
mov   [esp+340h+var_330], edx
mov   dword ptr [esp+340h+RootPathName], 3A0000h
mov   [esp+340h+var_324], 5Ch
cmp   [ebp+arg_0], bl
jz    loc_403221

```

```

mov   esi, dword_4160E0
push  0FFFFFFF8h ; dwMilliseconds
push  dword ptr [esi+38h] ; hHandle
mov   [esp+348h+FileSystemFlags], esi
call  ds:WaitForSingleObject
test  eax, eax
jz    short loc_4030D0

```

Fig.28.2 Calling GetLogicalDrives

Function name

```

and    esp, 0FFFFFFF8h
sub   esp, 334h
push  ebx
push  esi
mov   esi, ecx
push  edi
mov   [esp+340h+Handles], esi
call  ds:GetLogicalDrives
xor   bl, bl
mov   edx, eax
mov   [esp+340h+var_330], edx
mov   dword ptr [esp+340h+RootPathName], 3A0000h
mov   [esp+340h+var_324], 5Ch
cmp   [ebp+arg_0], bl
jz    loc_403221

```

```

movzx  eax, bl
add   ax, 41h
mov   [esp+340h+RootPathName], ax
lea   eax, [esp+340h+RootPathName]
push  eax ; lpRootPathName
call  ds:GetDriveTypeW
cmp   eax, 3
jz    short loc_4032A0

```

```

loc_4032A0:      ; nFileSystemNameSize
push  0           ; lpFileSystemNameBuffer
push  0           ; lpFileSystemFlags
lea   eax, [esp+348h+FileSystemFlags]
push  eax ; lpFileSystemFlags
push  0           ; lpMaximumComponentLength
push  0           ; lpVolumeSerialNumber
push  0           ; nVolumeNameSize
push  0           ; lpVolumeNameBuffer
lea   eax, [esp+35Ch+RootPathName]
push  eax ; lpRootPathName
call  ds:GetVolumeInformationW
test  eax, eax
jz    short loc_403338

```

Fig.28.3 Calling GetDriveTypeW after

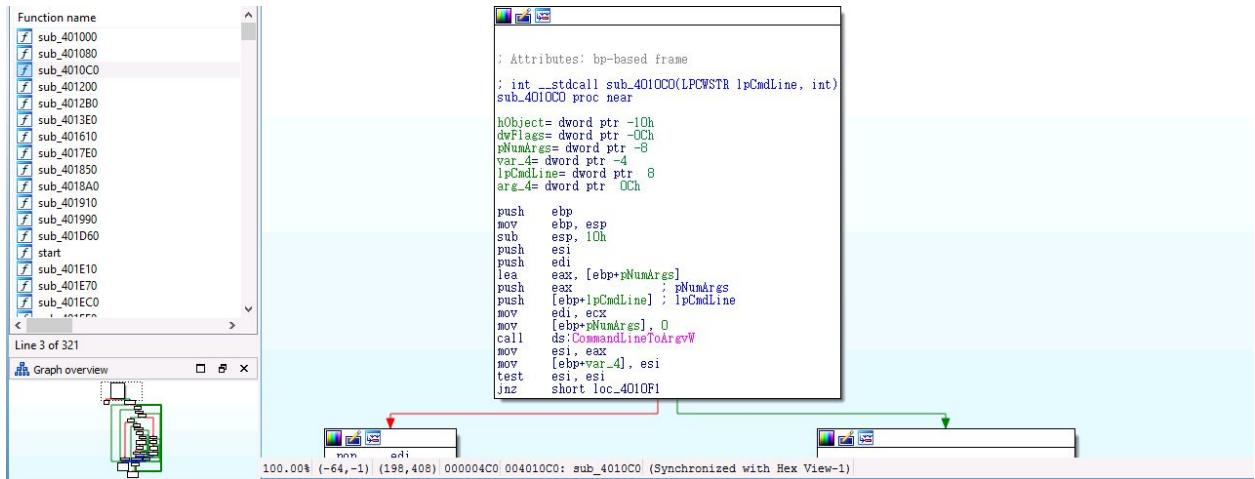


Fig.29 CommandLineToArgvW

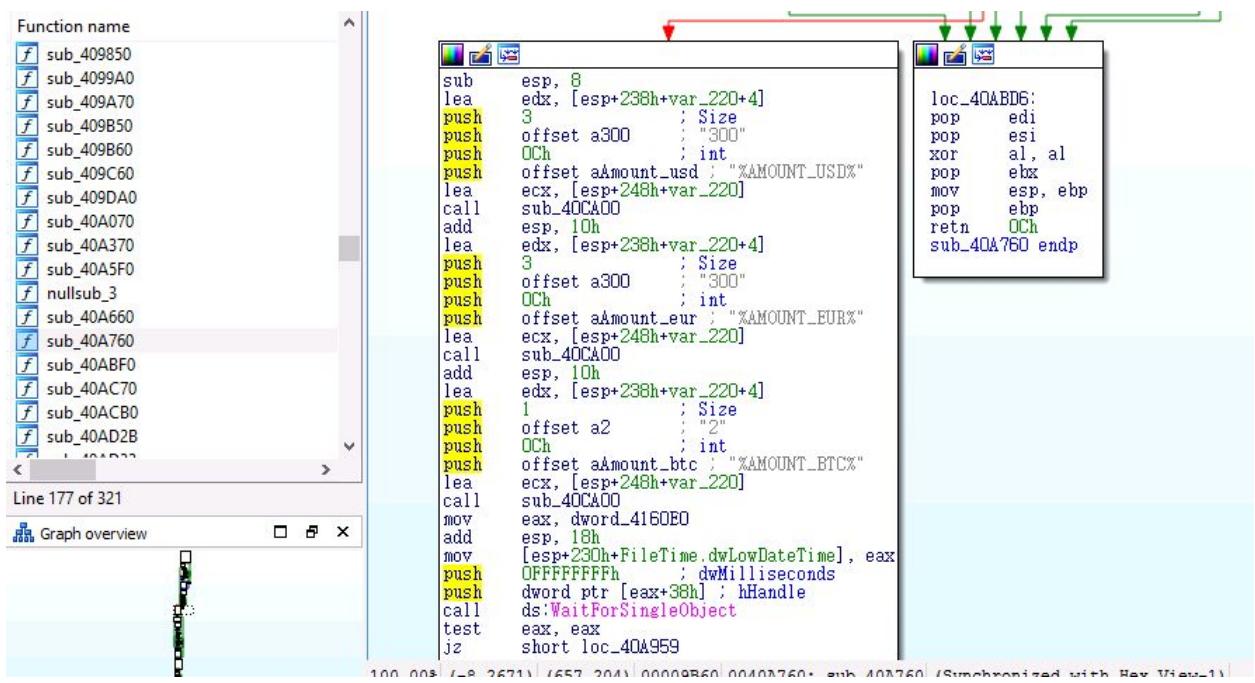


Fig.30 Currencies and prices

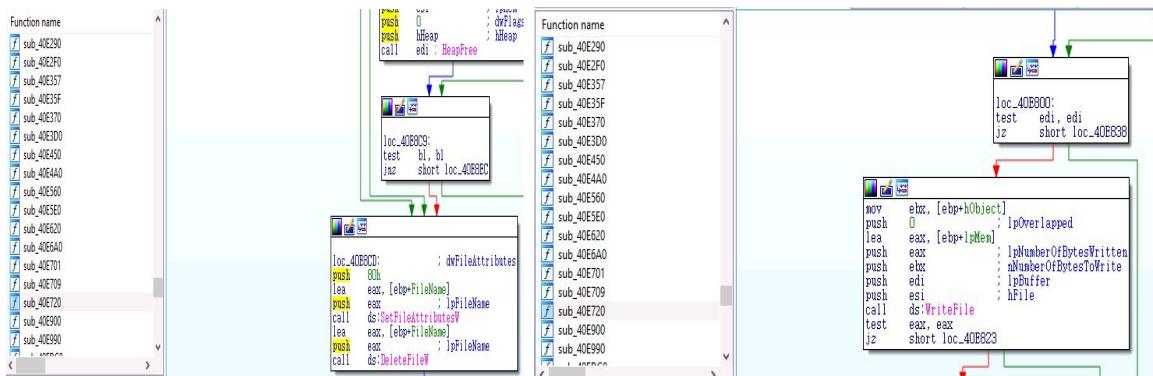


Fig.31 Creation and Deletion of executables

Function name

sub_4080F0	.text:004080F0	push	lpszpWws2ObjectName	, pwszObjectName
sub_408160	.text:00408160	push	ecx	pwszVerb
sub_408250	.text:00408250	push	dword ptr [esi+4]	; hConnect
sub_4082E0	.text:004082E0	call	ds:WinHttpOpenRequest	
sub_408340	.text:00408340	mov	[esi], eax	
sub_408410	.text:00408410	test	eax, eax	
sub_408640	.text:00408640	jz	short loc_4083F5	
sub_408690	.text:00408690	bl	2	
sub_408760	.text:00408760	jnz	short loc_4083B5	
sub_4087F0	.text:004087F0	push	0A0000000h	; dwModifiers
sub_408900	.text:00408900	push	13h	; dwHeadersLength
sub_408980	.text:00408980	push	offset pwszHeaders	; Connection: CloseWrWn
sub_408A70	.text:00408A70	push	eax	; hRequest
sub_408AE0	.text:00408AE0	call	ds:WinHttpAddRequestHeaders	
sub_408BC0	.text:00408BC0			; CODE XREF: sub_408340+60T
sub_408C80	.text:00408C80	loc_4083B5:		
sub_408D30	.text:00408D30	mov	eax, dword_416200	
sub_408E10	.text:00408E10	test	eax, eax	
sub_408F10	.text:00408F10	jz	short loc_4083C8	
sub_408FC0	.text:00408FC0	push	esi	
sub_409010	.text:00409010	push	dword ptr [esi]	
sub_4090C0	.text:004090C0	push	0	
sub_409140	.text:00409140	call	eax : dword_416200	
sub_4092A0	.text:004092A0	add	esp, OCh	
sub_409340	.text:00409340			; CODE XREF: sub_408340+7C1
		push	0	; dwContext
		push	[lphp+dwTotalLength]	; dwTotalLength
		push	0	; dwOptionalLength
		push	0	; lpOptional
		push	0	; dwHeadersLength
		push	0	; lpszHeaders
		push	dword ptr [esi]	; hRequest
		call	ds:WinHttpSendRequest	
		cmp	eax, 1	

Fig.32 Sending Http Request

```

Function name
f sub_407F0
f sub_407I40
f sub_407270
f sub_407300
f sub_407372
f sub_40737A
f sub_407390
f sub_4073E0
f sub_407470
f sub_407730
f sub_4078F0
f sub_4079E0
f sub_407C00
f sub_407FC0
f sub_408010

.text:004075AF
.text:004075B2
.text:004075B5
.text:004075BB
.text:004075B0
.text:004075C3
.text:004075C3 loc_4075C3:
.text:004075C3
.text:004075C5
.text:004075C8
.text:004075CB
.text:004075D0
.text:004075D6
.text:004075D9
.text:004075DE
.text:004075E3
.text:004075E9
.text:004075ED
.text:004075EF
.text:004075F2
.text:004075F4

push    [ebp+lpBuffer] ; lpBuffer
push    [ebp+hRequest] ; hRequest
call    ds:WinHttpWriteData
test   eax, eax
jz     loc_4076D4
; CODE XREF: sub_407470+138tj
push    0 ; lpReserved
push    [ebp+hRequest] ; hRequest
call    ds:WinHttpReceiveResponse
test   eax, eax
jz     loc_4076D4
lea    ecx, [ebp+hRequest]
call    sub_408640
cmp    eax, 0C8h
jnz   loc_4076D4
cmp    byte ptr [esi+38h], 0
jz     short loc_4075F4
mov    eax, [esi+34h]
jmp    short loc_4075F6

```

Fig.33 Receiving Http Response

### Indicators of compromise

The malware exhibits a large number of network based indicators. The DGA requires the malware to continuously attempt connections to a large number of urls generated by it. These urls belong to one of seven TLDs : org, com, biz, info, co.uk, ru and net. They are also 15 alphabetical characters in size and mostly appear in random order. If one observes his system attempting a large number of connections to domains that match the aforementioned pattern, then it can serve as a strong indicator of compromise.

Further, a variety of host based indicators can be found by analysing the registry and the file system. Cryptolocker initially creates an autorun registry key to ensure persistence across system reboots while the malware attempts to contact an active C2 server. This registry key "HKU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "CryptoLocker" : <Filepath>" can be used to identify the existence of the malware if the user locates it before the program establishes connection to an active server. Moreover, the registry key "HKU\SOFTWARE\CryptoLocker" stores configuration files pertaining to the malware which can again be used as an indicator.

Finally, the secondary executable created by the malware portrays a pattern in its naming. In particular, it consists of 32 random alphanumeric characters. If the user can locate hidden system files on his drives, then the identification of this executable serves as a strong indicator of potential compromise.

### Conclusion

Cryptolocker is a dangerous ransomware that is hard to mitigate once activated, hence prevention is definitely a critical priority. It uses very potent encryption algorithms and has a very efficient distribution system owing to the GameOver Zeus botnet and the pervasiveness of spam Email. Periodic backup of system files can help by facilitating system formats followed by system restores.