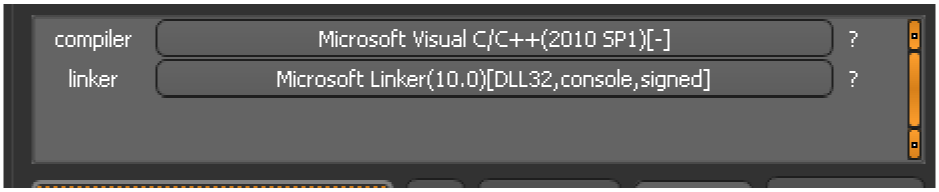
Basic static Analysis:

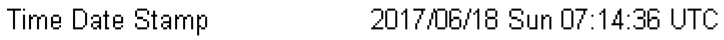
this ransomeware is not packed file and written with language called C or C++.



compiler Microsoft Visual C/C++(2010 SP1)[-] ?

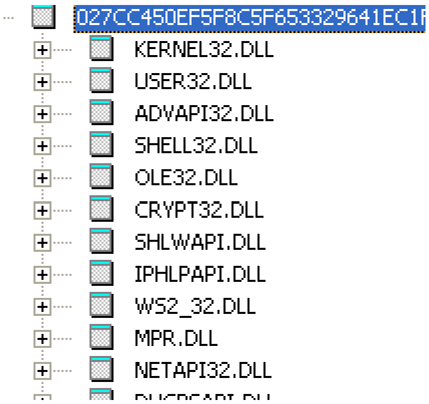
linker Microsoft Linker(10.0)[DLL32,console,signed] ?

Check for Time for Compilation of File.



Time Date Stamp 2017/06/18 Sun 07:14:36 UTC

It imports a lot of dll libraries.



```
027CC450EF5F8C5F653329641EC1F
  KERNEL32.DLL
  USER32.DLL
  ADVAPI32.DLL
  SHELL32.DLL
  OLE32.DLL
  CRYPT32.DLL
  SHLWAPI.DLL
  IPHLPAPI.DLL
  WS2_32.DLL
  MPR.DLL
  NETAPI32.DLL
  DHCPSAPI.DLL
```

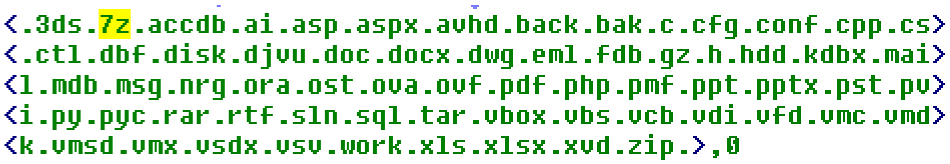
Connected Domain :

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX .

Attacker Email:

wowsmith123456@posteo.net.

Targets Some Files



```
<.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs>
<.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mai>
<l.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pv>
<i.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmd>
<k.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.>,0
```

Encryption Algorithms:

(1) AES

(2) RSA

(3) Windows Encryption

(4) ADLER 32 Encryption

(5) CRC32

(6) Zlib Compression

Process And Arguments

(1) IsWow64Process to check for malware running in OS 32 or 64 bit.

(2) ComSpec to make self-deletion.

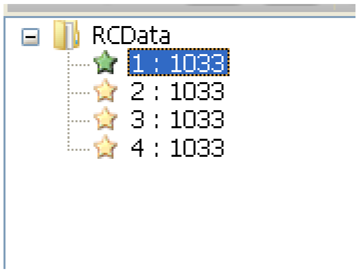
(3) Shutdown.exe /r /f to shutdown pc.

(4) %s /node:"%ws" /user:"%ws" /password:"%ws

(5) -d C:\Windows\System32\rundll32.exe "C:\Windows\%s",#1

(6) wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c (To cover tracks and delete logs)

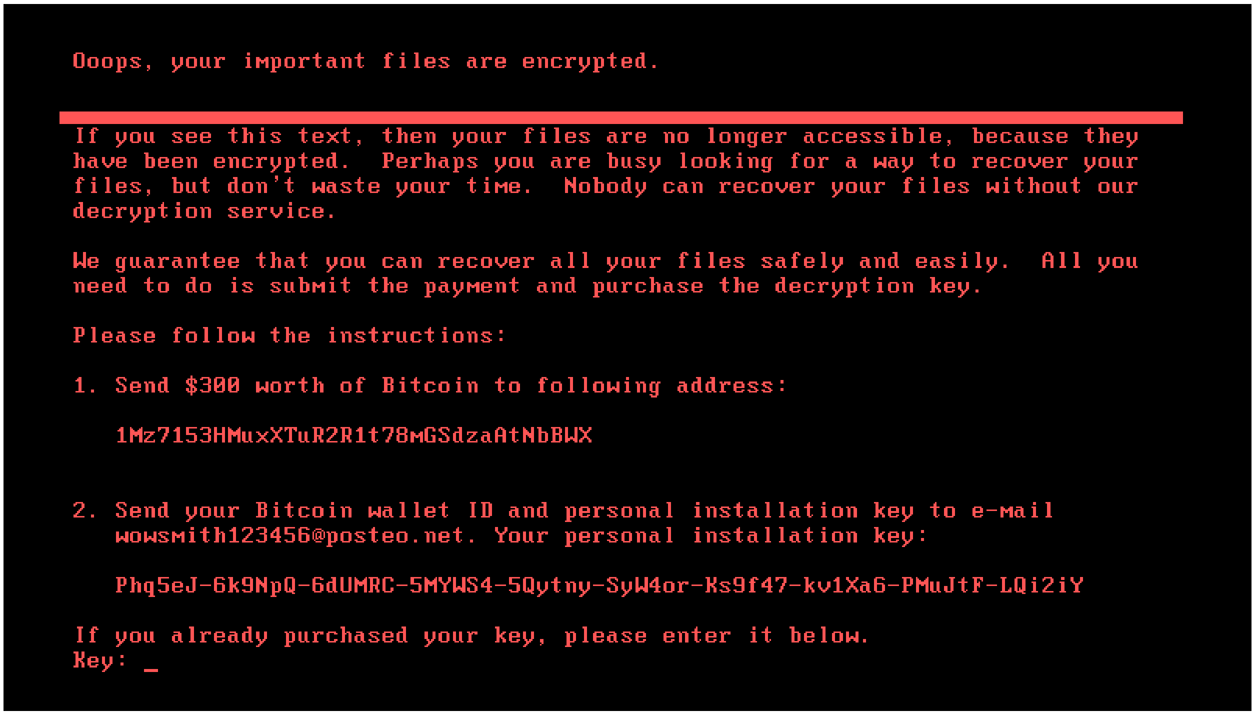
Other Resources:



RCData
1 : 1033
2 : 1033
3 : 1033
4 : 1033

Ransomware has resources that could that contain 2 versions (32 bit and 64 bit). Also contains encryption tool for AES and RSA.

After period of time it encrypts MBR File and shows this message that needs a payment to decrypt files.



```
Ooops, your important files are encrypted.

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

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

Please follow the instructions:

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

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   Phq5eJ-6k9NpQ-6dUMRC-5MYWS4-5Qytny-SyW4or-Ks9f47-kv1Xa6-PMuJtF-LQi2iY

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

Summary:

Petya ransomware is special type of other ransomware because it encrypt file system not all files in system it specially modifying master boot record (MBR) so when system reboot it causes crash and display window that need 300$ to decrypt file. Malware search for Other Ips In the table to connect with them. Get computer Name. Gain access To All Process .enumerate dhcp subnet.