University
POLITEHNICA
of Bucharest

Challenges in cyber security – Ransomware Phenomenon

Authors

Vlad-Raul Pașca

Email: vvladd_pasca@yahoo.com

Emil Simion

Email: emil.simion@upb.ro

Ransomware

- The most popular malware nowadays
- Huge profit for cybercriminals, Cryptowall produced 325 millions of dollars in 2015
- Ransomware as a service (RaaS) is giving cybercriminals (even beginners) the oportunity to launch sophisticated attacks
- Numerous families: Locky, CryptoWall, CryptoLocker, Spora, DMA Locker, Petya, Cerber, WannaCry, NotPetya/GoldenEye

Multiple distribution methods:

- Phising emails (the most popular method)
- Social Media
- Infected websites dropping malicious payload
- Exploits and 0-day exploits

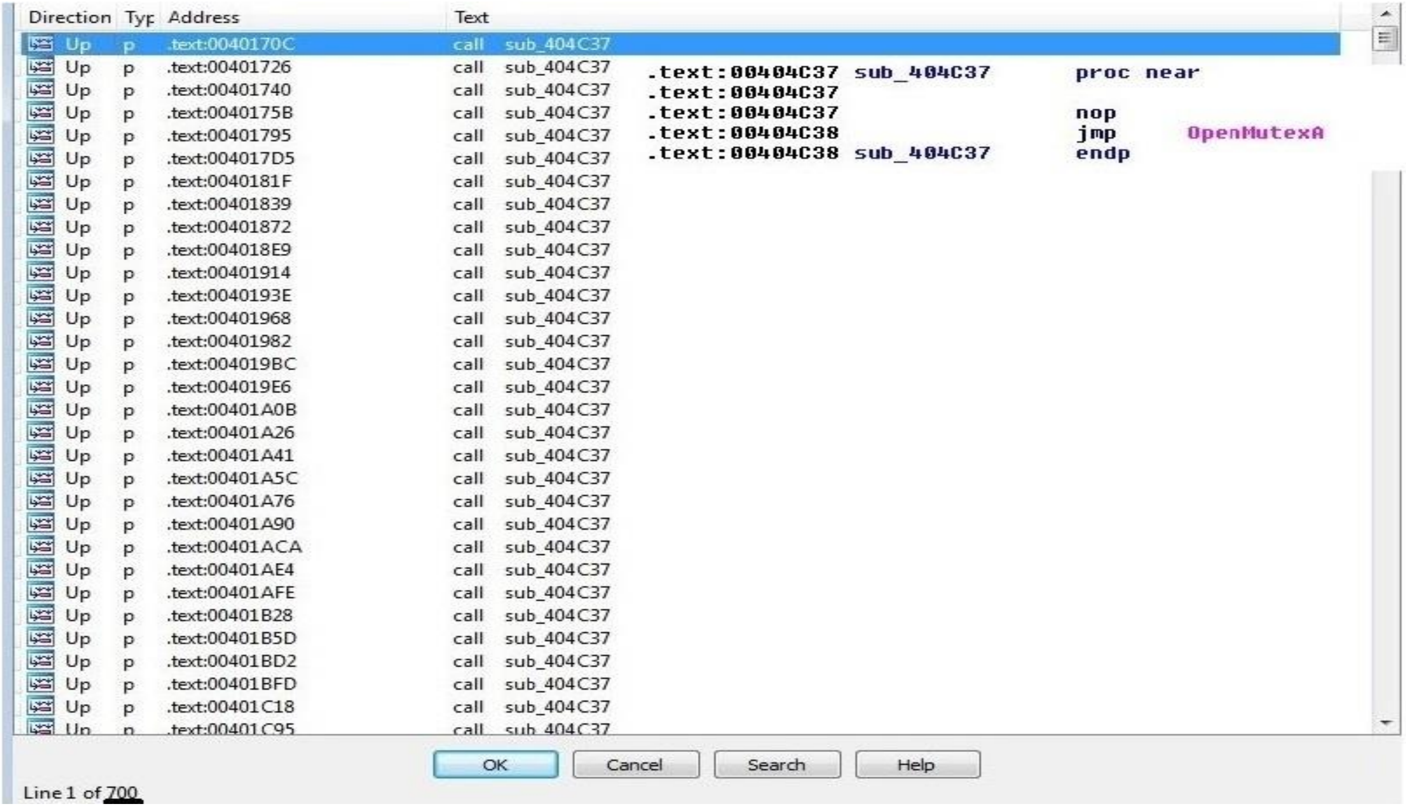
The network infection vector (EternalBlue) of WannaCry which exploits a vulnerability in Microsoft’s implementation of SMB protocol **wasn’t** a 0-day exploit

Spora ransomware

- It encrypts files offline like DMA Locker or Cerber (it doesn’t communicate with a C&C)
- RSA + AES encryption using Windows APIs (**CryptImportKey**, **CryptGenKey**, **CryptEncrypt**)
- The sample comes with an encrypted hardcoded RSA public key, for each victim is generated a new RSA 1024 pair of keys as well as a new AES key; the AES key is used to encrypt RSA private key and then itself is encrypted with RSA hardcoded key (these are stored in each ransom note); an individual AES key is generated for each file (in order to encrypt the file) and it is encrypted with RSA public key which was generated, and stored at the end of each encrypted file
- It uses VSSadmin to delete shadow copies (in order to make backup very difficult)

Spora ransomware

- The sample is obfuscated in order to make the analysis more difficult
- It tries to open a mutex (wddmnotbx) which doesn't exists (700 times)



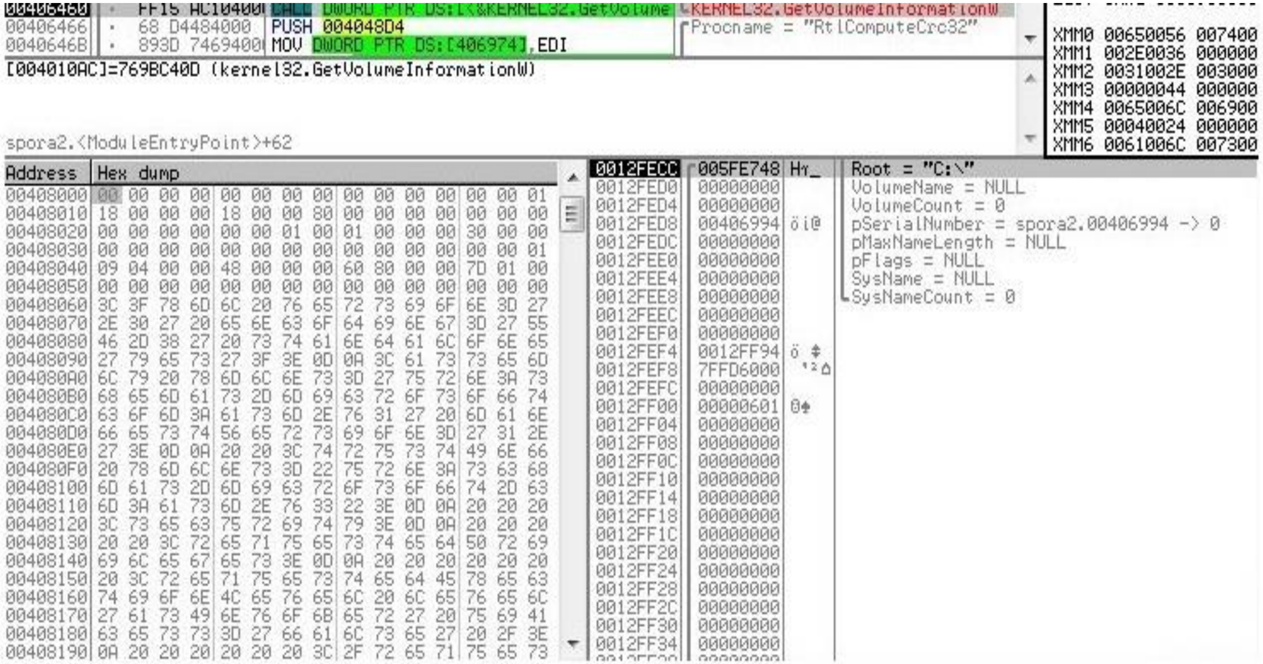
Direction	Typ	Address	Text
Up	p	.text:0040170C	call sub_404C37
Up	p	.text:00401726	call sub_404C37
Up	p	.text:00401740	call sub_404C37
Up	p	.text:0040175B	call sub_404C37
Up	p	.text:00401795	call sub_404C37
Up	p	.text:004017D5	call sub_404C37
Up	p	.text:0040181F	call sub_404C37
Up	p	.text:00401839	call sub_404C37
Up	p	.text:00401872	call sub_404C37
Up	p	.text:004018E9	call sub_404C37
Up	p	.text:00401914	call sub_404C37
Up	p	.text:0040193E	call sub_404C37
Up	p	.text:00401968	call sub_404C37
Up	p	.text:00401982	call sub_404C37
Up	p	.text:004019BC	call sub_404C37
Up	p	.text:004019E6	call sub_404C37
Up	p	.text:00401A0B	call sub_404C37
Up	p	.text:00401A26	call sub_404C37
Up	p	.text:00401A41	call sub_404C37
Up	p	.text:00401A5C	call sub_404C37
Up	p	.text:00401A76	call sub_404C37
Up	p	.text:00401A90	call sub_404C37
Up	p	.text:00401ACA	call sub_404C37
Up	p	.text:00401AE4	call sub_404C37
Up	p	.text:00401AFE	call sub_404C37
Up	p	.text:00401B28	call sub_404C37
Up	p	.text:00401B5D	call sub_404C37
Up	p	.text:00401BD2	call sub_404C37
Up	p	.text:00401BFD	call sub_404C37
Up	p	.text:00401C18	call sub_404C37
Up	p	.text:00401C95	call sub_404C37

```
.text:00404C37 sub_404C37      proc near
.text:00404C37
.text:00404C37                 nop
.text:00404C38                 jmp     OpenMutexA
.text:00404C38 sub_404C37      endp
```

Line 1 of 700

Spora ransomware

- It calls GetVolumeInformationW to get information about file system and volume associated with root dir



```
00406460  .  FF15 AC10400  CALL DWORD PTR DS:[<&KERNEL32.GetVolume   └KERNEL32.GetVolumeInformationW
00406466  .  68 D4484000   PUSH 004048D4                             ┌Procname = "RtlComputeCrc32"
0040646B  .  893D 7469400  MOV DWORD PTR DS:[406974],EDI
[004010AC]=769BC40D (kernel32.GetVolumeInformationW)

spora2.<ModuleEntryPoint>+62
```

```
XMM0 00650056 007400
XMM1 002E0036 000000
XMM2 0031002E 003000
XMM3 00000044 000000
XMM4 0065006C 006900
XMM5 00040024 000000
XMM6 0061006C 007300
```

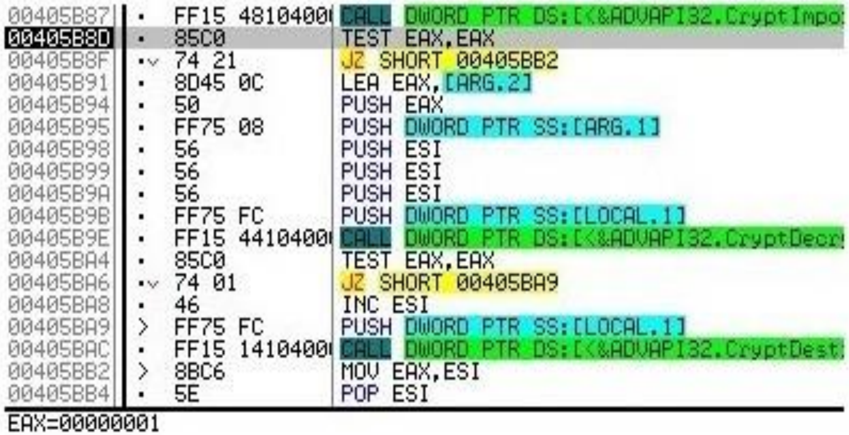
```
Address  Hex dump
00408000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
00408010 18 00 00 00 18 00 00 80 00 00 00 00 00 00 00
00408020 00 00 00 00 00 00 01 00 01 00 00 00 30 00 00
00408030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
00408040 09 04 00 00 48 00 00 00 60 80 00 00 7D 01 00
00408050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00408060 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 27
00408070 2E 30 27 20 65 6E 63 6F 64 69 6E 67 3D 27 55
00408080 46 2D 38 27 20 73 74 61 6E 64 61 6C 6F 6E 65
00408090 27 79 65 73 27 3F 3E 0D 0A 3C 61 73 73 65 6D
004080A0 6C 79 20 78 6D 6C 6E 73 3D 27 75 72 6E 3A 73
004080B0 68 65 6D 61 73 2D 6D 69 63 72 6F 73 6F 66 74
004080C0 63 6F 6D 3A 61 73 6D 2E 76 31 27 20 6D 61 6E
004080D0 66 65 73 74 56 65 72 73 69 6F 6E 3D 27 31 2E
004080E0 27 3E 0D 0A 20 20 3C 74 72 75 73 74 49 6E 66
004080F0 20 78 6D 6C 6E 73 3D 22 75 72 6E 3A 73 63 68
00408100 6D 61 73 2D 6D 69 63 72 6F 73 6F 66 74 2D 63
00408110 6D 3A 61 73 6D 2E 76 33 22 3E 0D 0A 20 20 20
00408120 3C 73 65 63 75 72 69 74 79 3E 0D 0A 20 20 20
00408130 20 20 3C 72 65 71 75 65 73 74 65 64 50 72 69
00408140 69 6C 65 67 65 73 3E 0D 0A 20 20 20 20 20 20
00408150 20 3C 72 65 71 75 65 73 74 65 64 45 78 65 63
00408160 74 69 6F 6E 4C 65 76 65 6C 20 6C 65 76 65 6C
00408170 27 61 73 49 6E 76 6F 6B 65 72 27 20 75 69 41
00408180 63 65 73 73 3D 27 66 61 6C 73 65 27 20 2F 3E
00408190 0A 20 20 20 20 20 20 3C 2F 72 65 71 75 65 73
```

```
0012FECC ┌005FE748 Hγ_    Root = "C:\"
0012FED0 │00000000        VolumeName = NULL
0012FED4 │00000000        VolumeCount = 0
0012FED8 │00406994 öi@    pSerialNumber = spora2.00406994 -> 0
0012FEDC │00000000        pMaxNameLength = NULL
0012FEE0 │00000000        pFlags = NULL
0012FEE4 │00000000        SysName = NULL
0012FEE8 │00000000       └SysNameCount = 0
0012FEEC  00000000
0012FEF0  00000000
0012FEF4  0012FF94 ö ‡
0012FEF8  7FFD6000  ¹²⌂
0012FEFC  00000000
0012FF00  00000601 0♠
0012FF04  00000000
0012FF08  00000000
0012FF0C  00000000
0012FF10  00000000
0012FF14  00000000
0012FF18  00000000
0012FF1C  00000000
0012FF20  00000000
0012FF24  00000000
0012FF28  00000000
0012FF2C  00000000
0012FF30  00000000
0012FF34  00000000
```

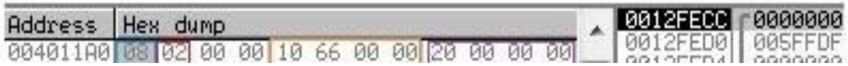
- The result is used to create a mutex which has the form: m<GetVolumeInformationWResult> to ensure that he malware runs only once

Spora ransomware

- The malware has a hardcoded key which is being imported using the function CryptImportKey



```
00405B87  .   FF15 4810400( CALL DWORD PTR DS:[<&ADVAPI32.CryptImpo:
00405B8D  .   85C0          TEST EAX,EAX
00405B8F  .v  74 21         JZ SHORT 00405BB2
00405B91  .   8D45 0C       LEA EAX,[ARG.2]
00405B94  .   50            PUSH EAX
00405B95  .   FF75 08       PUSH DWORD PTR SS:[ARG.1]
00405B98  .   56            PUSH ESI
00405B99  .   56            PUSH ESI
00405B9A  .   56            PUSH ESI
00405B9B  .   FF75 FC       PUSH DWORD PTR SS:[LOCAL.1]
00405B9E  .   FF15 4410400( CALL DWORD PTR DS:[<&ADVAPI32.CryptDecr
00405BA4  .   85C0          TEST EAX,EAX
00405BA6  .v  74 01         JZ SHORT 00405BA9
00405BA8  .   46            INC ESI
00405BA9  >   FF75 FC       PUSH DWORD PTR SS:[LOCAL.1]
00405BAC  .   FF15 1410400( CALL DWORD PTR DS:[<&ADVAPI32.CryptDest:
00405BB2  >   8BC6          MOV EAX,ESI
00405BB4  .   5E            POP ESI
EAX=00000001
```

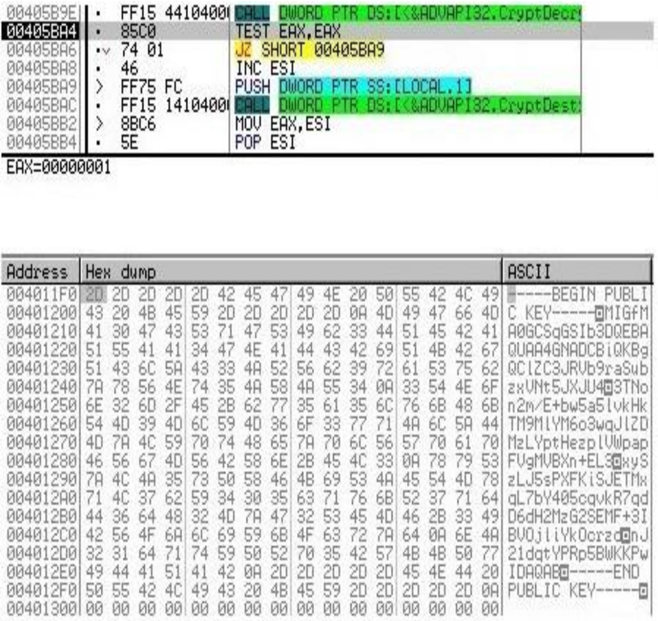


```
Address   Hex dump                                      0012FECC  0000000
004011A0  08 02 00 00 10 66 00 00 20 00 00 00           0012FED0  005FFDF
```

- It represents an AES256 key, stored in a form of blob. 0x08 represents PLAINTEXTKEY-BLOB, the key is a session key; 0x02 represents CUR_BLOB_VERSION; 0x6610 represents Alg_ID: CALG_AES_256; 0x20 represents key's length

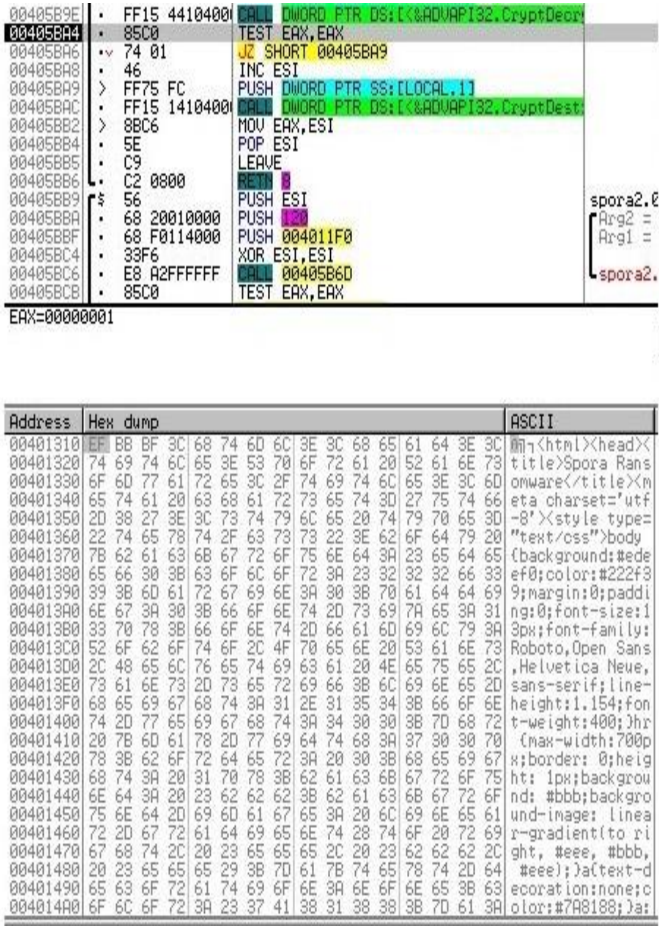
Spora ransomware

- The AES key is used to decrypt another elements, a RSA key, the ransom note and something which looks like a campaign id



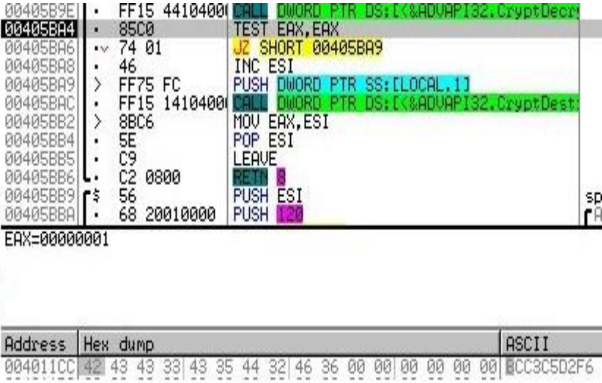
```
00405B9E  .   FF15 4410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDecr
00405BA4  .   85C0          TEST EAX,EAX
00405BA6  .v  74 01         JZ SHORT 00405BA9
00405BA8  .   46            INC ESI
00405BA9  >   FF75 FC       PUSH DWORD PTR SS:[LOCAL.1]
00405BAC  .   FF15 1410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDest
00405BB2  >   8BC6          MOV EAX,ESI
00405BB4  .   5E            POP ESI
EAX=00000001
```

```
Address  Hex dump                                         ASCII
004011F0 2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42 4C 49 -----BEGIN PUBLI
00401200 43 20 4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 47 66 4D C KEY-----□MIGfM
00401210 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 41 A0GCSqGSIb3DQEBA
00401220 51 55 41 41 34 47 4E 41 44 43 42 69 51 4B 42 67 QUAA4GNADCBiQKBg
00401230 51 43 6C 5A 43 33 4A 52 56 62 39 72 61 53 75 62 QClZC3JRVb9raSub
00401240 7A 78 56 4E 74 35 4A 58 4A 55 34 0A 33 54 4E 6F zxVNt5JXJU4□3TNo
00401250 6E 32 6D 2F 45 2B 62 77 35 61 35 6C 76 6B 48 6B n2m/E+bw5a5lvkHk
00401260 54 4D 39 4D 6C 59 4D 36 6F 33 77 71 4A 6C 5A 44 TM9MlYM6o3wqJlZD
00401270 4D 7A 4C 59 70 74 48 65 7A 70 6C 56 57 70 61 70 MzLYptHezplVWpap
00401280 46 56 67 4D 56 42 58 6E 2B 45 4C 33 0A 78 79 53 FVgMVBXn+EL3□xyS
00401290 7A 4C 4A 35 73 50 58 46 4B 69 53 4A 45 54 4D 78 zLJ5sPXFKiSJETMx
004012A0 71 4C 37 62 59 34 30 35 63 71 76 6B 52 37 71 64 qL7bY405cqvkR7qd
004012B0 44 36 64 48 32 4D 7A 47 32 53 45 4D 46 2B 33 49 D6dH2MzG2SEMF+3I
004012C0 42 56 4F 6A 6C 69 59 6B 4F 63 72 7A 64 0A 6E 4A BVOjliYkOcrzd□nJ
004012D0 32 31 64 71 74 59 50 52 70 35 42 57 4B 4B 50 77 21dqtYPRp5BWKKPw
004012E0 49 44 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44 20 IDAQAB□-----END
004012F0 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D 0A PUBLIC KEY-----□
00401300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
00405B9E  .   FF15 4410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDecr
00405BA4  .   85C0          TEST EAX,EAX
00405BA6  .v  74 01         JZ SHORT 00405BA9
00405BA8  .   46            INC ESI
00405BA9  >   FF75 FC       PUSH DWORD PTR SS:[LOCAL.1]
00405BAC  .   FF15 1410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDest
00405BB2  >   8BC6          MOV EAX,ESI
00405BB4  .   5E            POP ESI
00405BB5  .   C9            LEAVE
00405BB6  L.  C2 0800       RETN 8
00405BB9  r$  56            PUSH ESI                                   spora2.0
00405BBA  .   68 20010000   PUSH 120                                   rArg2 =
00405BBF  .   68 F0114000   PUSH 004011F0                              Arg1 =
00405BC4  .   33F6          XOR ESI,ESI
00405BC6  .   E8 A2FFFFFF   CALL 00405B6D                              Lspora2.
00405BCB  .   85C0          TEST EAX,EAX
EAX=00000001
```

```
Address  Hex dump                                         ASCII
00401310 EF BB BF 3C 68 74 6D 6C 3E 3C 68 65 61 64 3E 3C ∩╗┐<html><head><
00401320 74 69 74 6C 65 3E 53 70 6F 72 61 20 52 61 6E 73 title>Spora Rans
00401330 6F 6D 77 61 72 65 3C 2F 74 69 74 6C 65 3E 3C 6D omware</title><m
00401340 65 74 61 20 63 68 61 72 73 65 74 3D 27 75 74 66 eta charset='utf
00401350 2D 38 27 3E 3C 73 74 79 6C 65 20 74 79 70 65 3D -8'><style type=
00401360 22 74 65 78 74 2F 63 73 73 22 3E 62 6F 64 79 20 "text/css">body
00401370 7B 62 61 63 6B 67 72 6F 75 6E 64 3A 23 65 64 65 {background:#ede
00401380 65 66 30 3B 63 6F 6C 6F 72 3A 23 32 32 32 66 33 ef0;color:#222f3
00401390 39 3B 6D 61 72 67 69 6E 3A 30 3B 70 61 64 64 69 9;margin:0;paddi
004013A0 6E 67 3A 30 3B 66 6F 6E 74 2D 73 69 7A 65 3A 31 ng:0;font-size:1
004013B0 33 70 78 3B 66 6F 6E 74 2D 66 61 6D 69 6C 79 3A 3px;font-family:
004013C0 52 6F 62 6F 74 6F 2C 4F 70 65 6E 20 53 61 6E 73 Roboto,Open Sans
004013D0 2C 48 65 6C 76 65 74 69 63 61 20 4E 65 75 65 2C ,Helvetica Neue,
004013E0 73 61 6E 73 2D 73 65 72 69 66 3B 6C 69 6E 65 2D sans-serif;line-
004013F0 68 65 69 67 68 74 3A 31 2E 31 35 34 3B 66 6F 6E height:1.154;fon
00401400 74 2D 77 65 69 67 68 74 3A 34 30 30 3B 7D 68 72 t-weight:400;}hr
00401410 20 7B 6D 61 78 2D 77 69 64 74 68 3A 37 30 30 70  {max-width:700p
00401420 78 3B 62 6F 72 64 65 72 3A 20 30 3B 68 65 69 67 x;border: 0;heig
00401430 68 74 3A 20 31 70 78 3B 62 61 63 6B 67 72 6F 75 ht: 1px;backgrou
00401440 6E 64 3A 20 23 62 62 62 3B 62 61 63 6B 67 72 6F nd: #bbb;backgro
00401450 75 6E 64 2D 69 6D 61 67 65 3A 20 6C 69 6E 65 61 und-image: linea
00401460 72 2D 67 72 61 64 69 65 6E 74 28 74 6F 20 72 69 r-gradient(to ri
00401470 67 68 74 2C 20 23 65 65 65 2C 20 23 62 62 62 2C ght, #eee, #bbb,
00401480 20 23 65 65 65 29 3B 7D 61 7B 74 65 78 74 2D 64  #eee);}a{text-d
00401490 65 63 6F 72 61 74 69 6F 6E 3A 6E 6F 6E 65 3B 63 ecoration:none;c
004014A0 6F 6C 6F 72 3A 23 37 41 38 31 38 38 3B 7D 61 3A olor:#7A8188;}a:
```

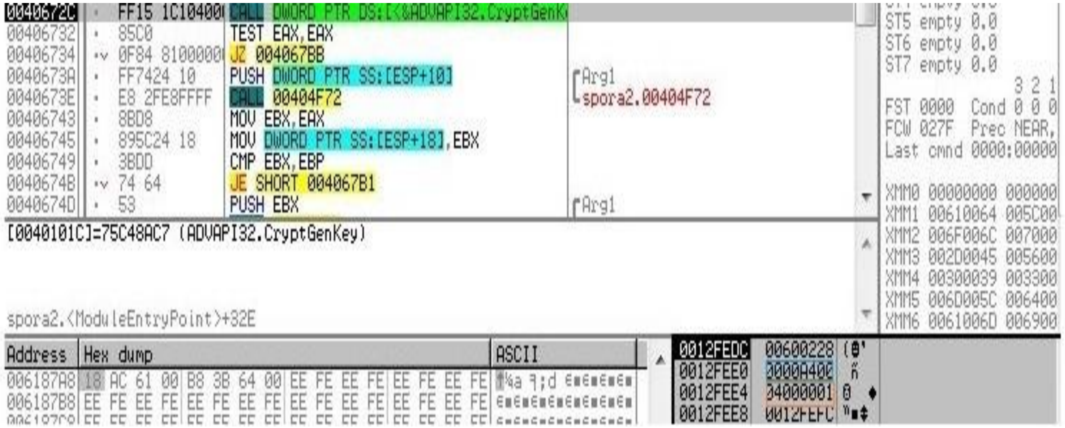


```
00405B9E  .   FF15 4410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDecr
00405BA4  .   85C0          TEST EAX,EAX
00405BA6  .v  74 01         JZ SHORT 00405BA9
00405BA8  .   46            INC ESI
00405BA9  >   FF75 FC       PUSH DWORD PTR SS:[LOCAL.1]
00405BAC  .   FF15 1410400  CALL DWORD PTR DS:[<&ADVAPI32.CryptDest
00405BB2  >   8BC6          MOV EAX,ESI
00405BB4  .   5E            POP ESI
00405BB5  .   C9            LEAVE
00405BB6  L.  C2 0800       RETN 8
00405BB9  r$  56            PUSH ESI                                   sp
00405BBA  .   68 20010000   PUSH 120                                   rA
EAX=00000001
```

```
Address  Hex dump                                         ASCII
004011CC 42 43 43 33 43 35 44 32 46 36 00 00 00 00 00 00 BCC3C5D2F6
```

Spora ransomware

- The sample uses GetLogicalDrives to obtain available disk drives, WNetOpenEnum and WNetEnumResource to enumerate the network resources
- A new pair of RSA1024 keys for every victim is generated, as is shown below:



```
0040672C  .  FF15 1C10400( CALL DWORD PTR DS:[<&ADVAPI32.CryptGenK
00406732  .  85C0          TEST EAX,EAX
00406734  .v 0F84 8100000( JZ 004067BB
0040673A  .  FF7424 10     PUSH DWORD PTR SS:[ESP+10]                 [Arg1
0040673E  .  E8 2FE8FFFF   CALL 00404F72                              [spora2.00404F72
00406743  .  8BD8          MOV EBX,EAX
00406745  .  895C24 18     MOV DWORD PTR SS:[ESP+18],EBX
00406749  .  3BDD          CMP EBX,EBP
0040674B  .v 74 64         JE SHORT 004067B1
0040674D  .  53            PUSH EBX                                   [Arg1
[0040101C]=75C48AC7 (ADVAPI32.CryptGenKey)

spora2.<ModuleEntryPoint>+32E
```

```
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1
FST 0000  Cond 0 0 0
FCW 027F  Prec NEAR,
Last cmnd 0000:00000

XMM0 0000000 000000
XMM1 00610064 005C00
XMM2 006F006C 007000
XMM3 002D0045 005600
XMM4 00300039 003300
XMM5 006D005C 006400
XMM6 0061006D 006900
```

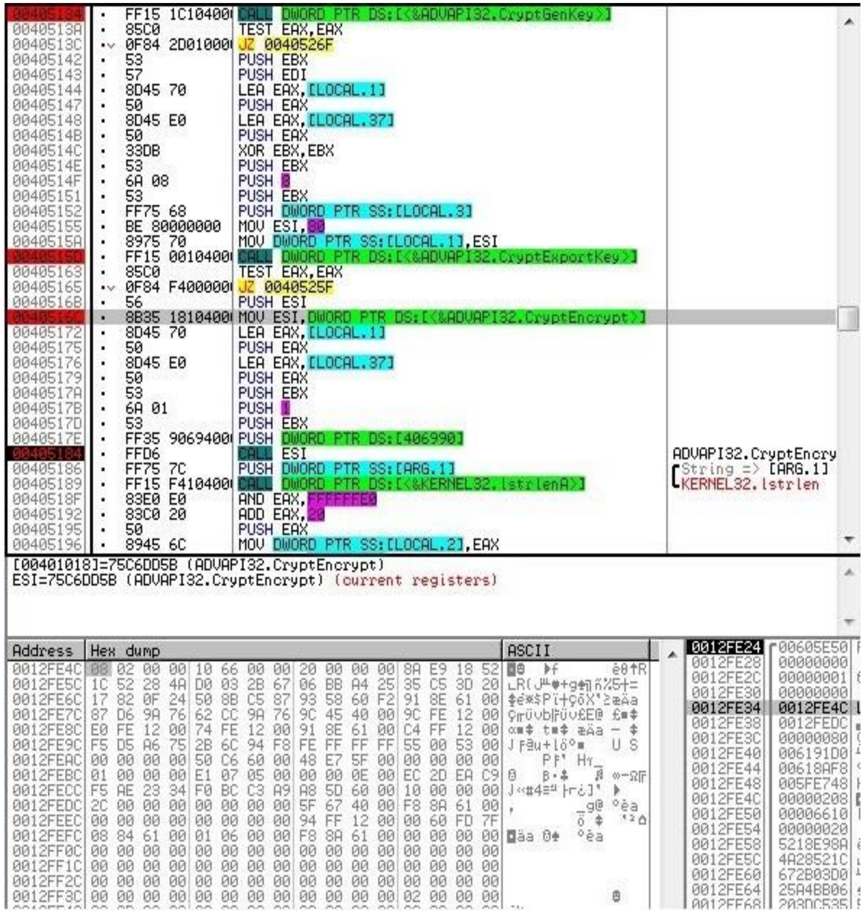
```
Address   Hex dump                                          ASCII
006187A8  18 AC 61 00|B8 3B 64 00|EE FE EE FE|EE FE EE FE   ↑¼a ╕;d ε■ε■ε■ε■
006187B8  EE FE EE FE|EE FE EE FE|EE FE EE FE|EE FE EE FE   ε■ε■ε■ε■ε■ε■ε■ε■
```

```
0012FEDC  00600228  (☻`
0012FEE0  0000A400   ñ
0012FEE4  04000001  ☺  ♦
0012FEE8  0012FEFC  ü■↕
```

- 0x600228 is a handle to CSP, 0xa400 represents AlgID: CALG_RSA_KEYX and 0x40000001 represents RSA1024BIT_KEY – CRYPT_EXPORTABLE.

Spora ransomware

- A unique AES key is generated, exported and encrypted with hardcoded RSA key, as is shown below:



```
00405134  .    FF15 1C10400( CALL DWORD PTR DS:[<&ADVAPI32.CryptGenKey>]
0040513A  .    85C0          TEST EAX,EAX
0040513C  .v   0F84 2D01000( JZ 0040526F
00405142  .    53            PUSH EBX
00405143  .    57            PUSH EDI
00405144  .    8D45 70       LEA EAX,[LOCAL.1]
00405147  .    50            PUSH EAX
00405148  .    8D45 E0       LEA EAX,[LOCAL.37]
0040514B  .    50            PUSH EAX
0040514C  .    33DB          XOR EBX,EBX
0040514E  .    53            PUSH EBX
0040514F  .    6A 08         PUSH 8
00405151  .    53            PUSH EBX
00405152  .    FF75 68       PUSH DWORD PTR SS:[LOCAL.3]
00405155  .    BE 80000000   MOV ESI,80
0040515A  .    8975 70       MOV DWORD PTR SS:[LOCAL.1],ESI
0040515D  .    FF15 0010400( CALL DWORD PTR DS:[<&ADVAPI32.CryptExportKey>]
00405163  .    85C0          TEST EAX,EAX
00405165  .v   0F84 F400000( JZ 0040525F
0040516B  .    56            PUSH ESI
0040516C  .    8B35 1810400( MOV ESI,DWORD PTR DS:[<&ADVAPI32.CryptEncrypt>]
00405172  .    8D45 70       LEA EAX,[LOCAL.1]
00405175  .    50            PUSH EAX
00405176  .    8D45 E0       LEA EAX,[LOCAL.37]
00405179  .    50            PUSH EAX
0040517A  .    53            PUSH EBX
0040517B  .    6A 01         PUSH 1
0040517D  .    53            PUSH EBX
0040517E  .    FF35 9069400( PUSH DWORD PTR DS:[406990]
00405184  .    FFD6          CALL ESI                                        ADVAPI32.CryptEncry
00405186  .    FF75 7C       PUSH DWORD PTR SS:[ARG.1]                       [String => [ARG.1]
00405189  .    FF15 F410400( CALL DWORD PTR DS:[<&KERNEL32.lstrlenA>]          [KERNEL32.lstrlen
0040518F  .    83E0 E0       AND EAX,FFFFFFE0
00405192  .    83C0 20       ADD EAX,20
00405195  .    50            PUSH EAX
00405196  .    8945 6C       MOV DWORD PTR SS:[LOCAL.2],EAX
```

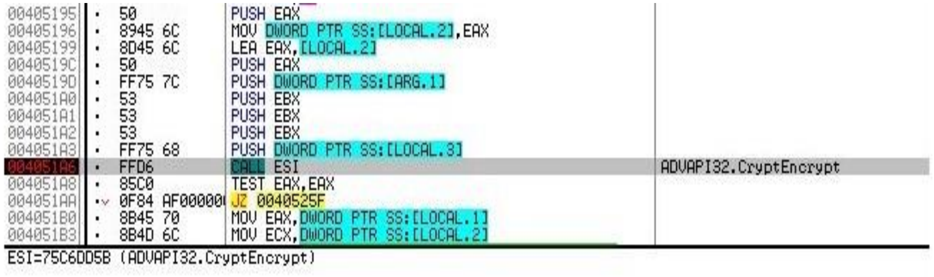
```
[00401018]=75C6DD5B (ADVAPI32.CryptEncrypt)
ESI=75C6DD5B (ADVAPI32.CryptEncrypt) (current registers)
```

```
Address  Hex dump                                         ASCII
0012FE4C 08 02 00 00 10 66 00 00 20 00 00 00 8A E9 18 52 ◘☻  ►f      è↑R
0012FE5C 1C 52 28 4A D0 03 2B 67 06 BB A4 25 35 C5 3D 20 ∟R(J╨♥+g♠╗ñ%5┼= 
0012FE6C 17 82 0F 24 50 8B C5 87 93 58 60 F2 91 8E 61 00 ↨é☼$Pï┼çôX`≥æÄa
0012FE7C 87 D6 9A 76 62 CC 9A 76 9C 45 40 00 9C FE 12 00 ç╓Üvb╠Üv£E@ £■↕
0012FE8C E0 FE 12 00 74 FE 12 00 91 8E 61 00 C4 FF 12 00 α■↕ t■↕ æÄa ─ ↕
0012FE9C F5 D5 A6 75 2B 6C 94 F8 FE FF FF FF 55 00 53 00 ⌡╒ªu+lö°■   U S
0012FEAC 00 00 00 00 50 C6 60 00 48 E7 5F 00 00 00 00 00     P╞` Hτ_
0012FEBC 01 00 00 00 E1 07 05 00 00 00 0E 00 EC 2D EA C9 ☺   ß•♣    ♫ ∞-Ω╔
0012FECC F5 AE 23 34 F0 BC C3 A9 A8 5D 60 00 10 00 00 00 ⌡«#4≡╝├⌐¿]` ►
0012FEDC 2C 00 00 00 00 00 00 00 5F 67 40 00 F8 8A 61 00 ,       _g@ °èa
0012FEEC 00 00 00 00 00 00 00 00 94 FF 12 00 00 60 FD 7F         ö ↕  `²⌂
0012FEFC 08 84 61 00 01 06 00 00 F8 8A 61 00 00 00 00 00 ◘äa ☺♠  °èa
0012FF0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF3C 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00             ☻
```

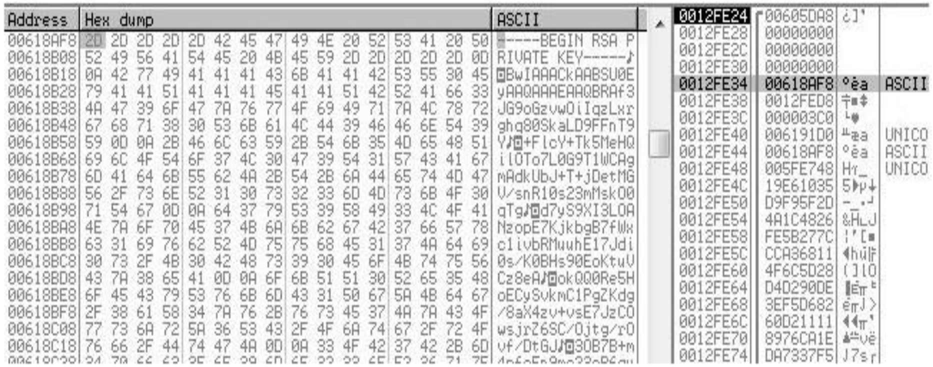
```
0012FE24  00605E50
0012FE28  00000000
0012FE2C  00000001
0012FE30  00000000
0012FE34  0012FE4C
0012FE38  0012FEDC
0012FE3C  00000080
0012FE40  006191D0
0012FE44  00618AF8
0012FE48  005FE748
0012FE4C  00000208
0012FE50  00006610
0012FE54  00000020
0012FE58  5218E98A
0012FE5C  4A28521C
0012FE60  672B03D0
0012FE64  25A4BB06
0012FE68  203DC535
```

Spora ransomware

- The AES key which was generated is used to encrypt RSA private key, as well as data about infection and the victim's machine, like date, username, country code, malware id and statistics about the encrypted files:



```
00405195  .  50           PUSH EAX
00405196  .  8945 6C      MOV DWORD PTR SS:[LOCAL.2],EAX
00405199  .  8D45 6C      LEA EAX,[LOCAL.2]
0040519C  .  50           PUSH EAX
0040519D  .  FF75 7C      PUSH DWORD PTR SS:[ARG.1]
004051A0  .  53           PUSH EBX
004051A1  .  53           PUSH EBX
004051A2  .  53           PUSH EBX
004051A3  .  FF75 68      PUSH DWORD PTR SS:[LOCAL.3]
004051A6  .  FFD6         CALL ESI                              ADVAPI32.CryptEncrypt
004051A8  .  85C0         TEST EAX,EAX
004051AA  .v 0F84 AF00000 JZ 0040525F
004051B0  .  8B45 70      MOV EAX,DWORD PTR SS:[LOCAL.1]
004051B3  .  8B4D 6C      MOV ECX,DWORD PTR SS:[LOCAL.2]
ESI=75C6DD5B (ADVAPI32.CryptEncrypt)
```



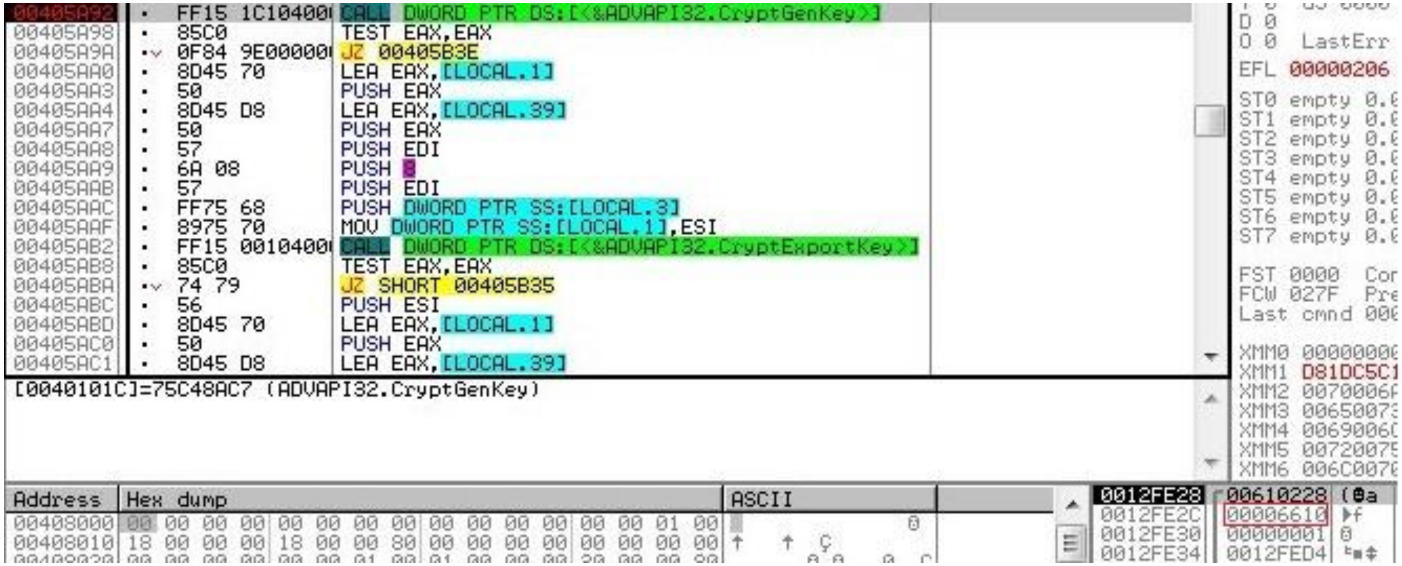
```
Address  Hex dump                                         ASCII
00618AF8 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 -----BEGIN RSA P
00618B08 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0D RIVATE KEY-----♪
00618B18 0A 42 77 49 41 41 41 43 6B 41 41 42 53 55 30 45 ◙BwIAAACkAABSU0E
00618B28 79 41 41 51 41 41 41 45 41 41 51 42 52 41 66 33 yAAQAAAEAAQBRAf3
00618B38 4A 47 39 6F 47 7A 76 77 4F 69 49 71 7A 4C 78 72 JG9oGzvwOiIqzLxr
00618B48 67 68 71 38 30 53 6B 61 4C 44 39 46 46 6E 54 39 ghq80SkaLD9FFnT9
00618B58 59 0D 0A 2B 46 6C 63 59 2B 54 6B 35 4D 65 48 51 Y♪◙+FlcY+Tk5MeHQ
00618B68 69 6C 4F 54 6F 37 4C 30 47 39 54 31 57 43 41 67 ilOTo7L0G9T1WCAg
00618B78 6D 41 64 6B 55 62 4A 2B 54 2B 6A 44 65 74 4D 47 mAdkUbJ+T+jDetMG
00618B88 56 2F 73 6E 52 31 30 73 32 33 6D 4D 73 6B 4F 30 V/snR10s23mMskO0
00618B98 71 54 67 0D 0A 64 37 79 53 39 58 49 33 4C 4F 41 qTg♪◙d7yS9XI3LOA
00618BA8 4E 7A 6F 70 45 37 4B 6A 6B 62 67 42 37 66 57 78 NzopE7KjkbgB7fWx
00618BB8 63 31 69 76 62 52 4D 75 75 68 45 31 37 4A 64 69 c1ivbRMuuhE17Jdi
00618BC8 30 73 2F 4B 30 42 48 73 39 30 45 6F 4B 74 75 56 0s/K0BHs90EoKtuV
00618BD8 43 7A 38 65 41 0D 0A 6F 6B 51 51 30 52 65 35 48 Cz8eA♪◙okQQ0Re5H
00618BE8 6F 45 43 79 53 76 6B 6D 43 31 50 67 5A 4B 64 67 oECySvkmC1PgZKdg
00618BF8 2F 38 61 58 34 7A 76 2B 76 73 45 37 4A 7A 43 4F /8aX4zv+vsE7JzCO
00618C08 77 73 6A 72 5A 36 53 43 2F 4F 6A 74 67 2F 72 4F wsjrZ6SC/Ojtg/rO
00618C18 76 66 2F 44 74 47 4A 0D 0A 33 4F 42 37 42 2B 6D vf/DtGJ♪◙3OB7B+m
```

```
0012FE24  00605DA8  ¿]'
0012FE28  00000000
0012FE2C  00000000
0012FE30  00000000
0012FE34  00618AF8  °èa   ASCII
0012FE38  0012FED8  ╤■‡
0012FE3C  000003C0  └♥
0012FE40  006191D0  ╨æa   UNICO
0012FE44  00618AF8  °èa   ASCII
0012FE48  005FE748  Hτ_   UNICO
0012FE4C  19E61035  5►µ↓
0012FE50  D9F95F2D  -_·┘
0012FE54  4A1C4826  &H∟J
0012FE58  FE5B277C  |'[■
0012FE5C  CCA36811  ◄hú╠
0012FE60  4F6C5D28  (]lO
0012FE64  D4D290DE  ▐Éπ╘
0012FE68  3EF5D682  éπJ>
0012FE6C  60D21111  ◄◄π'
0012FE70  8976CA1E  ▲╩vë
0012FE74  DA7337F5  J7s┌
```

- The encrypted content is stored in the ransom note, which will be uploaded to the attacker's website in order to make the payment

Spora ransomware

- For every file a new AES key is generated, it is encrypted using the generated RSA public key and stored at the end of every encrypted file:



```
00405A92  .   FF15 1C10400 CALL DWORD PTR DS:[<&ADVAPI32.CryptGenKey>]
00405A98  .   85C0         TEST EAX,EAX
00405A9A  .v  0F84 9E00000 JZ 00405B3E
00405AA0  .   8D45 70      LEA EAX,[LOCAL.1]
00405AA3  .   50           PUSH EAX
00405AA4  .   8D45 D8      LEA EAX,[LOCAL.39]
00405AA7  .   50           PUSH EAX
00405AA8  .   57           PUSH EDI
00405AA9  .   6A 08        PUSH 8
00405AAB  .   57           PUSH EDI
00405AAC  .   FF75 68      PUSH DWORD PTR SS:[LOCAL.3]
00405AAF  .   8975 70      MOV DWORD PTR SS:[LOCAL.1],ESI
00405AB2  .   FF15 0010400 CALL DWORD PTR DS:[<&ADVAPI32.CryptExportKey>]
00405AB8  .   85C0         TEST EAX,EAX
00405ABA  .v  74 79        JZ SHORT 00405B35
00405ABC  .   56           PUSH ESI
00405ABD  .   8D45 70      LEA EAX,[LOCAL.1]
00405AC0  .   50           PUSH EAX
00405AC1  .   8D45 D8      LEA EAX,[LOCAL.39]
[0040101C]=75C48AC7 (ADVAPI32.CryptGenKey)
```

```
D 0
O 0  LastErr
EFL 00000206
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000  Cor
FCW 027F  Pre
Last cmnd 000
XMM0 0000000
XMM1 D81DC5C1
XMM2 0070006
XMM3 0065007
XMM4 0069006
XMM5 0072007
XMM6 006C007
```

```
Address  Hex dump                                          ASCII
00408000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00
00408010 18 00 00 00 18 00 00 80 00 00 00 00 00 00 00 00
```

```
0012FE28  00610228  (@a
0012FE2C  00006610  ▸f
0012FE30  00000001  
0012FE34  0012FED4  
```

- Like before, 0x610228 is a handle to a CSP, 0x6610 represents Alg_ID: CALG_AES_256
- A ransom note is created in every directory and needs to be uploaded to the website which is given; it is in russian language (it is important to mention, the malware checks if the language identifier is 0x419 (ru), if it is, the samples exits)

Spora ransomware

- Let's summarize the encryption process:

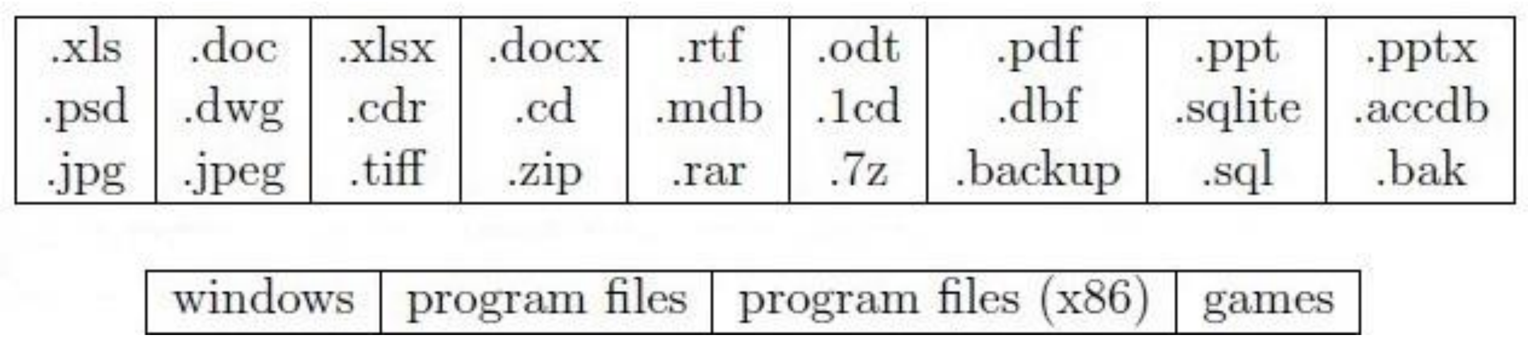
1. The malware has a hardcoded AES256 key, let's call it key1, it is used to decrypt another key.
2. A RSA2048 key is decrypted, let's call it key2.
3. A new pair of RSA1024 keys is generated, let's call them key3P(public) and key3p(private).
4. An unique AES256 key is generated, let's call it key4. It is used to encrypt key3p, it is encrypted with key2 and stored in the ransom note.
5. For every file a new AES256 key is generated, let's call it key5 (the file is encrypted using key5). key5 is finally encrypted with key3P and stored at the end of every file.

- Decryption process:

1. The victim uploads the ransom note to the website, so the attacker is able to decrypt key4 using his private RSA key.
2. The key4 is used to decrypt key3p (RSA private key)
3. The key3p is used to decrypt every key5 which was generated for every file.
4. The key5 is used to decrypt each file individually.

Spora ransomware

- There are some extensions which are attacked by the malware and some folders which are excluded because the system must remain functional to make the payment



.xls	.doc	.xlsx	.docx	.rtf	.odt	.pdf	.ppt	.pptx
.psd	.dwg	.cdr	.cd	.mdb	.1cd	.dbf	.sqlite	.accdb
.jpg	.jpeg	.tiff	.zip	.rar	.7z	.backup	.sql	.bak

windows	program files	program files (x86)	games

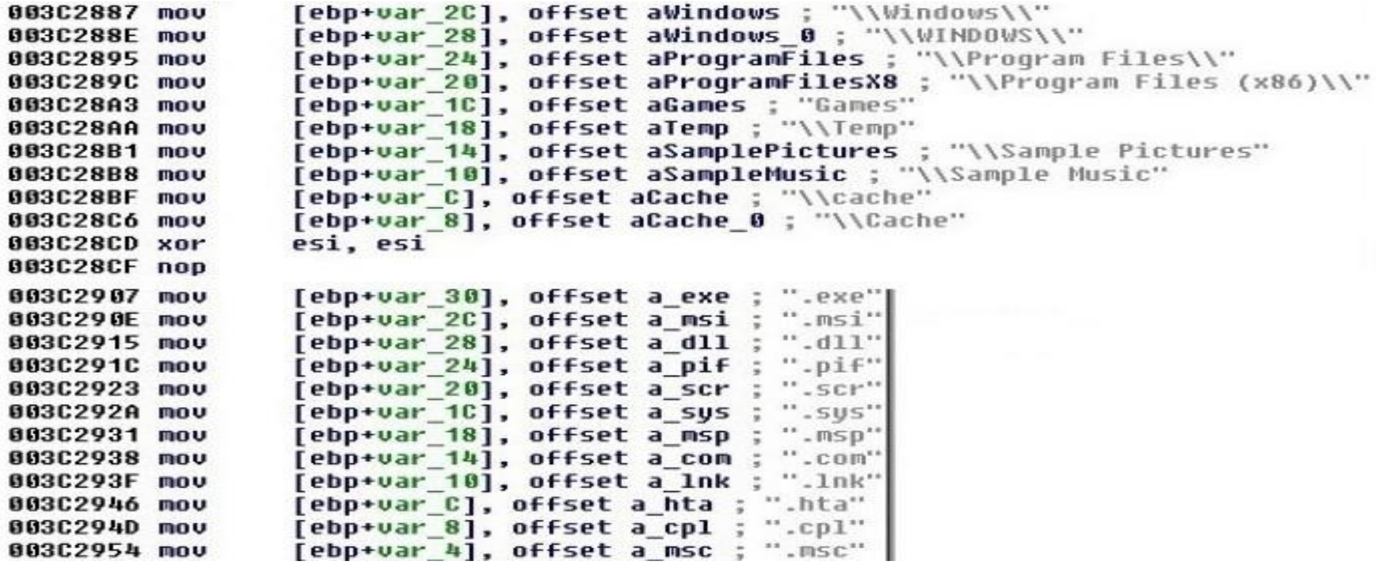
- No decryptor available so far, the encryption process seems to be consistent. It is probably the most complex encryption process for a ransomware so far

DMA Locker 3.0 ransomware

- It encrypts files offline like Spora or Cerber (it doesn’t communicate with a C&C)
- RSA 1024 + AES 256 encryption using Windows APIs (**CryptImportKey**, **CryptGenRandom**, **CryptEncrypt**)
- Like Spora, the sample has a hardcoded RSA key which is used to encrypt AES 256 keys that are generated for each individual file
- It uses VSSadmin to delete shadow copies, logical disks and network shares are attacked

DMA Locker 3.0 ransomware

- DMA Locker doesn't attack files that have the following extensions, as well as some folders are excluded from the encryption process



```
003C2887 mov     [ebp+var_2C], offset aWindows ; "\\Windows\\"
003C288E mov     [ebp+var_28], offset aWindows_0 ; "\\WINDOWS\\"
003C2895 mov     [ebp+var_24], offset aProgramFiles ; "\\Program Files\\"
003C289C mov     [ebp+var_20], offset aProgramFilesX8 ; "\\Program Files (x86)\\"
003C28A3 mov     [ebp+var_1C], offset aGames ; "Games"
003C28AA mov     [ebp+var_18], offset aTemp ; "\\Temp"
003C28B1 mov     [ebp+var_14], offset aSamplePictures ; "\\Sample Pictures"
003C28B8 mov     [ebp+var_10], offset aSampleMusic ; "\\Sample Music"
003C28BF mov     [ebp+var_C], offset aCache ; "\\cache"
003C28C6 mov     [ebp+var_8], offset aCache_0 ; "\\Cache"
003C28CD xor     esi, esi
003C28CF nop
003C2907 mov     [ebp+var_30], offset a_exe ; ".exe"
003C290E mov     [ebp+var_2C], offset a_msi ; ".msi"
003C2915 mov     [ebp+var_28], offset a_dll ; ".dll"
003C291C mov     [ebp+var_24], offset a_pif ; ".pif"
003C2923 mov     [ebp+var_20], offset a_scr ; ".scr"
003C292A mov     [ebp+var_1C], offset a_sys ; ".sys"
003C2931 mov     [ebp+var_18], offset a_msp ; ".msp"
003C2938 mov     [ebp+var_14], offset a_com ; ".com"
003C293F mov     [ebp+var_10], offset a_lnk ; ".lnk"
003C2946 mov     [ebp+var_C], offset a_hta ; ".hta"
003C294D mov     [ebp+var_8], offset a_cpl ; ".cpl"
003C2954 mov     [ebp+var_4], offset a_msc ; ".msc"
```

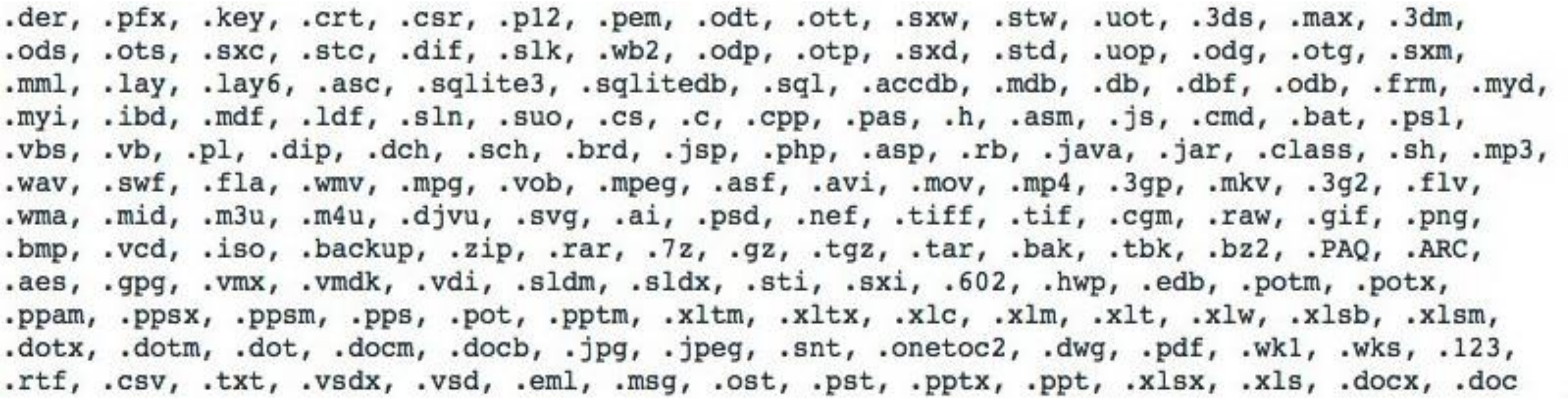
- The encrypted file has the following structure: "!Encrypt!##" + (Encrypted AES key with RSA hardcoded key) + (Encrypted original content using AES key)
- A method of prevention: the presence of **start.txt** and **cryptinfo.txt** in ProgramData directory, the malware checks for them and doesn't encrypt the files (the malware drops the files when the encryption finishes, so it doesn't encrypt the files again)
- No decryptor available for this version, there are some decryptors for some older versions of DMA Locker (the encryption process is different there)

WannaCry ransomware

- Over 230.000 computers in over 150 countries were infected
- Two components: Worm + Ransomware
- The worm is looking for vulnerable SMB (Server Message Block) ports, it uses EternalBlue exploit to get on the network and DoublePulsar exploit to establish persistence and install WannaCry
- It can propagate to other vulnerable machines in the same network
- The Windows vulnerability wasn’t a 0-day exploit, because Microsoft released a security patch in March 2017
- It is possible that North Korean group Lazarus to be behind the attack, because of some similarities between the WannaCry’s code and a backdoor’s code by Lazarus

WannaCry ransomware

- Initially, the malware is trying to connect to www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, if it succeeds, the malware exits.
- RSA 2048 + AES 128 with null initialization vector is used
- The ransomware appends .wncry extension to every encrypted file and attacks the following extensions



```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm,
.ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm,
.mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .db, .dbf, .odb, .frm, .myd,
.myi, .ibd, .mdf, .ldf, .sln, .suo, .cs, .c, .cpp, .pas, .h, .asm, .js, .cmd, .bat, .ps1,
.vbs, .vb, .pl, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .rb, .java, .jar, .class, .sh, .mp3,
.wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv,
.wma, .mid, .m3u, .m4u, .djvu, .svg, .ai, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png,
.bmp, .vcd, .iso, .backup, .zip, .rar, .7z, .gz, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC,
.aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .edb, .potm, .potx,
.ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm,
.dotx, .dotm, .dot, .docm, .docb, .jpg, .jpeg, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123,
.rtf, .csv, .txt, .vsdx, .vsd, .eml, .msg, .ost, .pst, .pptx, .ppt, .xlsx, .xls, .docx, .doc
```

- There are some decryptors for WannaCry, but work only for Windows XP and Windows 7. The RSA key is somehow recovered from the memory, because **CryptReleaseContext** doesn't clean memory

Conclusions

Strategies to avoid loss of data:

- Backup and validate those backups regularly
- Update and patch the software
- The macros in Microsoft Word, Excel, etc. must be disabled
- Rename vssadmin.exe (the ransomware can’t use it to delete shadow copies)
- Best antivirus protection or use www.virustotal.com to scan with multiple antiviruses a suspected file
- Be informed about security events, especially malware ones

Questions?