Malware Triage

IOCs

Workshop

Using Open Data to Help Develop Robust Indicators

Hello, My Name is:

Sergei Frankoff

sergei@openanalysis.net

Sean Wilson

sean@openanalysis.net

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.

WORKSHOP PREP

This is a hands on workshop and you will need the following:

- Computer (preferably a VM) that you can use to analyze malware
- The Internet
- Python and pip installed
- Text editor
- Recommended tools
- Instructions are in your workbook!

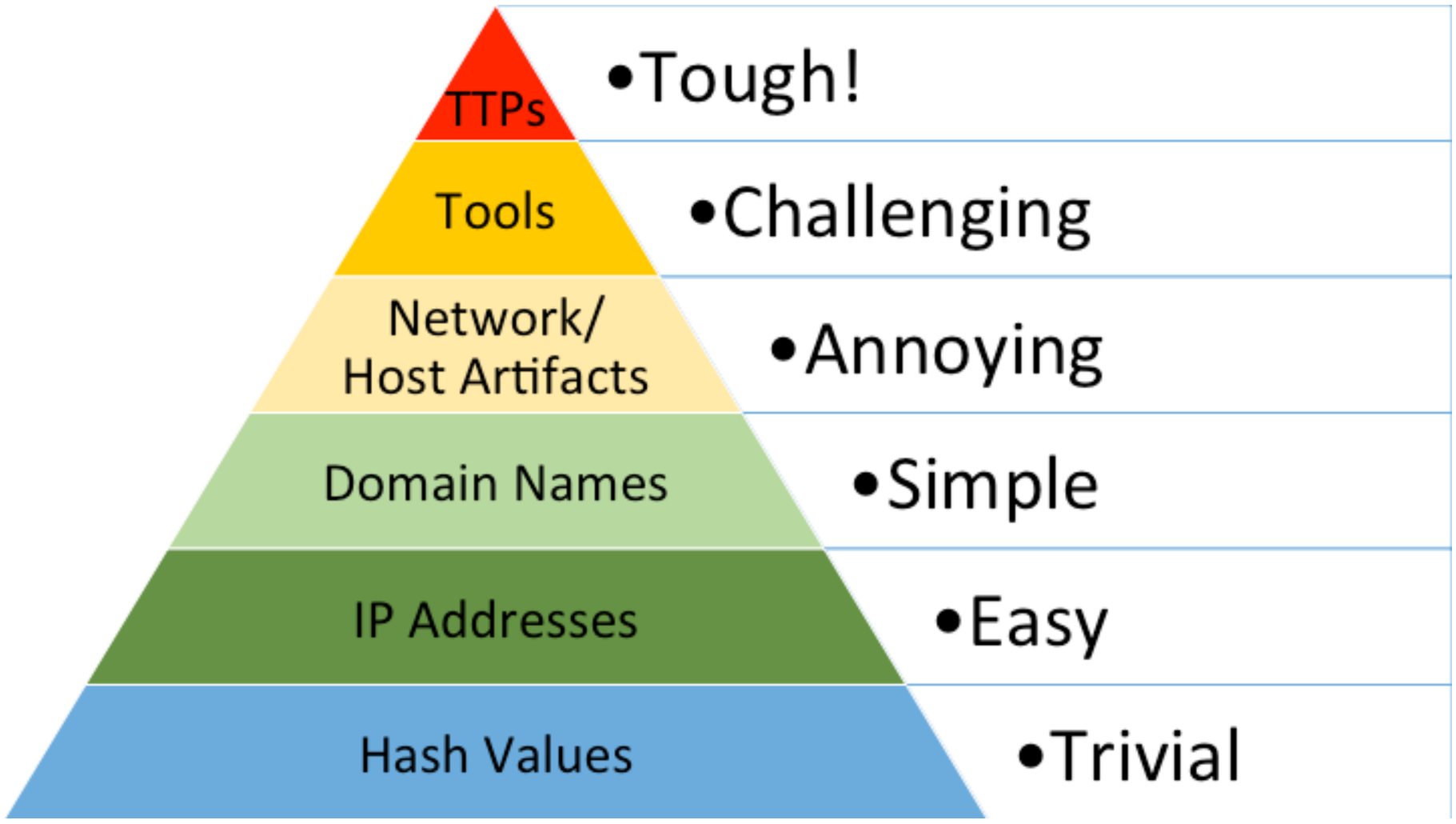
What is an IOC

Indicators of Compromise (IOCs) *are forensic artifacts of an intrusion that can be identified on a host or network.*

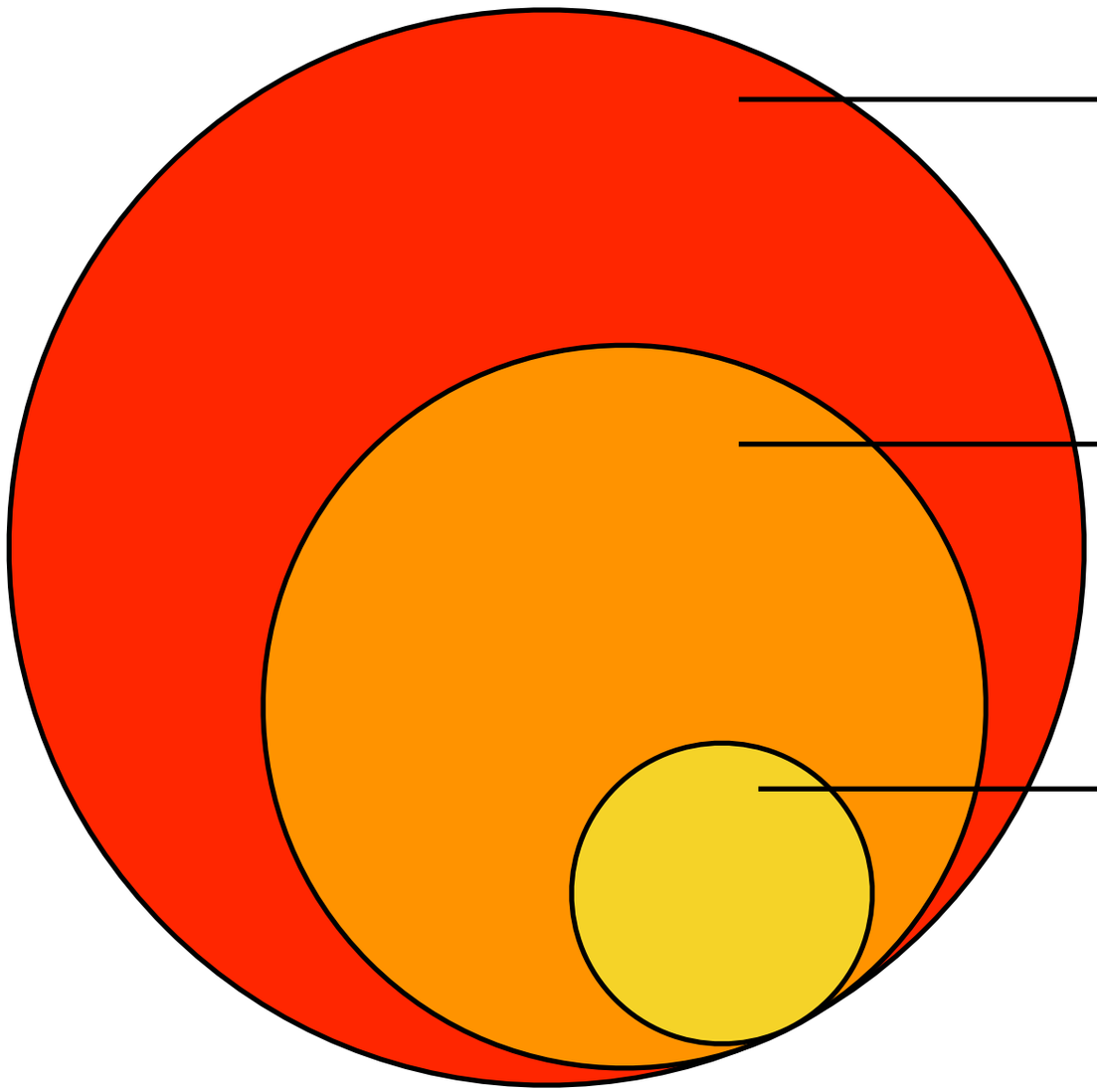
opinioc.org

(http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf)

Traditional View: Pyramid of Pain



Malware Specific IOCs



IOCs:
Indicators of Compromise.

Malware Specific IOCs:
forensic artifacts resulting from the presence or execution of malware.

AV Signatures

The Problem With AV

Artemis!1A5E05B1B9E1

Artemis!262BC0AE2FB0

Artemis!04296F13925B

Artemis!110C43F8A337

Artemis!9BFC61456261

Artemis!9BE792AC4667

The Problem With AV

👎 Small teams rely on host and network AV for information about threats.

👎Good coverage but poor fidelity; signatures are often generic and don’t provide much information.

👎Can’t be used to make automated decisions.

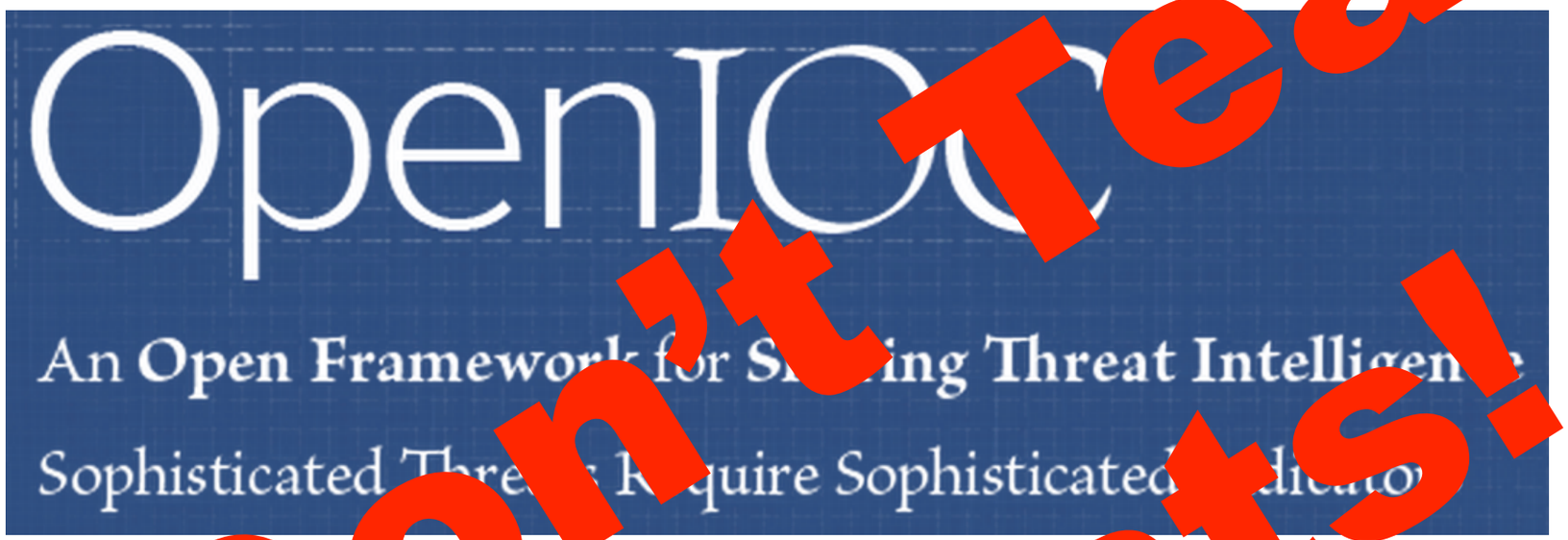
Alternative: Build Your Own IOCs

👍 You control the fidelity (or can verify it in the case of shared IOCs).

👍 You are already creating them as the output from your Triage/IR process. Good ROI for your SOC.

👍 Can be trusted (and validated) for automated decisions.

IOC Formats



VS.

We Don't Teach Formats!

IOC Format Basics

VS.

OpenIOC Basics

Core Strengths

- Perfect for describing malware families or threat actors. Good for sharing.
- Covers multiple aspects of malware in one description (network, host, file).
- Good for describing the **effect** that malware has on its environment.

Weaknesses

- Require environment data collection to fully leverage IOC
- Requires “heavy” tooling for automation (ex. Redline).

OpenIOC Basics

- Or
  - Process Handle Name contains Global\msiff0x1
  - File MD5 contains 4165a7df15dc05feae07dc2ecc7b9829
  - And
    - File Strings contains Global\msiff0x1
    - File Strings contains Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
    - File Strings contains 30f5877bda910f27840f2e21461723f1
  - And
    - Network String URI contains last.so
    - Network String HTTP Referr contains https://www.bing.com/
    - Or
      - Network DNS contains dxqaz6k85i.ru
      - Port Remote IP contains 185.103.252.64

Yara Basics

Core Strengths

- Perfect for identifying malware files that belong to the same developer (family).
- Good for describing specific characteristics in a malware **file**.
- Easy to start automation with “light” tooling.

Weaknesses

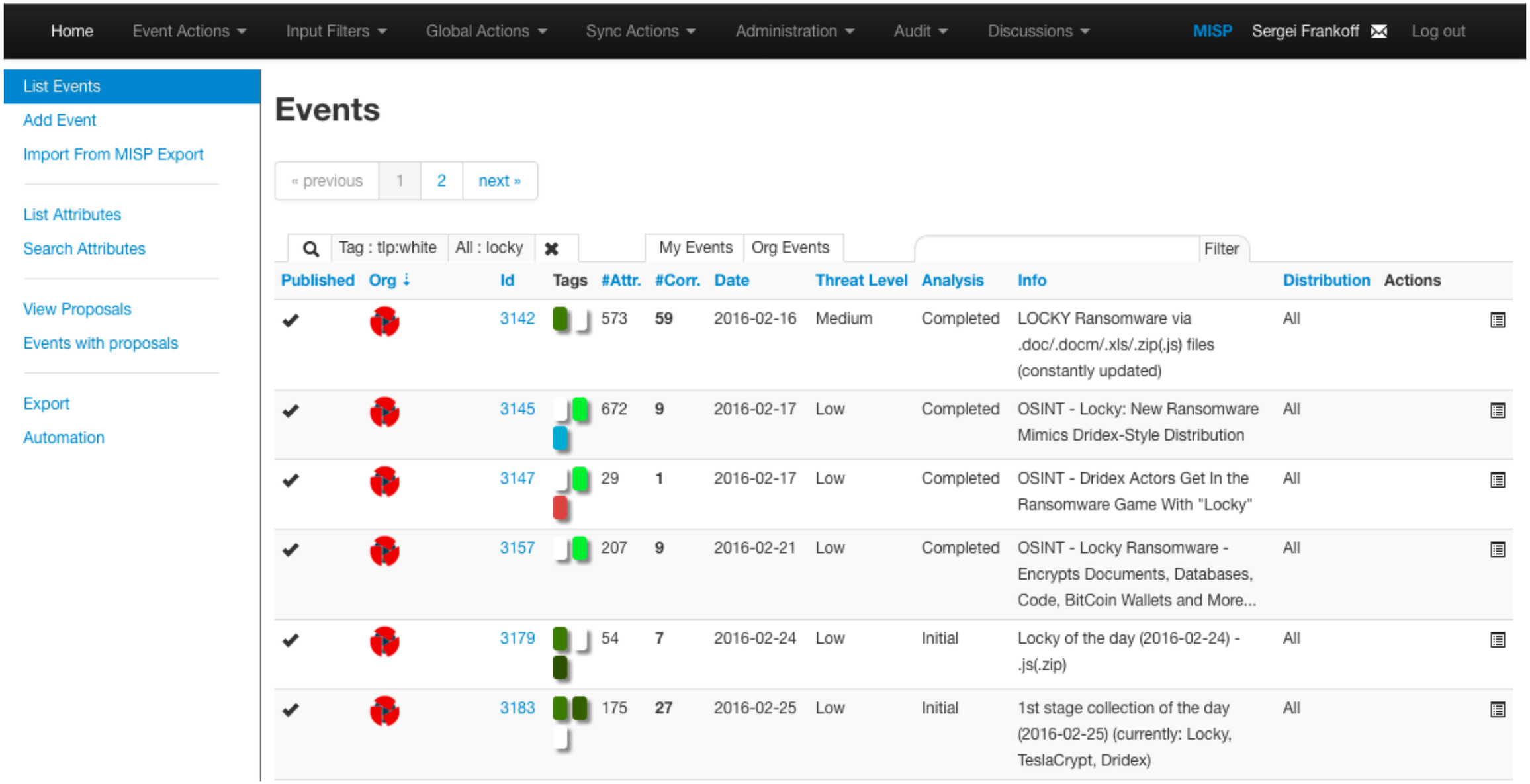
- Limited to describing files only (no network or environment).
- Can be run against memory dumps for dynamic signatures but generally limited to static artifacts.

Yara Basics

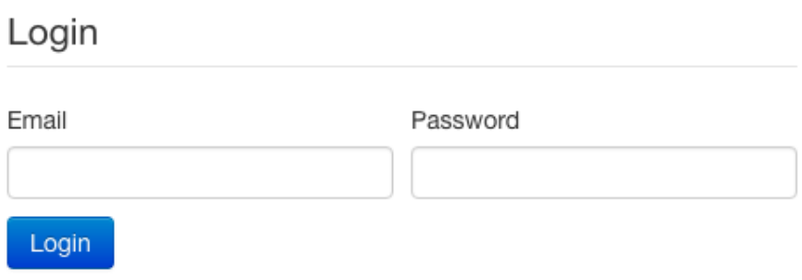
```
rule Andromeda
{
    meta:
        author = "@herrcore"
        Description = "Andromeda dropper"
        maltype = "Malware dropper"
        filetype = "PE"

    strings:
        $a1 = "Referer: https://www.bing.com/"
        $a2 = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
        $a3 = "/last.so"
        $a4 = "30f5877bda910f27840f2e21461723f1"
        $a5 = "Global\msiff0x1


    condition:
    $a5 or ($a1 and $a2 and $a3 and $a4) or ($a2 and $a4)
}
```

Storing | Consuming | Sharing MISP

MISP: Example



CIRCL MISP
Getting Access

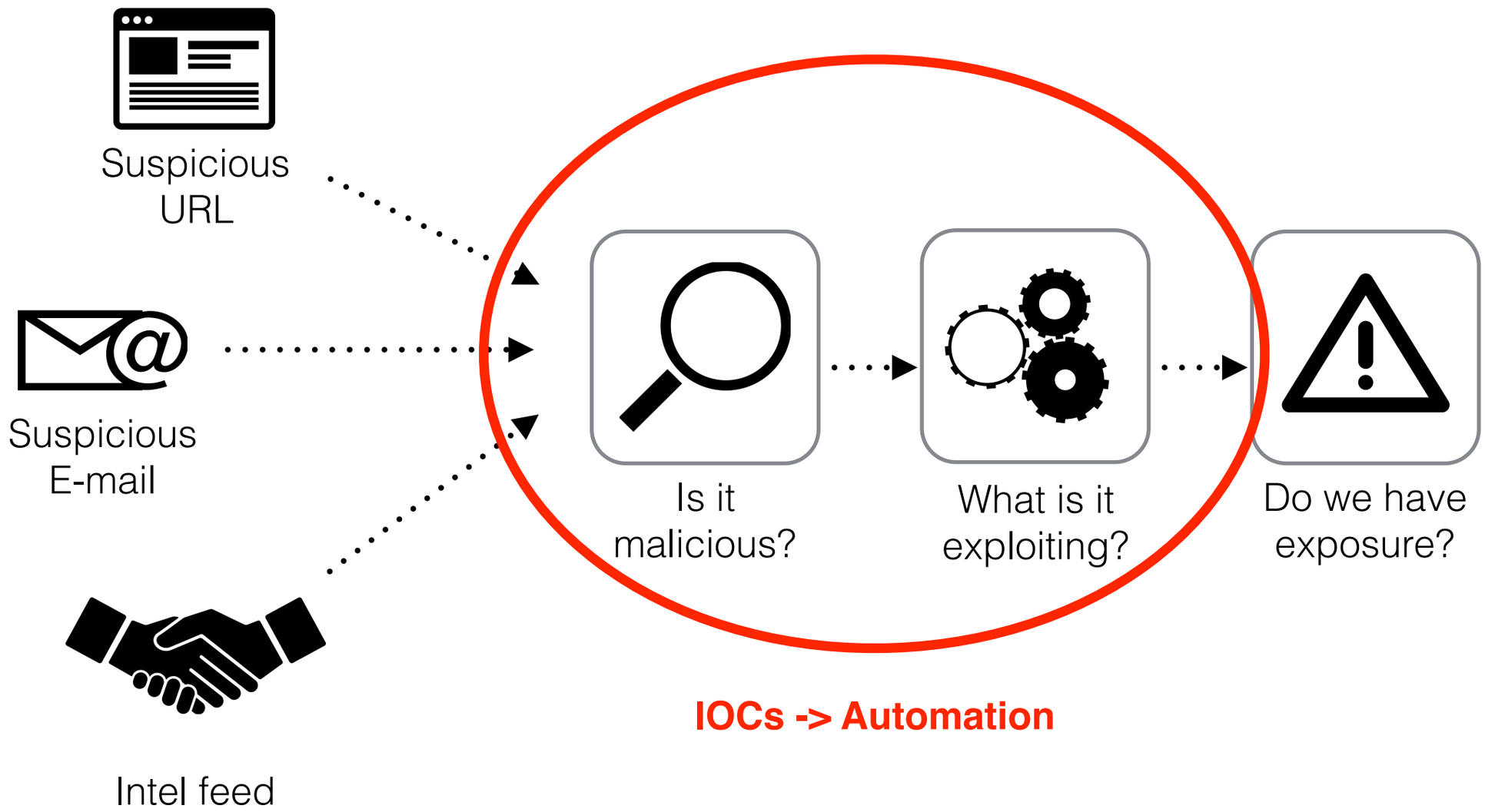


Using IOCs…

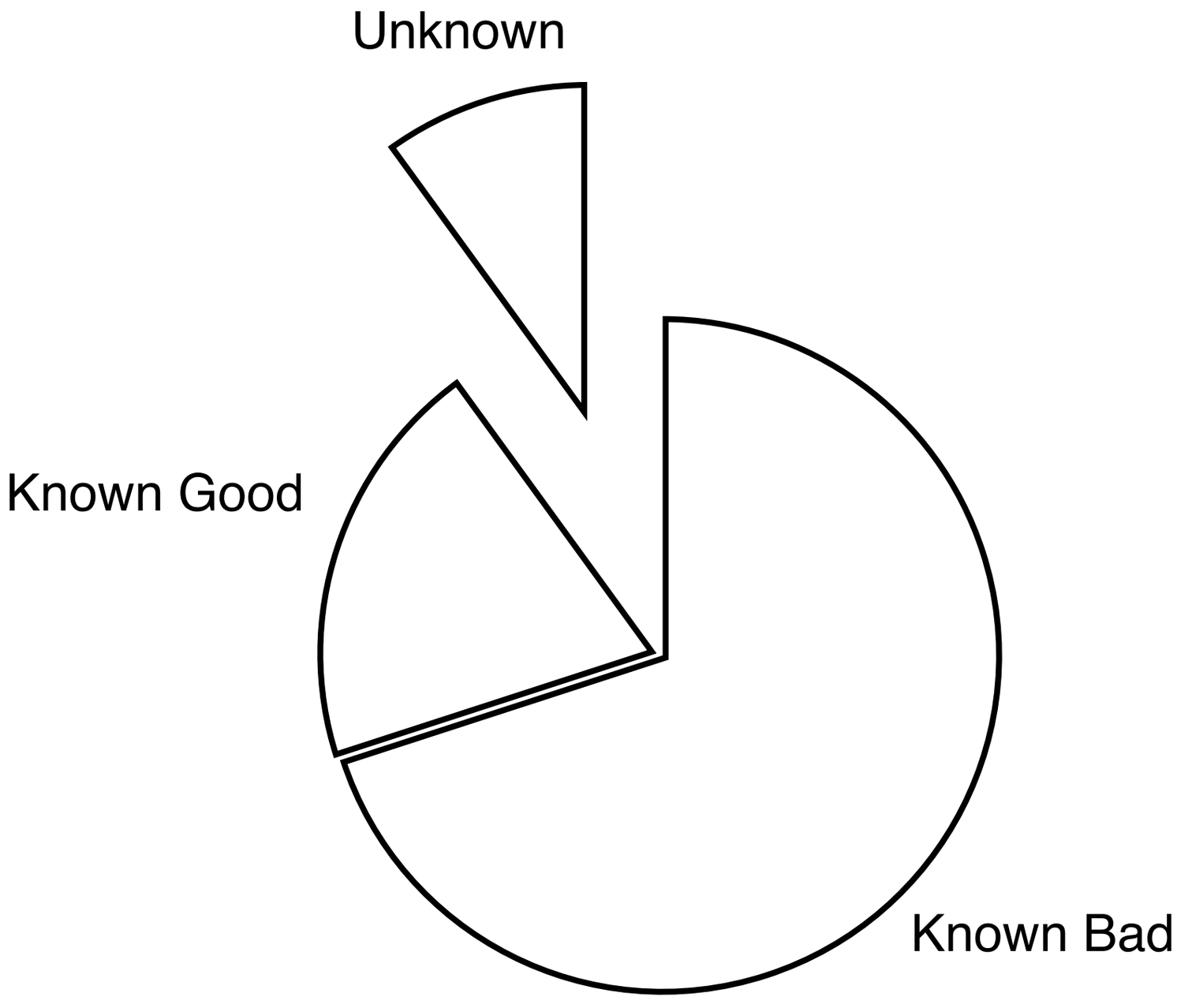
- As part of your hunting strategy
- As part of your triage process
- As a researcher to sort samples
- Sharing…
- AUTOMATION!

Hunting With IOCs

Malware Triage Automation With IOCs



IOCs Remove The Knowns And Reveal The Unknown



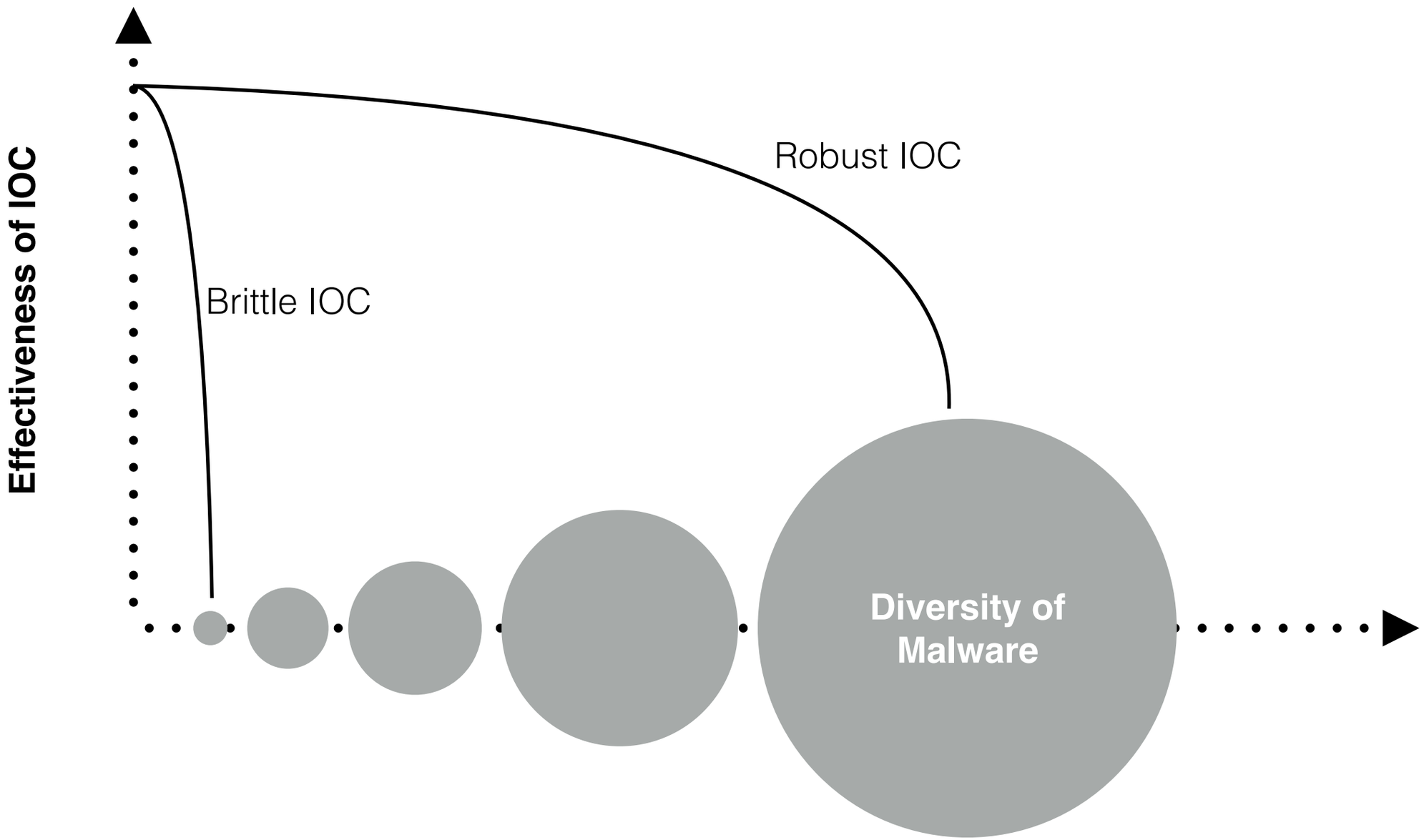
Not All IOCs Are Equal

- Are they resilient to change? Think “pyramid of pain”.

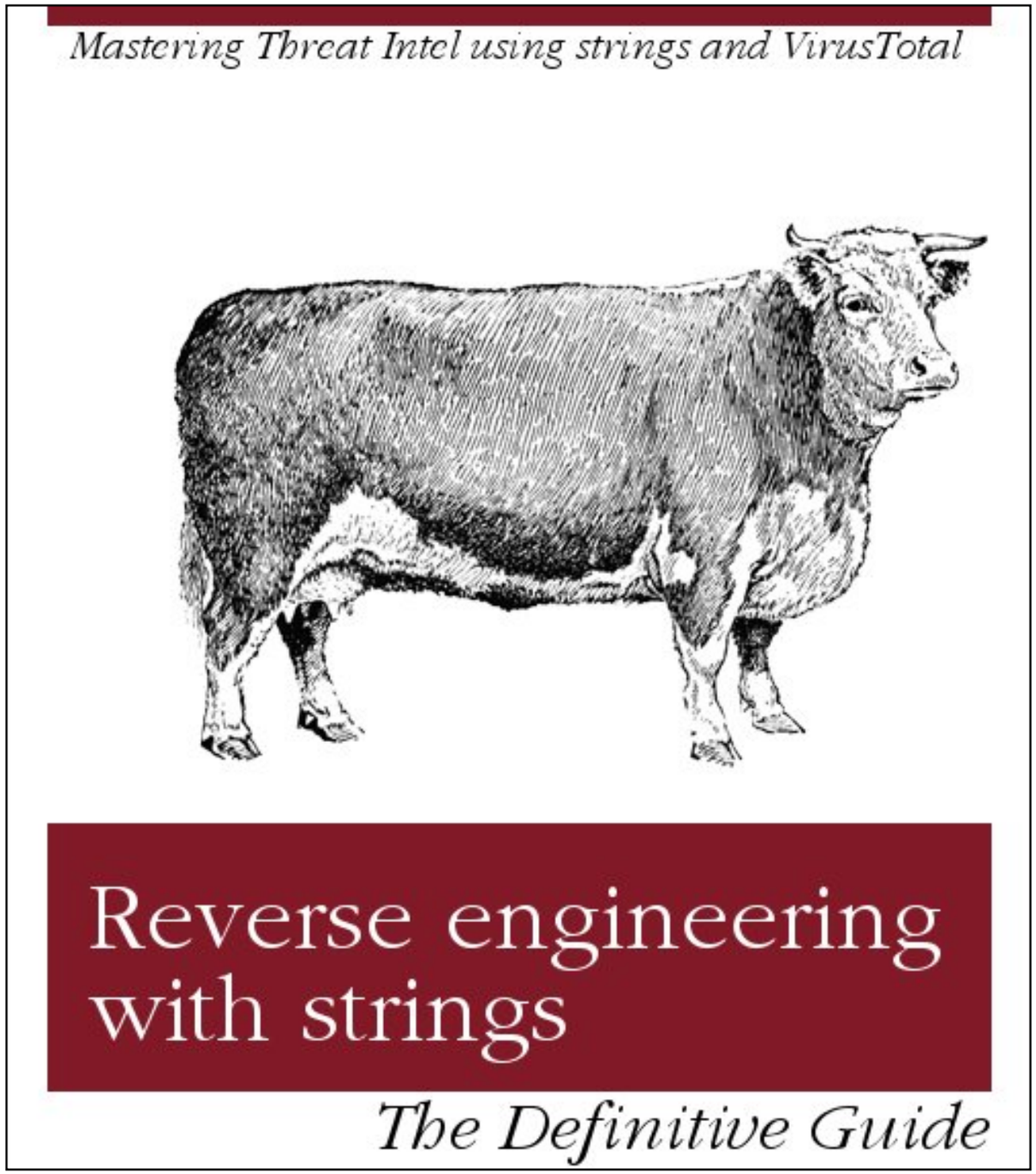
- Are they too generic? Possible misidentification or false positives?

- The best IOCs are ones that will continue to identify a family of malware regardless of small changes and diversification over its lifetime. We call these **ROBUST IOCs**!

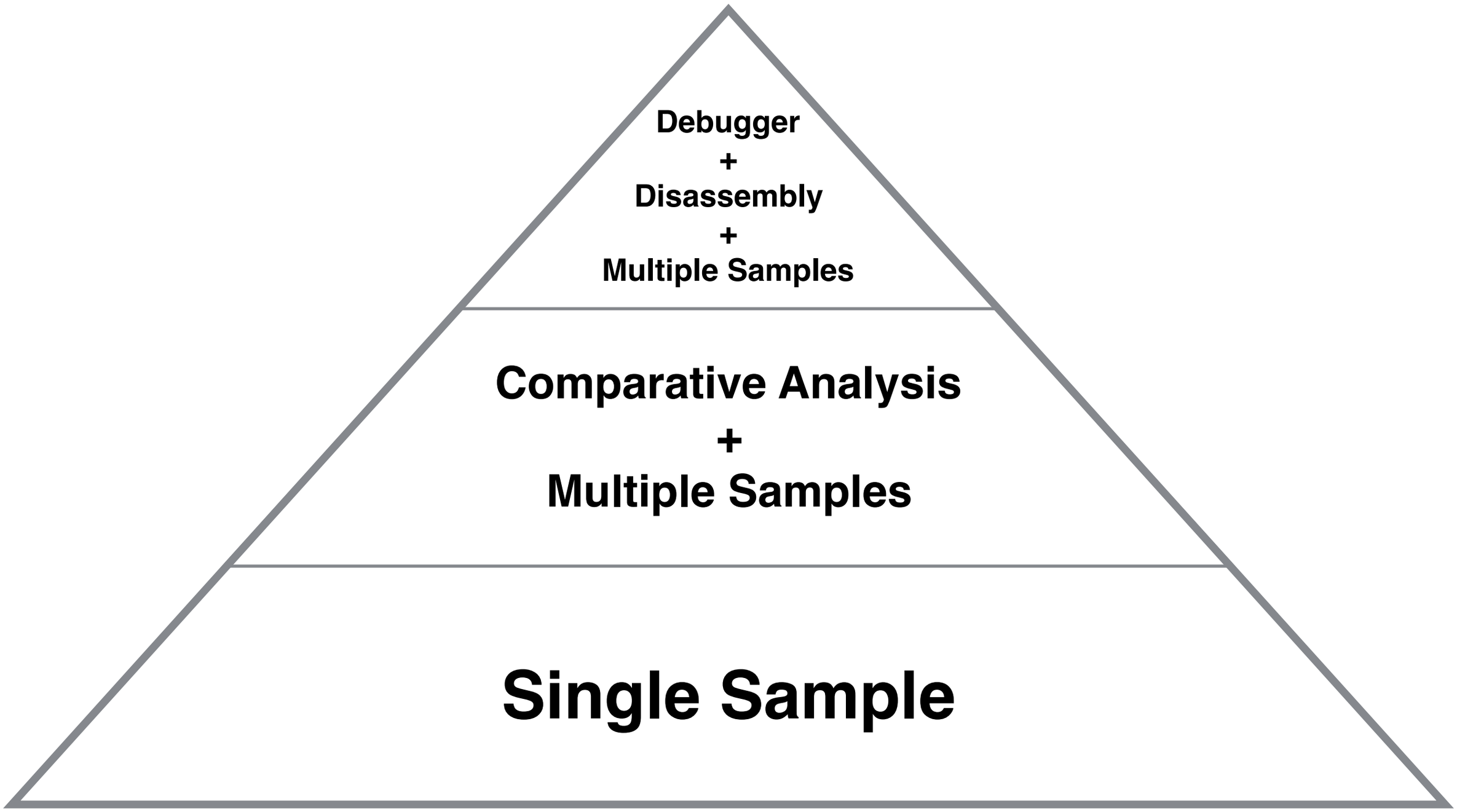
Robust IOCs


Effectiveness of IOC
Robust IOC
Brittle IOC
Diversity of Malware
Lifetime of Malware Family

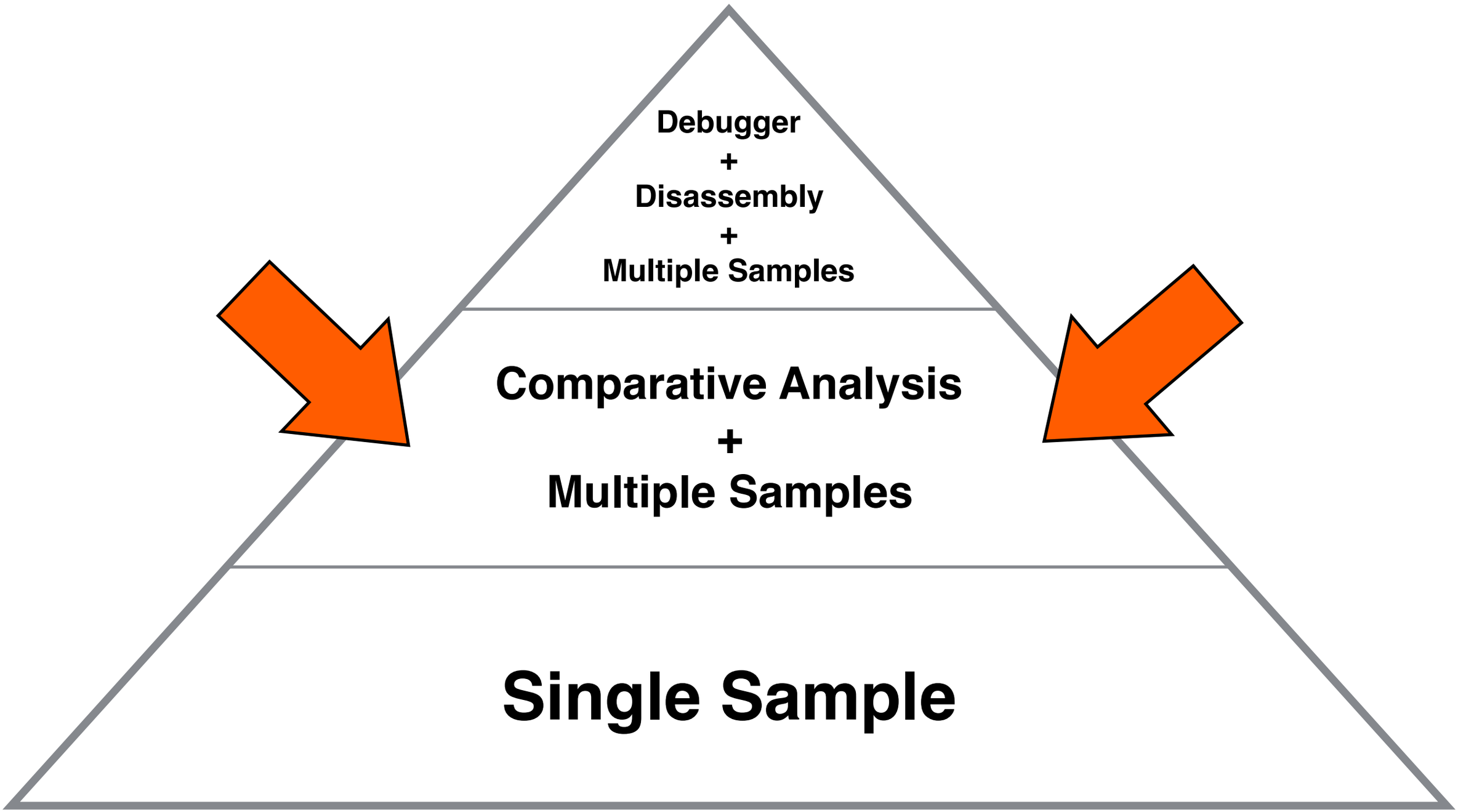
Robust Is Not...



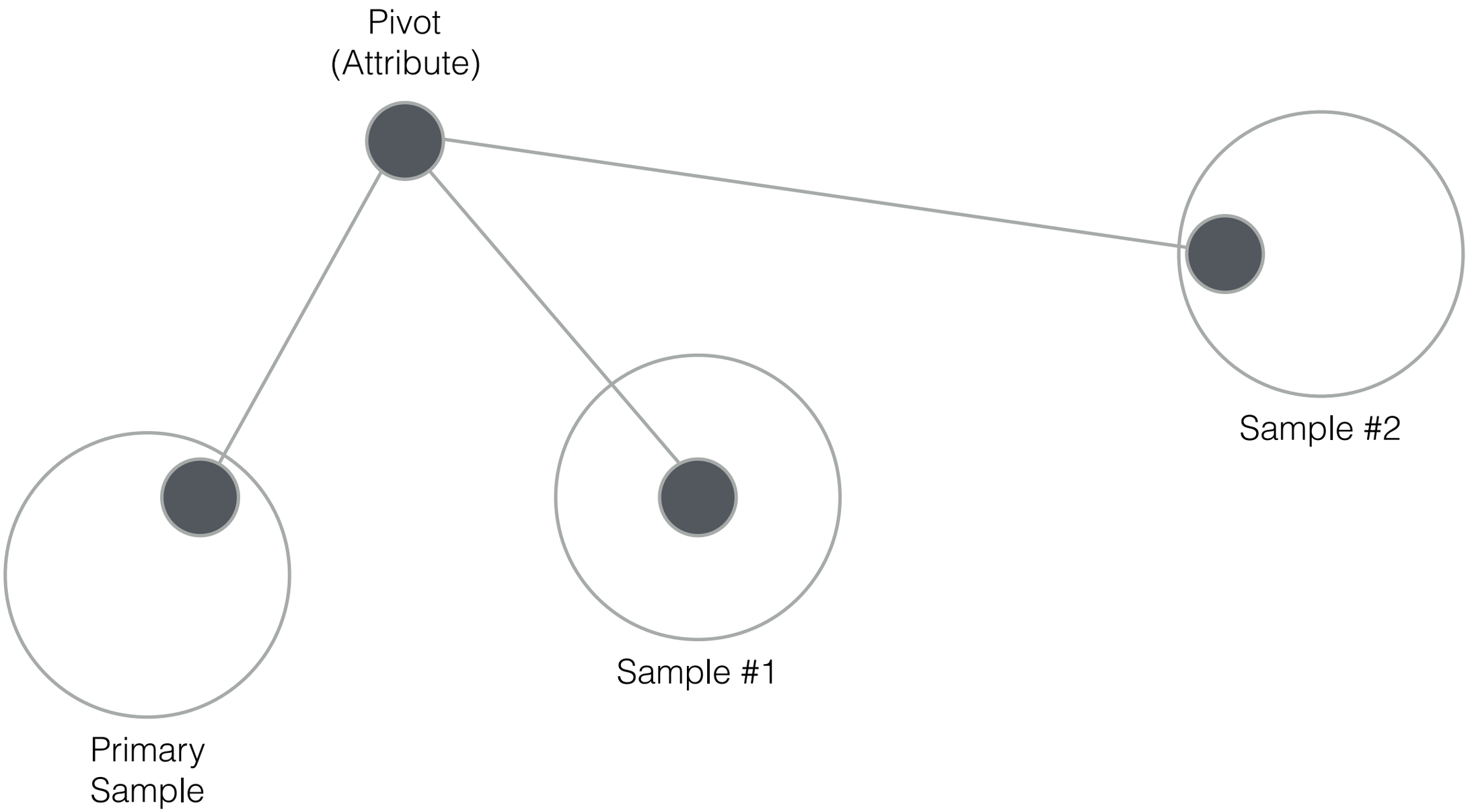
Approaches for Developing Robustness



This Workshop: Robustness Level



Comparative Analysis



Mining Open Data

PASSIVETOTAL

OPEN THREAT EXCHANGE

{{ \\ YaraRules ... }}

malwr

virusshare.com

#totalhash

BROWSE HELP API / MALTEGO CONTACT

A search engine for threats

Search

THREATCONNECT

IOC Bucket

virustotal

Binarly

PAYLOAD SECURITY

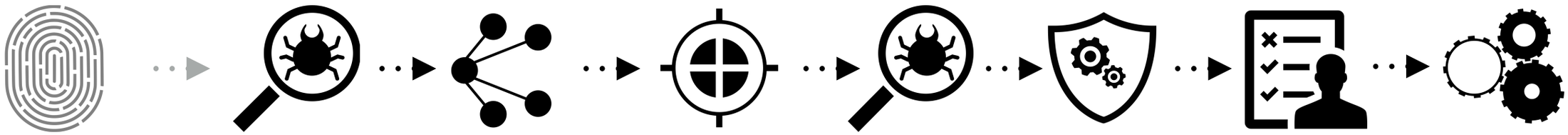
ThreatMiner

Data Mining for Threat Intelligence

OPSEC Warning!

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

Building Robust Indicators



Identification (Primary sample)

Analysis (Triage)

Develop Primary IOC (Pivots)

Discovery (Hunting)

Analysis (Triage)

Develop IOC

Test (Validate)

Automation …

The Scenario

CloudScan 2.0

OnAccess Threat Detection

Threat: KraftDinner.Generic
File: C:\Users\Bob\AppData\Local\Temp\~a0ow02
Status: Quarantined

CloudScan has successfully protected your computer

Identification

What type of file is it

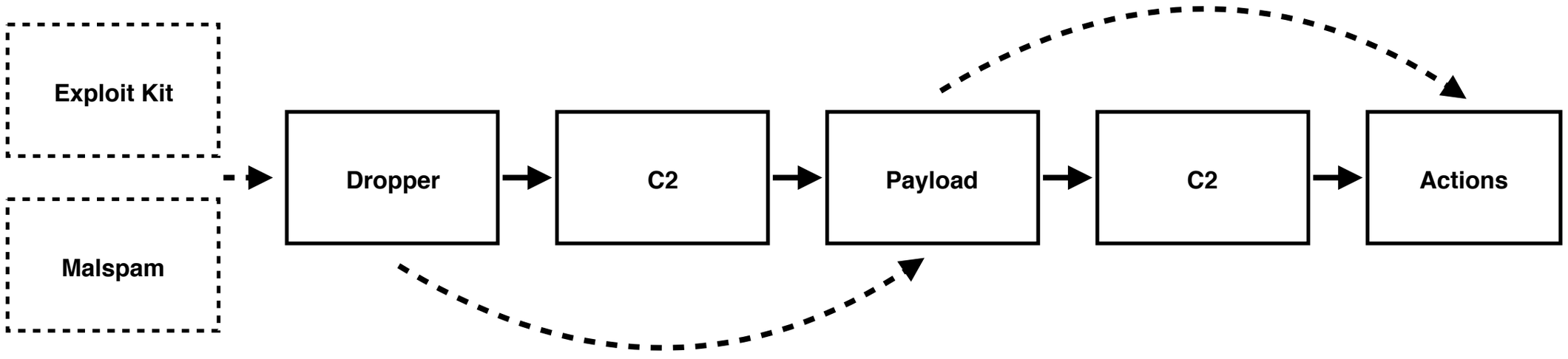
What attributes are relevant to the file

How do we analyze the file

Placing The Initial Sample In Context

Lockheed Martin Intrusion Kill Chain

Typical Crimeware Lifecycle



Common File Types

	Exploit Kit	Malspam	Dropper	Payload
Web	· HTML · Javascript · Flash · Java Applet			
Document		· Document (.doc .docx .rtf) · Powerpoint · Excel		
Interpreted / Bytecode			· Java · .NET · *batch	· Java · .NET · *powershell
Executable			· PE	· PE

Documents

Details:
Word | PowerPoint | Excel (old format): OLE container
Word | PowerPoint | Excel (new format): Zip
Rich Text Format (RTF): OLE container

Common extensions:
Word | PowerPoint | Excel (old format): .doc .ppt .xls
Word | PowerPoint | Excel (new format): .docm .pptm .xlsm
Rich Text Format (RTF): .rtf

Magic Bytes:
Word | PowerPoint | Excel (old format): D0 CF 11 E0 A1 B1 1A E1
Word | PowerPoint | Excel (new format): 50 4B 03 04 [PK]
Rich Text Format (RTF): 7B 5C 72 74 66 31 [{ tf1]

Documents:
Legacy Format

```
├── 1Table
├── Macros
│   ├── PROJECT
│   ├── PROJECTwm
│   └── VBA
│       ├── ThisDocument
│       ├── _VBA_PROJECT
│       ├── __SRP_0
│       ├── __SRP_1
│       ├── __SRP_2
│       ├── __SRP_3
│       └── dir
├── WordDocument
├── [1]CompObj
├── [5]DocumentSummaryInformation
└── [5]SummaryInformation
```

Documents: OOXML

```
.
├── [Content_Types].xml
├── _rels
├── customXml
|   ├── _rels
|   |   └── item1.xml.rels
|   ├── item1.xml
|   └── itemProps1.xml
├── docProps
|   ├── app.xml
|   ├── core.xml
|   └── thumbnail.jpeg
└── word
    ├── _rels
    |   ├── document.xml.rels
    |   └── vbaProject.bin.rels
    ├── document.xml
    ├── fontTable.xml
    ├── settings.xml
    ├── styles.xml
    ├── theme
    |   └── theme1.xml
    ├── vbaData.xml
    ├── vbaProject.bin
    └── webSettings.xml
```

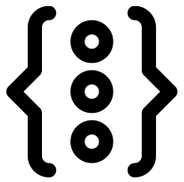
Contained files

This file is a compressed stream containing 15 files.

[+] word/vbaProject.bin	Microsoft Office	38400 Bytes	✖
[+] word/document.xml	XML	1517 Bytes	?
[+] word/vbaData.xml	XML	1442 Bytes	?
[+] word/settings.xml	XML	7245 Bytes	?
[+] word/stylesWithEffects.xml	XML	10928 Bytes	?
[+] word/styles.xml	XML	10175 Bytes	?
[+] docProps/core.xml	XML	623 Bytes	?
[+] word/fontTable.xml	XML	1186 Bytes	?
[+] docProps/app.xml	XML	992 Bytes	?
[+] [Content_Types].xml	XML	1563 Bytes	✔
[+] _rels/.rels	XML	590 Bytes	✔
[+] word/_rels/document.xml.rels	XML	1075 Bytes	✔
[+] word/theme/theme1.xml	XML	7127 Bytes	✔
[+] word/_rels/vbaProject.bin.rels	XML	277 Bytes	✔
[+] word/webSettings.xml	XML	428 Bytes	✔

SHA256	b3725e37271b56386103fa9c02f4335e2677b3cd283b54b28d947a37076a548f
Datetime	1980-01-01 00:00:00
Detection ratio	30 / 54 *when this report was generated*

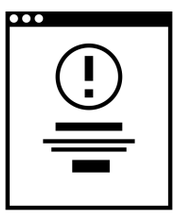
Documents:
Code Execution



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

Documents
Points To Remember!

1. Old version is binary format. Easy to create static IOCs.

2. New version is ZIP file. Difficult to create static IOCs.

PE

Details:
Portable Executable

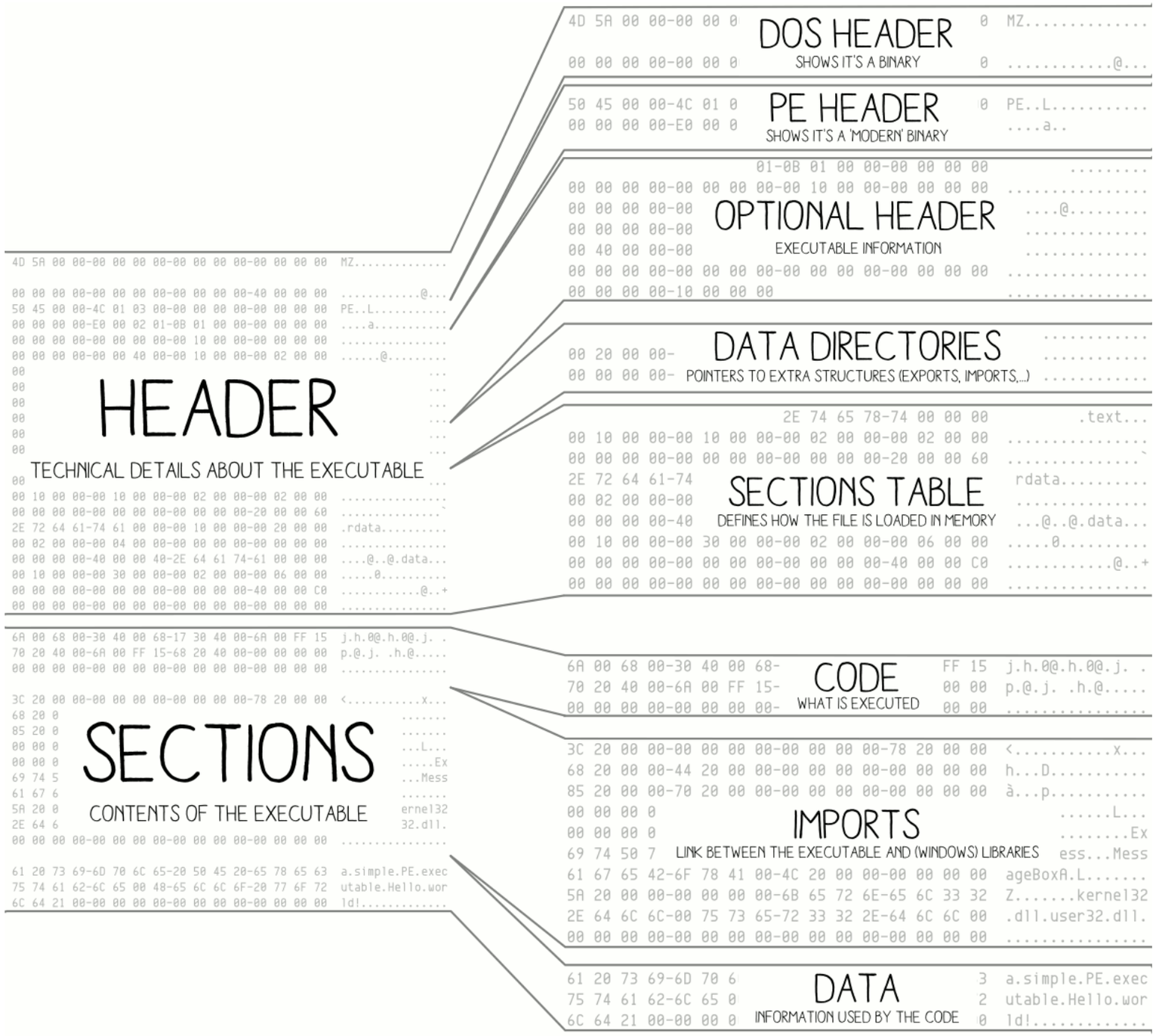
Common extensions:
.exe .dll .pif .scr .cpl .sys .drv

Magic Bytes:
4d 5a [MZ]

PE: Raw View

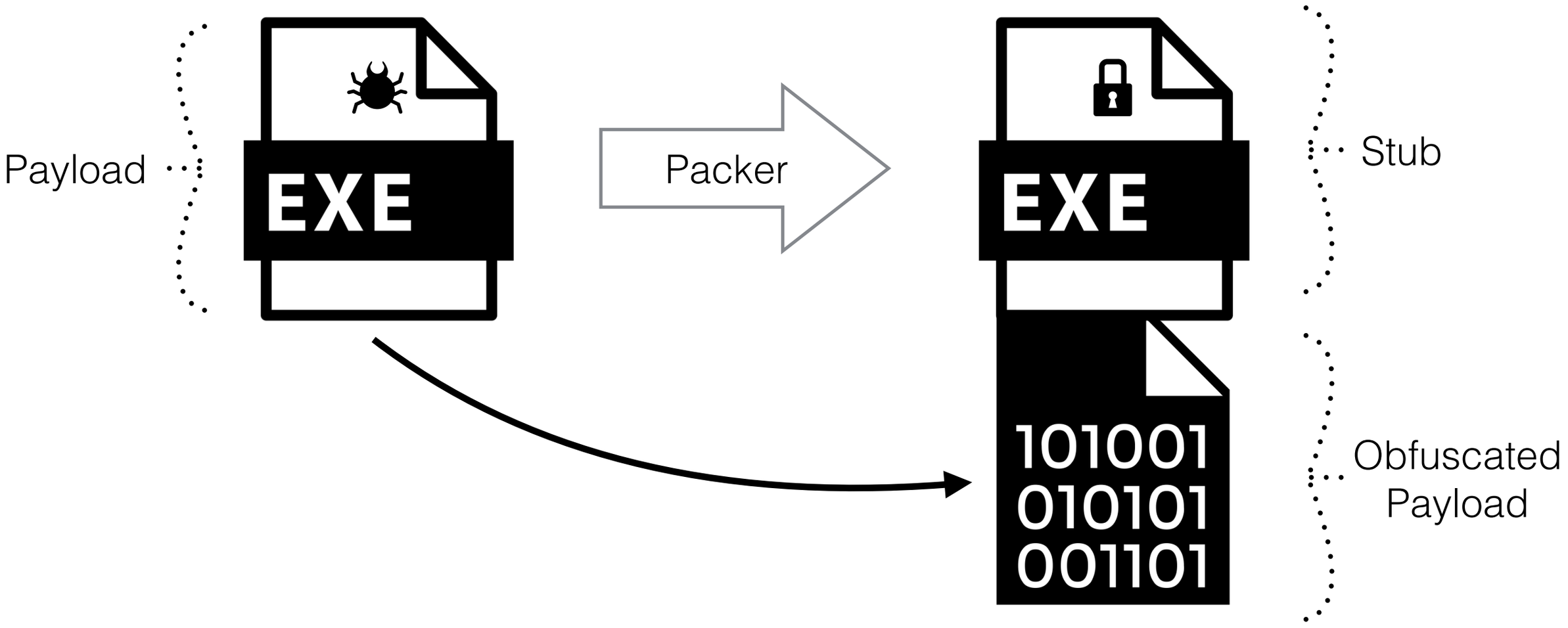
```
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ..............|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00  |................|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000070  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
00000080  91 d7 78 49 d5 b6 16 1a  d5 b6 16 1a d5 b6 16 1a  |..xI............|
00000090  ba c0 bd 1a ce b6 16 1a  ba c0 88 1a db b6 16 1a  |................|
000000a0  ba c0 bc 1a b3 b6 16 1a  dc ce 85 1a d2 b6 16 1a  |................|
000000b0  d5 b6 17 1a bf b6 16 1a  ba c0 b8 1a d4 b6 16 1a  |................|
000000c0  ba c0 8c 1a d4 b6 16 1a  ba c0 8b 1a d4 b6 16 1a  |................|
000000d0  52 69 63 68 d5 b6 16 1a  00 00 00 00 00 00 00 00  |Rich............|
000000e0  00 00 00 00 00 00 00 00  50 45 00 00 4c 01 05 00  |........PE..L...|
000000f0  3e 91 bf 4d 00 00 00 00  00 00 00 00 e0 00 02 01  |>..M............|
00000100  0b 01 0a 00 00 a4 00 00  00 64 02 00 00 00 00 00  |.........d......|
00000110  cf 22 00 00 00 10 00 00  00 c0 00 00 00 00 40 00  |."............@.|
00000120  00 10 00 00 00 02 00 00  05 00 01 00 00 00 00 00  |................|
00000130  05 00 01 00 00 00 00 00  00 50 03 00 00 04 00 00  |.........P......|
00000140  0b 36 03 00 03 00 40 81  00 00 10 00 00 10 00 00  |.6....@.........|
00000150  00 00 10 00 00 10 00 00  00 00 00 00 10 00 00 00  |................|
00000160  00 00 00 00 00 00 00 00  34 eb 00 00 50 00 00 00  |........4...P...|
00000170  00 30 01 00 68 0c 02 00  00 00 00 00 00 00 00 00  |.0..h...........|
00000180  00 0c 03 00 88 1e 00 00  00 40 03 00 ec 08 00 00  |.........@......|
```

PE: Overview

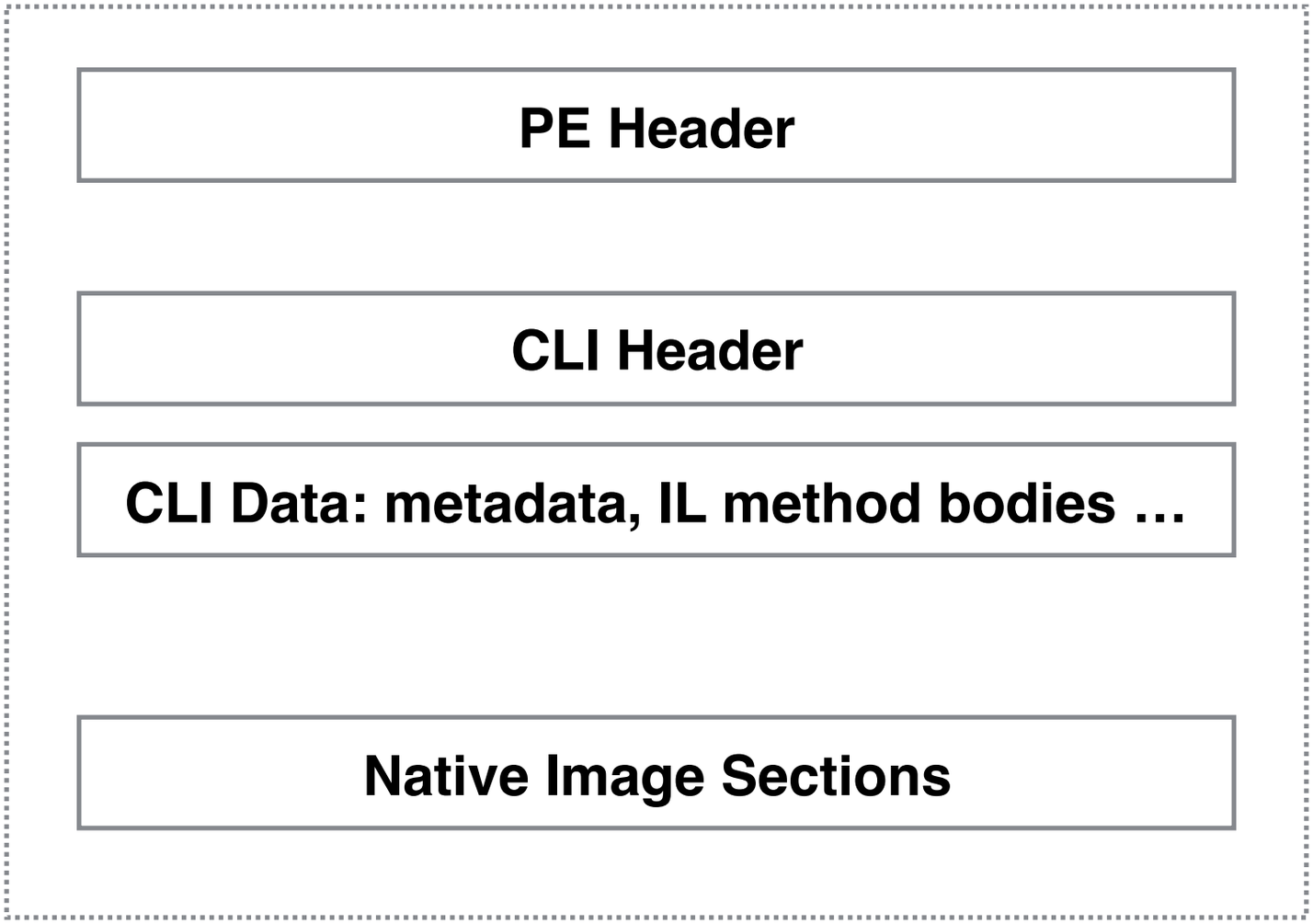


Courtesy of **Corkami** (https://github.com/corkami)

PE:
Packer/Crypter Basics



.NET (PE)


PE Header
CLI Header
CLI Data: metadata, IL method bodies …
Native Image Sections

.NET (PE)

Data Directories

0	Export Table
	...
14	~~COM~~ CLR Header

RVA and Size of CLR header inside .text section

PE
Points To Remember!

1. PE files come in many different formats, but they will always have a unique identifiable header.

2. .NET is interpreted code but it is packaged as a PE file.

Java

Details:

Java class file: java byte code
JAR: zip file containing Java class files

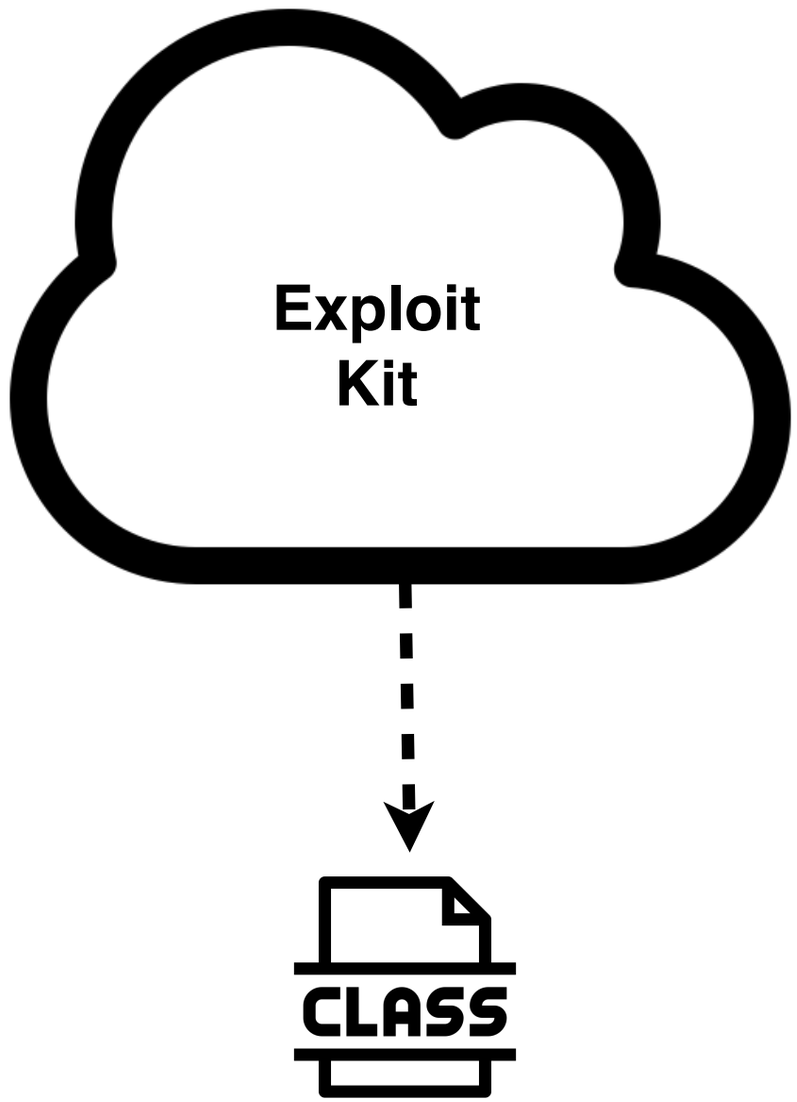
Common extensions:

Java class file: .class
JAR: .jar

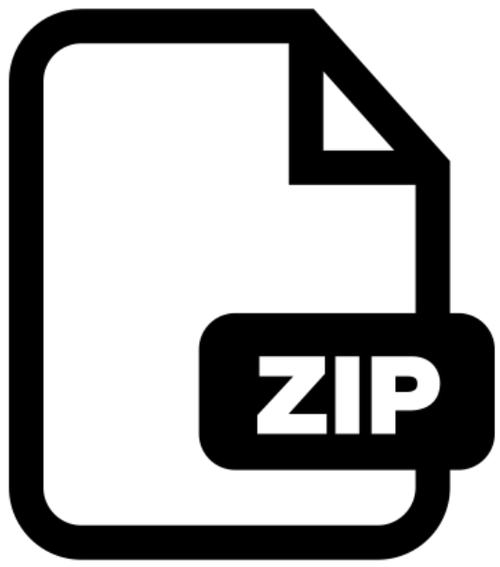
Magic Bytes:

Java class file: CA FE BA BE
JAR: 50 4B 03 04 14 00 08 00 08 00 [PK]

Java: Class Files



Java: Jar Files



```
.
├── Detection.class
├── META-INF
|   └── MANIFEST.MF
├── av.list
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooa.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooob.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooc.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooe.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooof.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooog.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooh.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooj.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggook.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooool.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooon.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooooo.class
├── iooooggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooop.class
```

Java
Points To Remember!

1. Java .class files are not executable by themselves and are mostly only associated with web based malware (exploit kits).

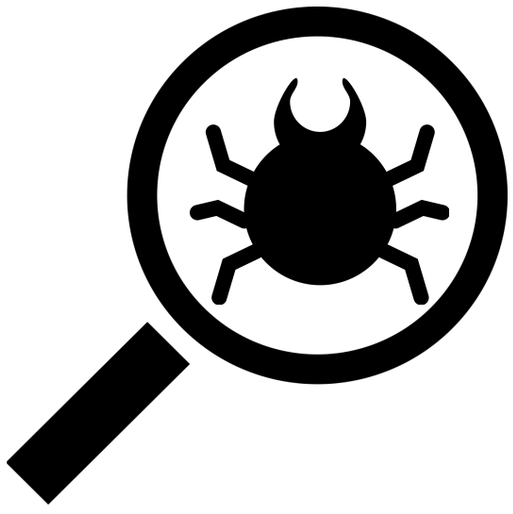
2. Java JAR files are ZIP files. Difficult to build static IOCs.

JUST DO IT!!!!!

Workshop

Details in your workbook.

Analysis



Is it Malicious

Identify Classification

Identify Family

Attributes when resident on disk

Attributes when resident in memory

Analysis
Step 1: Identification

1. Is this actually malware?

2. Can we use AV signatures etc. to identify the malware family?

virustotal

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

VTOOL v0.9.4
Find the name of the evil
Robby Zeitfuchs, Mark Lawrenz
Copyright (c) 2013-2015
--- scanner malware classification ---
ransomware: 33
dropper: 0
exploit: 0
downloader: 1
riskware: 3
rootkit: 0
worm: 0
trojan: 26
--- average detection rate ---
count hashes: 1
totalscanner: 56
positives: 48
--- scanner malware family determination ---
Most frequent word: filecoder (count=3)
Second most frequent word: drop (count=2)

Deleted files

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\svchost.exe:Zone.Identifier (failed)

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\sys1.tmp (successful)

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\svchost.exe (successful)

Created processes

C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\svchost.exe (successful)

cmd.exe /C del /Q /F C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\sys1.tmp"" (successful)

vssadmin.exe Delete Shadows /All /Quiet (successful)

C:\WINDOWS\system32\NOTEPAD.EXE C:\WINDOWS\system32\NOTEPAD.EXE" C:\Documents and Settings\<USER>\Desktop_Locky_recover_instructions.txt" (successful)

cmd.exe /C del /Q /F C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\svchost.exe"" (successful)

Shell commands

(open) C:\Documents and Settings\<USER>\Desktop_Locky_recover_instructions.txt(null) [(null)] (successful)

(open) C:\Documents and Settings\<USER>\Desktop_Locky_recover_instructions.bmp(null) [(null)] (failed)

Created mutexes

RasPbFile (failed)

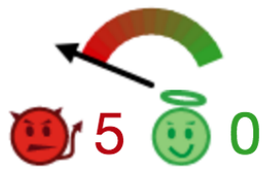
virustotal

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

hash.cymru.com/cgi-bin/bulkmhr.cgi

Team Cymru SHA1/MD5 MHR Lookup v1.0

[CYMRU] [MHR INFO] [MHR LOOKUP]

Executing commands. Please be patient!

hash.cymru.com

The server returned 3 lines.

```
# Bulk mode; hash.cymru.com [2016-04-27 00:41:54 +0000]
# SHA1|MD5 TIME(unix_t) DETECTION_PERCENT
0929bff19771c253ea7f8f3f7d6f1e98804e2845 1455981144 79
```

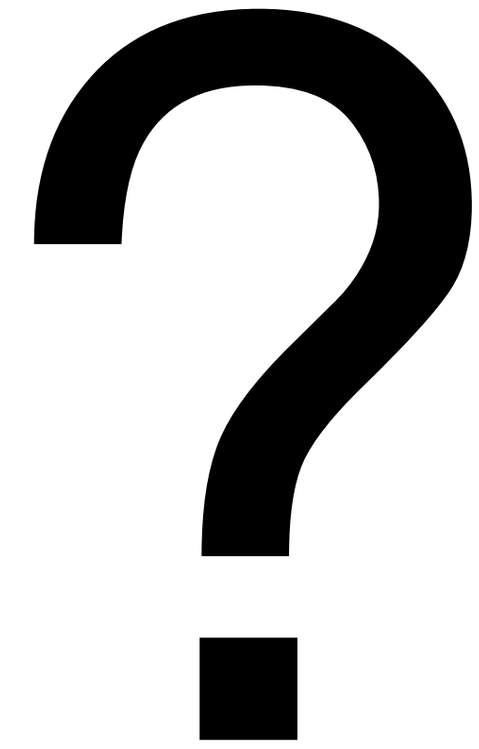
Full results have been stored at the following URL.
http://hash.cymru.com/upload/1461718245.whois.txt

NOTE: URLs are not guaranteed to last more than 7 days.

Click **HERE** to go back to the main page.

Questions? Comments? Suggestions? Please contact **TEAM CYMRU (team-cymru@cymru.com)**

No ID No Problem

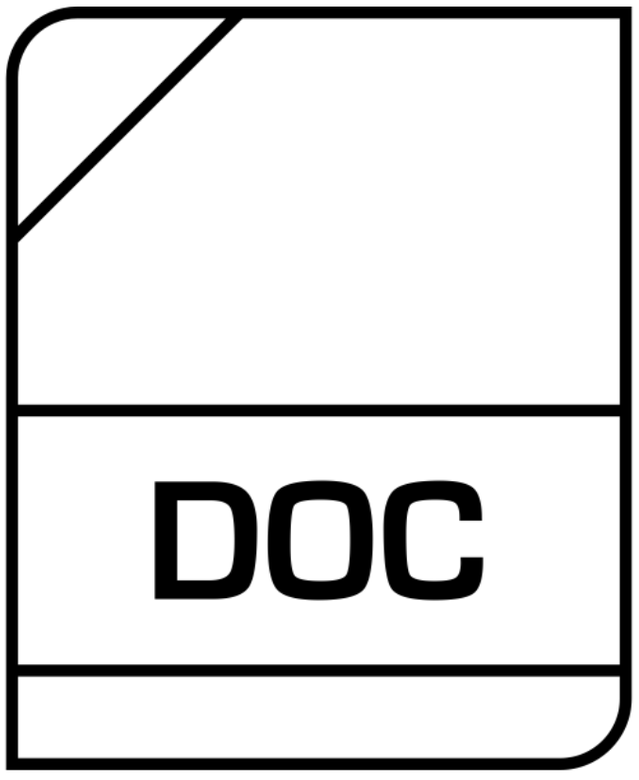


Analysis
Step 2: Static Attributes

1. Use static analysis tools to analyze the sample.

2. Collect static attributes for the sample.

Documents



Doc Static Attributes: Metadata

Core.xml

- Creator
- Revision
- LastModifiedBy
- CreateDate
- UpdateDate

App.xml

- AppVersion
- Template
- Characters
- CharactersWithSpace
- Lines
- SharedDoc
- Pages
- Words
- Paragraphs
- Company
- DocSecurity
- LinksUpToDate

Doc Static Attributes: More Macro

Macros Storage

```
├── 1Table
├── Macros
│   ├── PROJECT
│   ├── PROJECTwm
│   └── VBA
│       ├── ThisDocument
│       ├── _VBA_PROJECT
│       ├── __SRP_0
│       ├── __SRP_1
│       ├── __SRP_2
│       ├── __SRP_3
│       └── dir
├── WordDocument
├── [1]CompObj
├── [5]DocumentSummaryInformation
└── [5]SummaryInformation
```

vbaProject.bin

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

Doc Static Attributes: Macro Streams

Name	Description
PROJECT	Specifics VBA Project Properties
PROJECTwm	Specifies names of modules in both MBCS and UTF-16 encoding
__VBA_PROJECT	Specifies the version-dependent project information
__SRP_	Specifies implementation specific and version dependent performance cache.
dir	Specifies VBA Project properties, project references & module properties
ThisDocument	Default module stream associated with the Office Document.

Doc Static Attributes: PROJECT

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

```
0000000: 4944 3d22 7b44 4341 3038 3945 362d 4343  ID="{DCA089E6-CC
0000010: 4238 2d35 3034 452d 4133 3042 2d38 4636  B8-504E-A30B-8F6
0000020: 3946 3638 4342 3937 387d 220d 0a44 6f63  9F68CB978}"..Doc
0000030: 756d 656e 743d 5468 6973 446f 6375 6d65  ument=ThisDocume
0000040: 6e74 2f26 4830 3030 3030 3030 300d 0a4e  nt/&H00000000..N
0000050: 616d 653d 2250 726f 6a65 6374 220d 0a48  ame="Project"..H
0000060: 656c 7043 6f6e 7465 7874 4944 3d22 3022  elpContextID="0"
0000070: 0d0a 434d 473d 2244 4144 3846 3832 3044  ..CMG="DAD8F820D
0000080: 3632 3444 3632 3444 3632 3444 3632 3422  624D624D624D624"
0000090: 0d0a 4450 423d 2242 3442 3639 3630 3241  ..DPB="B4B69602A
00000a0: 4144 4441 4244 4441 4244 4422 0d0a 4743  ADDABDDABDD"..GC
00000b0: 3d22 3845 3843 4143 3734 3543 3934 3337  ="8E8CAC745C9437
00000c0: 3935 3337 3935 4338 220d 0a0d 0a5b 486f  953795C8"....[Ho
00000d0: 7374 2045 7874 656e 6465 7220 496e 666f  st Extender Info
00000e0: 5d0d 0a26 4830 3030 3030 3030 313d 7b33  ]..&H00000001={3
00000f0: 3833 3244 3634 302d 4346 3930 2d31 3143  832D640-CF90-11C
0000100: 462d 3845 3433 2d30 3041 3043 3931 3130  F-8E43-00A0C9110
0000110: 3035 417d 3b56 4245 3b26 4830 3030 3030  05A};VBE;&H00000
0000120: 3030 300d 0a                             000..
```

Doc Static Attributes: PROJECTwm

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

```
0000000: 5468 6973 446f 6375 6d65 6e74 0054 0068  ThisDocument.T.h
0000010: 0069 0073 0044 006f 0063 0075 006d 0065  .i.s.D.o.c.u.m.e
0000020: 006e 0074 0000 0000 00                   .n.t.....
```

Doc Static Attributes: __VBA_PROJECT

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

```
9360 1000 0704 5072 6f6a 6563 742d ae10  .`....Project-..
000c 0454 6869 7344 6f63 756d 656e 743c  ...ThisDocument<
9e10 0009 8000 00ff 0303 005f 4576 616c  ..........._Eval
7561 7465 18d9 1000 0600 4e6f 726d 616c  uate......Normal
dfd8 1000 0684 0800 ff03 0300 4f66 6669  ............Offi
6365 1575 1000 0704 4d6f 6475 6c65 3162  ce.u....Module1b
1110 0007 044d 6f64 756c 6532 6311 1000  .....Module2c...
0804 446f 6375 6d65 6e74 6ad3 1000 0c04  ..Documentj.....
446f 6375 6d65 6e74 5f4e 6577 3b45 1000  Document_New;E..
0d04 446f 6375 6d65 6e74 5f4f 7065 6ec1  ..Document_Open.
8910 0006 004d 7367 426f 7897 5210 000e  .....MsgBox.R...
0444 6f63 756d 656e 745f 436c 6f73 6537  .Document_Close7
5c10 0007 0458 4d4c 4e6f 6465 43d1 1000  \....XMLNodeC...
1704 446f 6375 6d65 6e74 5f58 4d4c 4166  ..Document_XMLAf
7465 7249 6e73 6572 742e fd10 000a 044e  terInsert......N
6577 584d 4c4e 6f64 65b6 9310 000a 0449  ewXMLNode......I
6e55 6e64 6f52 6564 6fa7 db10 000e 0443  nUndoRedo......C
6f6e 7465 6e74 436f 6e74 726f 6c55 d910  ontentControlU..
001f 0444 6f63 756d 656e 745f 436f 6e74  ...Document_Cont
656e 7443 6f6e 7472 6f6c 4166 7465 7241  entControlAfterA
6464 0101 1000 1104 4e65 7743 6f6e 7465  dd......NewConte
6e74 436f 6e74 726f 6c33 0e10 000e 8000  ntControl3......
00ff 0301 0058 4d4c 4166 7465 7249 6e73  .....XMLAfterIns
6572 74f2 c510 0002 ffff 0101 6000 0000  ert.........`...
```

Doc Static Attributes: __VBA_PROJECT Shadow Artifacts

```
9360 1000 0704 5072 6f6a 6563 742d ae10  .`....Project-..
000c 0454 6869 7344 6f63 756d 656e 743c  ...ThisDocument<
9e10 0009 8000 00ff 0303 005f 4576 616c  ..........._Eval
7561 7465 18d9 1000 0600 4e6f 726d 616c  uate......Normal
dfd8 1000 0684 0800 ff03 0300 4f66 6669  ............Offi
6365 1575 1000 0704 4d6f 6475 6c65 3162  ce.u....Module1b
1110 0007 044d 6f64 756c 6532 6311 1000  .....Module2c...
0804 446f 6375 6d65 6e74 6ad3 1000 0c04  ..Documentj.....
446f 6375 6d65 6e74 5f4e 6577 3b45 1000  Document_New;E..
0d04 446f 6375 6d65 6e74 5f4f 7065 6ec1  ..Document_Open.
8910 0006 004d 7367 426f 7897 5210 000e  .....MsgBox.R...
0444 6f63 756d 656e 745f 436c 6f73 6537  .Document_Close7
5c10 0007 0458 4d4c 4e6f 6465 43d1 1000  \....XMLNodeC...
1704 446f 6375 6d65 6e74 5f58 4d4c 4166  ..Document_XMLAf
7465 7249 6e73 6572 742e fd10 000a 044e  terInsert......N
6577 584d 4c4e 6f64 65b6 9310 000a 0449  ewXMLNode......I
6e55 6e64 6f52 6564 6fa7 db10 000e 0443  nUndoRedo......C
6f6e 7465 6e74 436f 6e74 726f 6c55 d910  ontentControlU..
001f 0444 6f63 756d 656e 745f 436f 6e74  ...Document_Cont
656e 7443 6f6e 7472 6f6c 4166 7465 7241  entControlAfterA
6464 0101 1000 1104 4e65 7743 6f6e 7465  dd......NewConte
6e74 436f 6e74 726f 6c33 0e10 000e 8000  ntControl3......
00ff 0301 0058 4d4c 4166 7465 7249 6e73  .....XMLAfterIns
6572 74f2 c510 0002 ffff 0101 6000 0000  ert.........`...
```

Removed Modules

Default Sub created when selecting Document UI

Removed Event listeners

Doc Static Attributes: __SRP_ Streams

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

```
009f a004 0000 03f6 0902 0000 0000 00c0  ................
0000 0000 0000 4603 0000 0208 0000 0044  ......F........D
6f63 756d 656e 7402 0000 0204 0000 0074  ocument........t
6573 7403 0000 0d0c 000c 0040 0000 0000  est........@....
0000 0000 0004 0000 0b08 0000 0074 0065  .............t.e
0073 0074 0007 0000 07ff ffff ffff ffff  .s.t............
ff53 020b 00b9 0500 0000 0000 00b0 0000  .S..............
0000 0000 0023 0000 0e02 0570 0069 a7f1  .....#.....p.i..
```

Cached content from previous revision

Doc Static Attributes: ThisDocument

```
.
├── PROJECT
├── PROJECTwm
└── VBA
    ├── ThisDocument
    ├── _VBA_PROJECT
    ├── __SRP_0
    ├── __SRP_1
    ├── __SRP_2
    ├── __SRP_3
    └── dir
```

```
0000650: ff00 0001 ecb0 0041 7474 7269 6275 7400  .......Attribut.
0000660: 6520 5642 5f4e 616d 0065 203d 2022 5468  e VB_Nam.e = "Th
0000670: 6900 7344 6f63 756d 656e 1074 220d 0a0a  i.sDocumen.t"...
0000680: 8c42 6173 0102 8c31 4e6f 726d 616c 022e  .Bas...1Normal..
0000690: 1956 476c 6f62 616c 2101 aa53 7061 6301  .VGlobal!..Spac.
00006a0: 6c46 6108 6c73 650c a243 7265 6110 7461  lFa.lse..Crea.ta
00006b0: 626c 151f 5072 6520 6465 636c 6100 0649  bl..Pre decla..I
00006c0: 6411 009e 5472 750d 4245 7870 086f 7365  d...Tru.BExp.ose
00006d0: 141c 5465 6d70 006c 6174 6544 6572 6902  ..Temp.lateDeri.
00006e0: 7615 2443 7573 746f 6d6c 697a 8443 8331  v.$Customliz.C.1
00006f0: 5000 1800 1c20 1053 7562 2085 875f 4f70  P.... .Sub ..._Op
0000700: 0065 6e28 290d 0a4d 7300 6742 6f78 2028  .en()..Ms.gBox (
0000710: 2249 0027 6d20 696e 2061 2000 6d61 6372  "I.'m in a .macr
0000720: 6f20 706f 2070 7069 6e67 8107 6573 0073  o po pping..es.s
0000730: 6167 6520 626f 7822 2200 1845 6e64 8124  age box""..End.$
0000740: 0d0a 00                                  ...
```

</> **Macros and VBA code streams**

[+] ThisDocument.cls	word/vbaProject.bin	VBA/ThisDocument	53 bytes
[+] Module1.bas	word/vbaProject.bin	VBA/Module1	13216 bytes

create-file create-ole handle-file obfuscated open-file write-file

```
Public Function VerAuditoria()
Dim SQL As String


VerAuditoria = False
RsUsu.ActiveConnection = Con

SQL = "Select * FROM usuarios "
SQL = SQL & " WHERE usu_id=" & IdUsuario
RsUsu.Open SQL

    If Not RsUsu.EOF Then
     If RsUsu!usu_auditor = "S" Then
        VerAuditoria = True
     Else
```

Doc Static Attributes: Embedded Objects

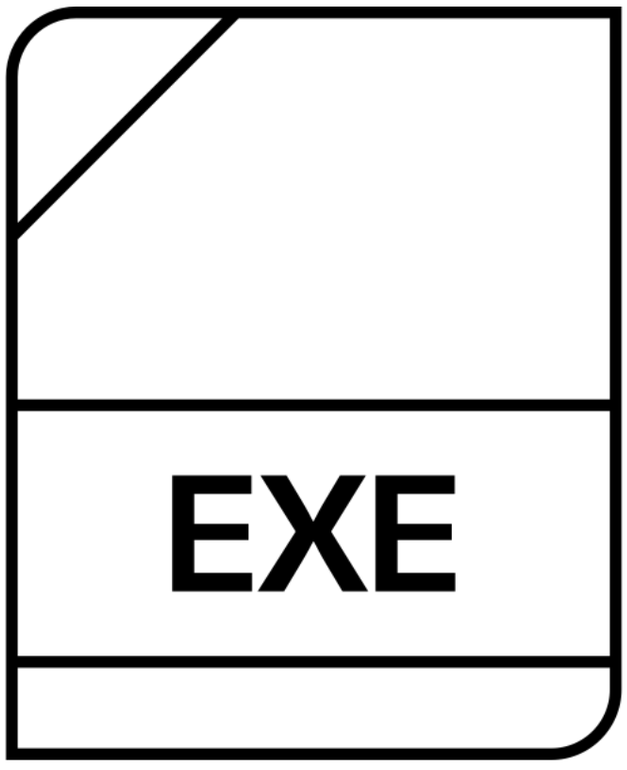
Doc Static Attributes: Packager Format

hacklu.rtf

```
1  {\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033{\
2  {\*\generator Riched20 10.0.14393}\viewkind4\uc1
3  \pard\sa200\sl276\slmult1\f0\fs22\lang9
4  {\object\objemb
5      {\*\objclass Package}\objw1680\objh810{\*\objdata
6  01050000
7  02000000
8  08000000
9  5061636b61676500
10 00000000
11 00000000
12 3db91300
13 02004f67686a58354652397a302e65786500443a5c68656c6c6f5c
14 58354652397a302e657865000000030032000000433a5c55736572
15 6174615c4c6f63616c5c54656d705c4f67686a58354652397a302e
```

```
[*] Analyzing file....
[*] Scanning file for embedded objects
----------------------------------------
[*] Found object at:   177
    Type:              OLE Embedded
    OLE Version:       01050000
    Format:            EmbeddedObject (02000000)
    ClassName:         Package
    Total Data Length: 1292605
[*] Processing Embedded Package Data
 Header:         0200
 Label:          OghjX5FR9z0.exe
 FormatId:       00000300
 OriginalPath:   D:\hello\hack.lu\OghjX5FR9z0.exe
 Extract Path:   C:\Users\idiom\AppData\Local\Temp\OghjX5FR9z0.exe
 Data Size:      1292288
 Data (SHA1):    1b2af5c89719f2ac3bf56b42a44cb6dd89b242c4

----------------------------------------
```

PE



PE Static Attributes: Exif Metadata

Details:
Exif metadata is extra information that is used to describe the file. PE files are bundled with their own metadata though it is contained in structures that need a tool to parse.

Tools:
- pftriage.py
- VirusTotal “File detail” tab
- Malwr “Static Analysis” tab

Notes for triage:
PE metadata is very easy to alter so most malware developers will simply overwrite the metadata with garbage. Metadata is not a reliable attribute for robust IOCs however it may be useful as an initial **pivot** to find related samples.

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_7d69f3934 be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142.exe

Advanced heuristic and reputation engines

F-Secure Deepguard	Suspicious:W32/Malware!Online

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

Authenticode signature block and FileVersionInfo properties

Copyright	Copyright © 2014-2015 F-Secure Corporation
Product	F-Secure Service Enabler
Original name	NetworkInstaller.exe
Internal name	NetworkInstaller
File version	3.05.108.0
Description	F-Secure Network Installer
Signature verification	Signed file, verified signature
Signing date	10:56 AM 10/7/2015
Signers	[+] F-Secure Corporation [+] GlobalSign CodeSigning CA - G2 [+] GlobalSign
Counter signers	[+] GlobalSign TSA for MS Authenticode - G2 [+] GlobalSign Timestamping CA - G2 [+] GlobalSign

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2015-08-25 11:39:50
Entry Point	0x00029398
Number of sections	5

malwr

- Quick Overview
- Static Analysis
- Behavioral Analysis
- Network Analysis
- Dropped Files
- Comment Board (0)

Static Analysis | Strings | Antivirus

PE Imphash

f32dfedd091ef17095981aa85a1194bb

Version Infos

LEGALCOPYRIGHT	Copyright \xa9 2014-2015 F-Secure Corporation
INTERNALNAME	NetworkInstaller
FILEVERSION	3.05.108.0
COMPANYNAME	F-Secure Corporation
PRIVATEBUILD	
LEGALTRADEMARKS	
COMMENTS	
PRODUCTNAME	F-Secure Service Enabler
SPECIALBUILD	
PRODUCTVERSION	3.05.108.0
FILEDESCRIPTION	F-Secure Network Installer
ORIGINALFILENAME	NetworkInstaller.exe

PE Static Attributes: Imports

Details:
PE file imports (import table) is a list of all the libraries (DLLs) and functions (APIs) that the PE will need to call during execution. Individual imports aren't unique but comparing all of them might be unique to the sample… this is what **imphash** does!

Tools:

- pftriage.py
- VirusTotal "Additional information" tab
- Malwr "Static Analysis" tab

Notes for triage:
Imphash creates a unique hash of all the imports listed for the PE file. This hash can then be used as a **pivot** to attempt to identify other related samples. Import hashing is generally more useful for payload identification as droppers will usually add random imports to circumvent this identification technique.

PE imports

[+] ADVAPI32.dll

[+] COMCTL32.dll

ImageList_DrawEx

ImageList_LoadImageW

ImageList_Destroy

[+] CRYPT32.dll

CertGetNameStringW

[+] GDI32.dll

[+] KERNEL32.dll

[+] OLEAUT32.dll

[+] USER32.dll

[+] VERSION.dll

[+] WINHTTP.dll

[+] WINTRUST.dll

[+] WTSAPI32.dll

[+] gdiplus.dll

[+] ole32.dll

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

File identification

MD5	2b873cc024ae4f530fe264b69c91516c
SHA1	a2f68471f4a23a308f077b3fd4042f21d849362f
SHA256	eec2c87845e4fd708e32c202d2055a73f3990a129b8d14890f3328a975aef04c
ssdeep	12288:8V33nozhCLNrhKkUEZIMkOzm4XGZ1L4qU1nlpT:8V34zhCLZcUZrOvGZ1L4qOnlx
authentihash	4b59bd22f94d44a484bbdbbfba0aba6198a57dfe60f5c5a461fe44a223185629
imphash	f32dfedd091ef17095981aa85a1194bb
File size	843.0 KB (863272 bytes)
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable (generic) (52.9%) Generic Win/DOS Executable (23.5%) DOS Executable Generic (23.5%)
Tags	peexe signed overlay

VirusTotal metadata

First submission	2016-09-16 15:13:19 UTC (3 hours, 26 minutes ago)
Last submission	2016-09-16 15:13:19 UTC (3 hours, 26 minutes ago)
File names	NetworkInstaller NetworkInstaller.exe FSecureSafeNetworkInstaller.exe

PE Static Attributes: Strings

Details:
The most valuable, though possibly also the most misunderstood static attribute, ascii and unicode strings contained in the PE file can be used to uniquely identify the file.

Tools:
- Sysinternals Strings
- uStrings.py

Notes for triage:
Without the ability to disassemble the sample and review the code for unique blocks identifying unique strings is the next best approach for finding static **pivots** and developing static **IOC**s.
Strings may be obfuscated even if no packer is used!

PE Static Attributes:

Tips for Strings!

Do's:

- Locate strings that are relevant to the malware's operation (ex. Registry keys, File names, Decryption keys, Domain names, etc.)
- Check to see if there is a .pdb path
- Verify your strings against sandbox output in dynamic analysis

Don'ts:

- Include strings that are compiler artifacts
- *Include generic strings (ex. generic registry key path, generic file path, etc.)
- Forget to check unicode strings
- Include individual imports

```
sh-3.2$ strings sample1.exe
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
gr?Z+x
@hr~
)rK@@NKm
y7Og6
[FhF_l
^h^)(
$1\
{Uuo*
HbiI0
0}Zo
BVfHY
p9<*
*I>t
"D$i(
.tIFnh`
83'>l
'k"$VH
0Q+;
VXes
>.'6%
*Sj`Uo
31nm5

XGWa
:ggz
```

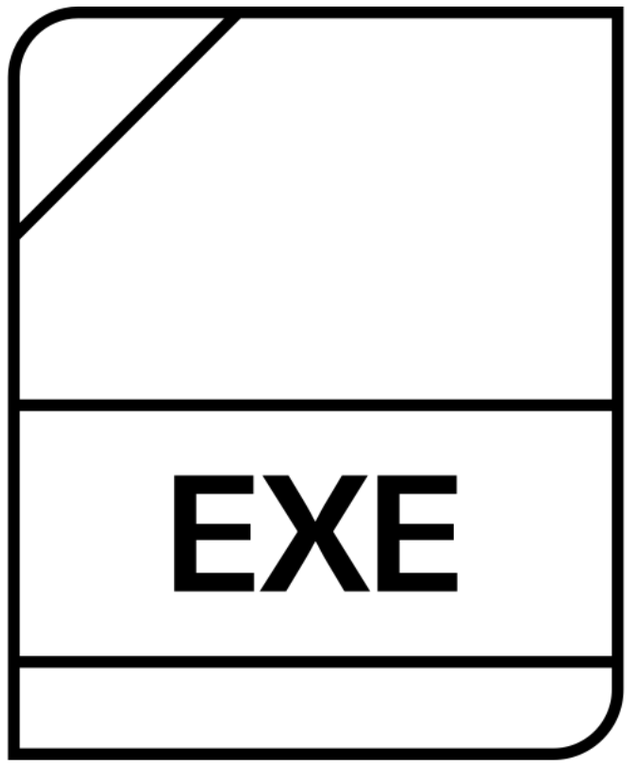
malwr

Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Comment Board (0)

Static Analysis Strings Antivirus

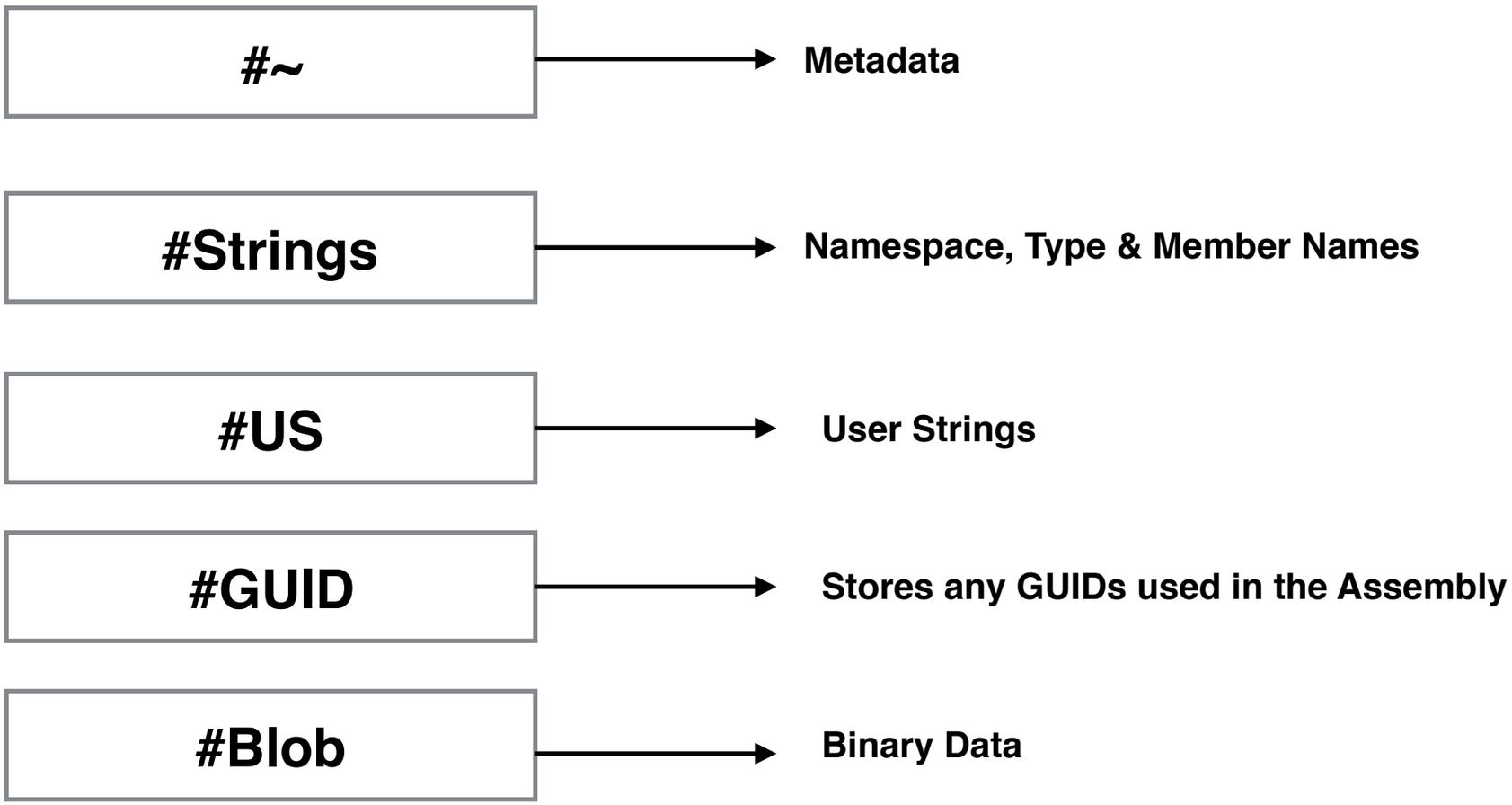
```
!This program cannot be run in DOS mode.
`.rdata
@.data
@.reloc
gr?Z+x
)rK@@NKm
[FhF_l
.tIFnh`
'k"$VH
*Sj`Uo
q|PT@d,
K#'T?A
UT.Lwi
tk!K&^
YP{EKU
[HL_05
!HQtL\
"er[@PP<
st:!D`
```

PE (.NET)



.NET Static Attributes: Streams

Predefined Streams



CFF Explorer VIII - [Program.exe]

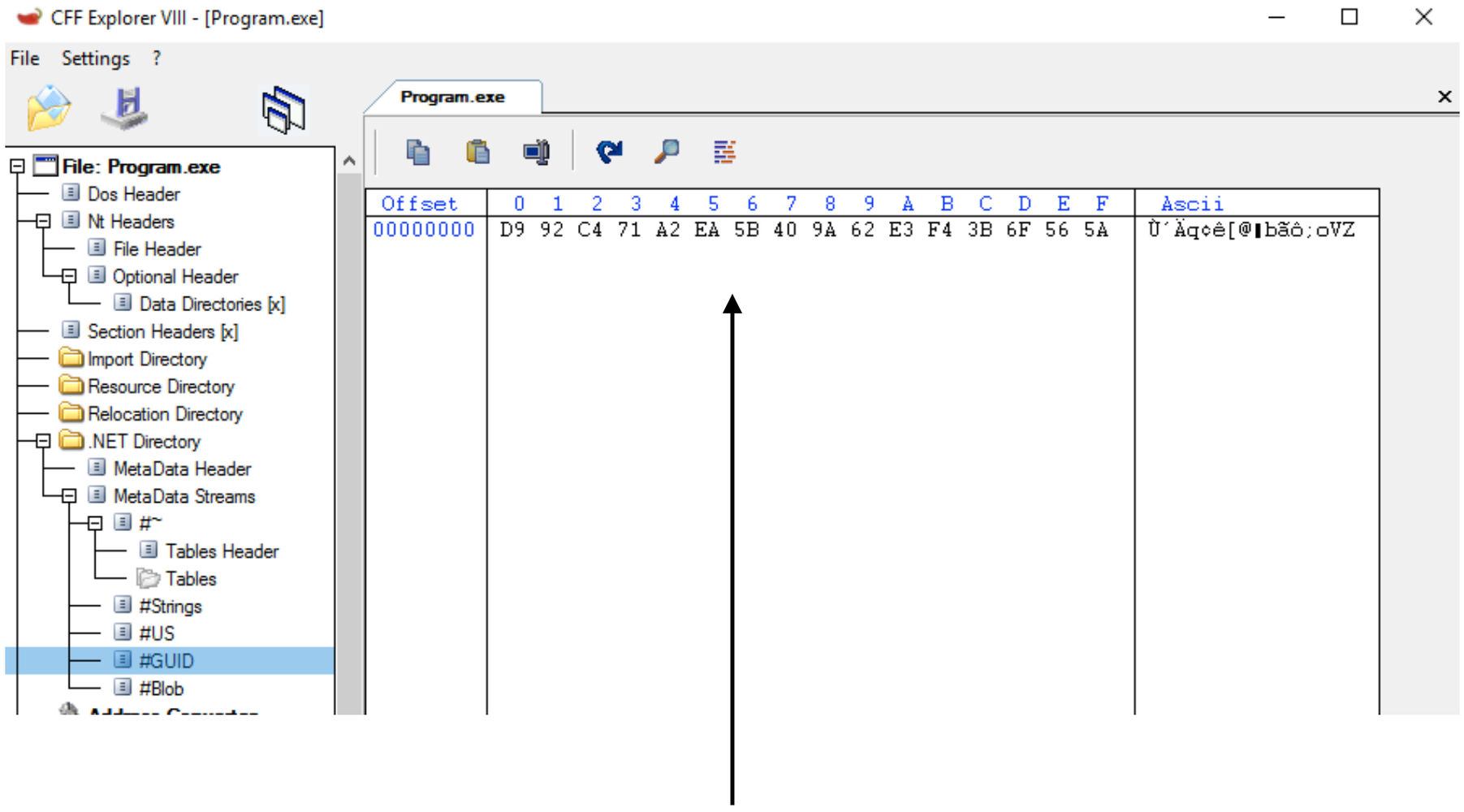
File Settings ?

- File: Program.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [x]
  - Section Headers [x]
  - Import Directory
  - Resource Directory
  - Relocation Directory
  - .NET Directory
    - MetaData Header
    - MetaData Streams
      - #~
        - Tables Header
        - Tables
      - #Strings
      - #US
      - #GUID
      - #Blob

Program.exe

Offset	Size	Name
Dword	Dword	szAlignedAnsi
0000006C	00000128	#~
00000194	0000012C	#Strings
000002C0	0000002C	#US
000002EC	00000010	#GUID
000002FC	00000060	#Blob

.NET Static Attributes: GUIDS: MVID



MVID Module Version Id
Unique Per Build
{D992C471-A2EA-5B40-9A62-E3F43B6F565A}

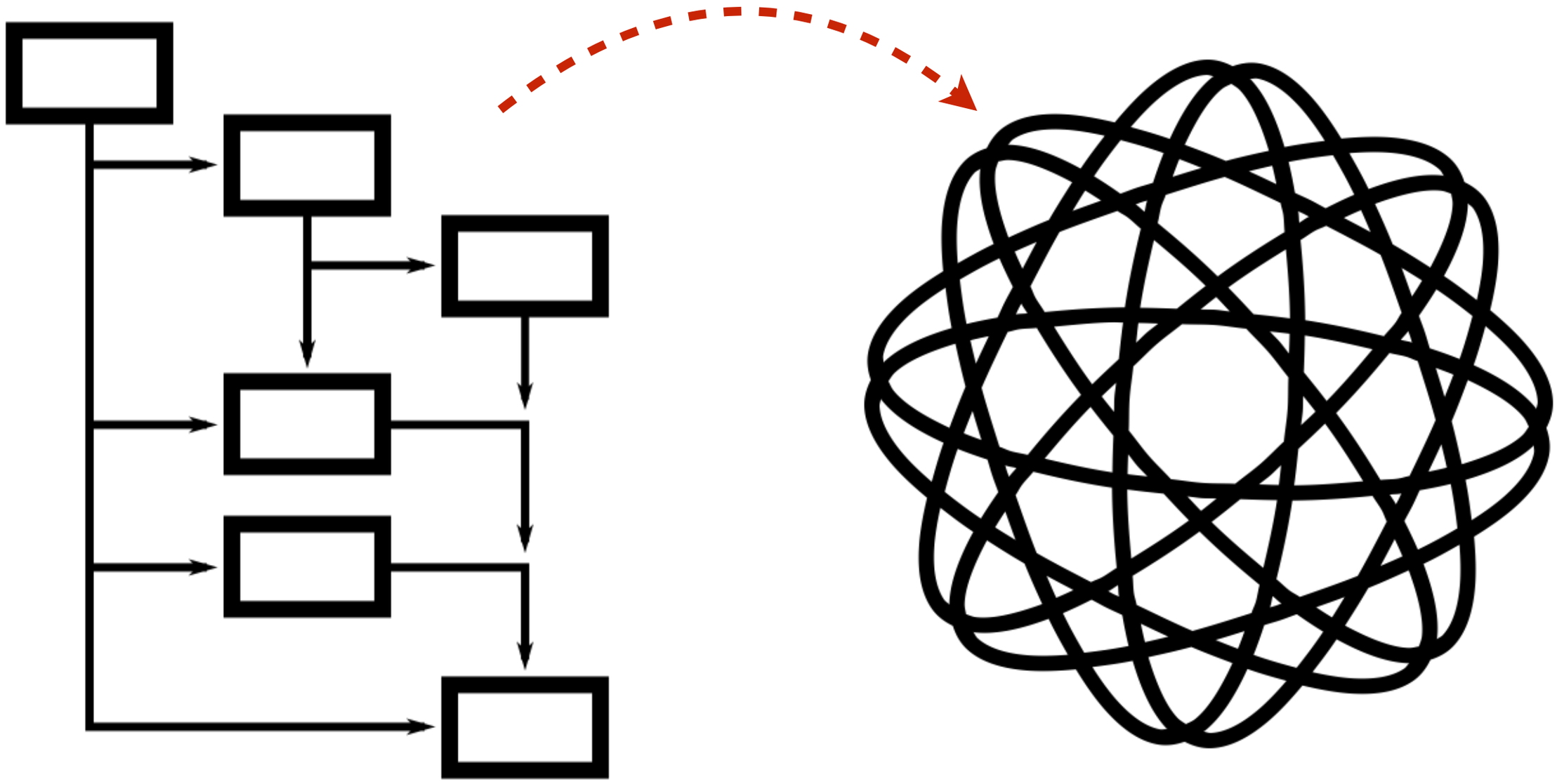
.NET Static Attributes: GUIDS: TYPELIB ID

```
13      [assembly: AssemblyCopyright("Copyright ©  2016")]
14      [assembly: AssemblyTrademark("")]
15      [assembly: AssemblyCulture("")]
16
17      // Setting ComVisible to false makes the types in this assembly not visible
18      // to COM components.  If you need to access a type in this assembly from
19      // COM, set the ComVisible attribute to true on that type.
20      [assembly: ComVisible(false)]
21
22      // The following GUID is for the ID of the typelib if this project is exposed to COM
23      [assembly: Guid("f707dac9-5779-4c8b-bdfc-6ccec6f6efad")]
24
25      // Version information for an assembly consists of the following four values:
26      //
27      //      Major Version
```

TypeLib Id
Unique Per Project

```
using ...

[assembly: AssemblyCompany("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("Copyright ©  2016")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: AssemblyProduct("c          :")]
[assembly: AssemblyTitle("c          t")]
[assembly: AssemblyTrademark("")]
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: ComVisible(false)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default
[assembly: Guid("f707dac9-5779-4c8b-bdfc-6ccec6f6efad")]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows=true)]
[assembly: TargetFramework(".NETFramework,Version=v4.5.2", Frame
```

.NET Static Attributes: Obfuscation



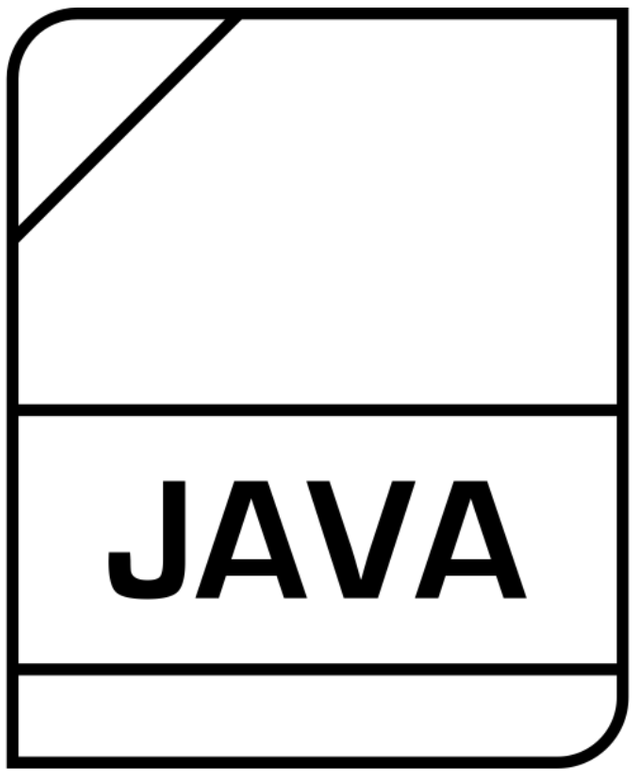
```
Label1:
    HtmlElement htmlElement = null;
    num3 = 51;
    while (true)
    {
    Label14:
        switch (num3)
        {
            case 0:
            {
                if (htmlDocument.GetElementById("new_comment_field") != null)
                {
                    this.□ = true;
                    Explorer explorer = this;
                    explorer.□ = explorer.□ + 1;
                    num3 = 15;
                    continue;
                }
                else
                {
                    num3 = 59;
                    continue;
                }
            }
            case 1:
            {
                goto Label2;
            }
            case 2:
            {
                htmlElement = htmlDocument.get_All().get_Item(num2);
                num3 = 30;
                continue;
            }
            case 3:
            {
                string name = document.get_All().get_Item(num).get_Name();
                str = name;
                if (name == null)
                {
                    goto Label2;
                }
                num3 = 39;
                continue;
            }
```

.NET Static Attributes: Obfuscation as a Pivot

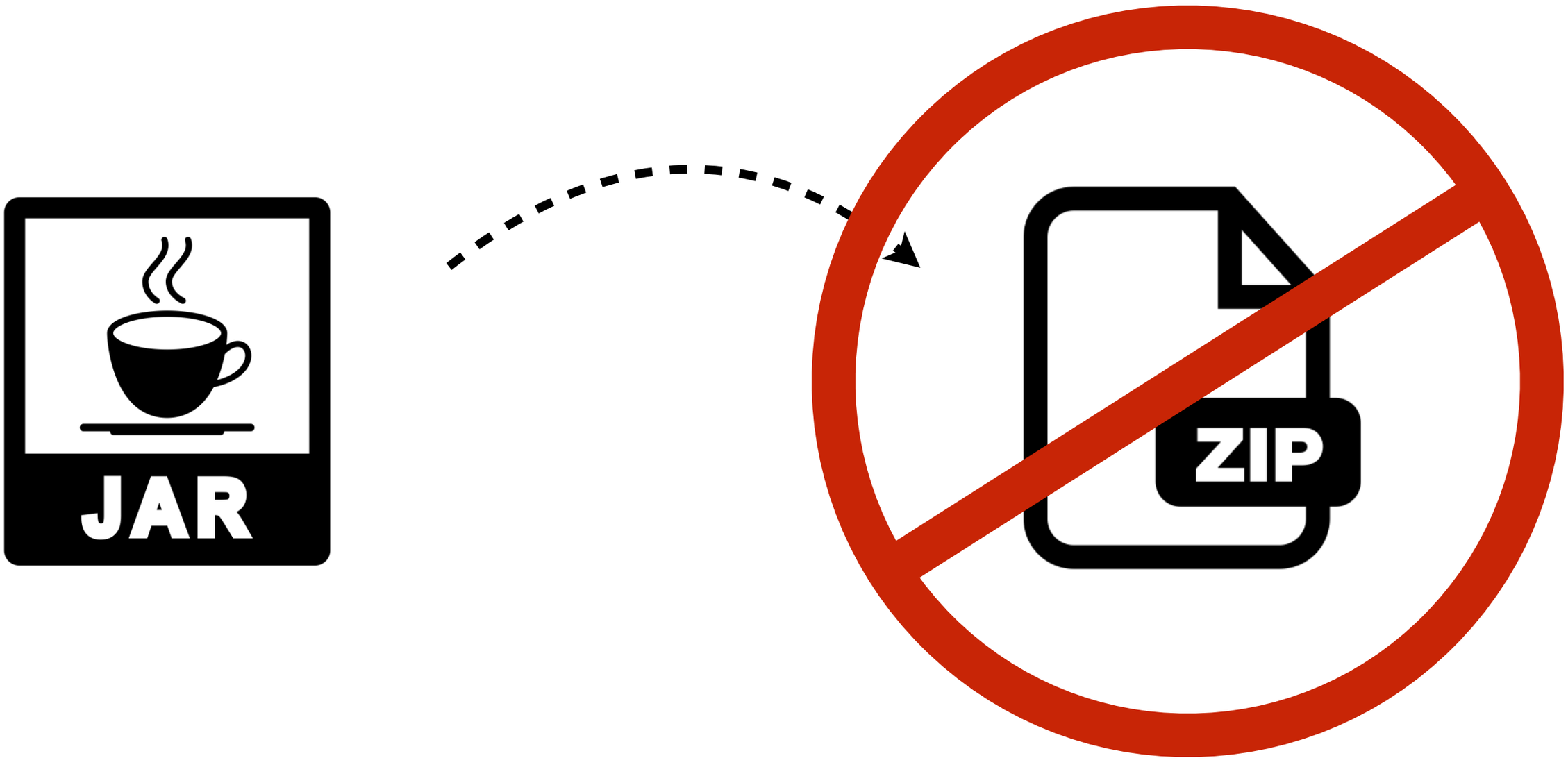
```
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: Dotfuscator("124576:1:1:4.9.6005.29054", 1, true)]
[assembly: AssemblyCompany("Cisco Systems Inc")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("Copyright ©  2016")]
[assembly: AssemblyDescription("patch for Cisco")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: AssemblyProduct("patch")]
[assembly: AssemblyTitle("patch for Cisco")]
[assembly: AssemblyTrademark("")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: ComVisible(false)]
[assembly: Guid("02fe7f38-7e3f-4fc5-9ab4-64a30666492a")]
```

Product ID and Version information

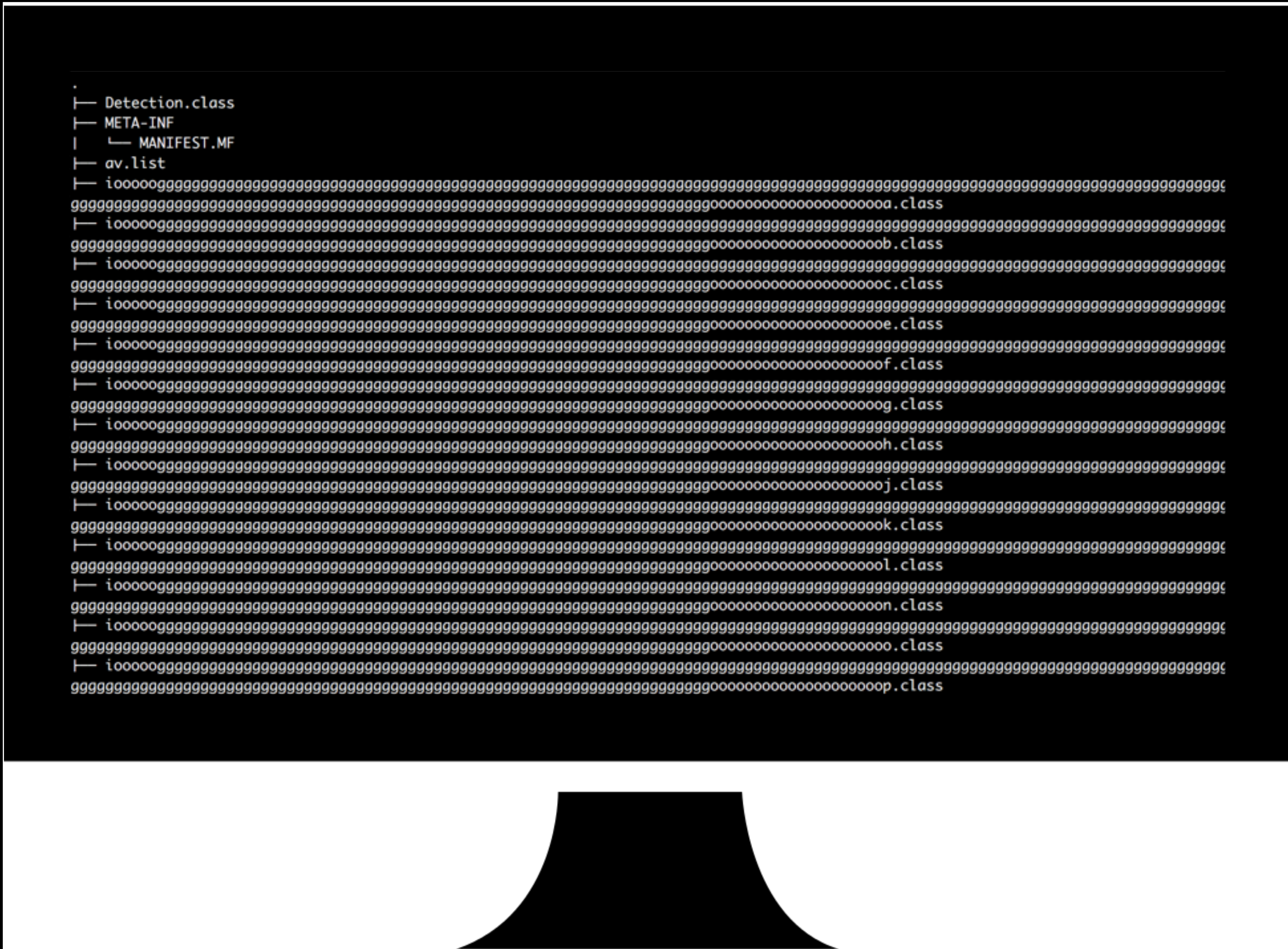
Java



Java Static Attributes: Jar Files are Zip Files



Low Quality Static Attributes


.
├── Detection.class
├── META-INF
| └── MANIFEST.MF
├── av.list
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooa.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooob.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooc.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooe.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooof.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooog.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooh.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooooj.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggook.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggooooooooooooooooooool.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooon.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooooo.class
├── iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggoooooooooooooooooooop.class

Java Static Attributes: Manifest

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.9.4
X-COMMENT: Main-Class will be added automatically by build
Class-Path:
Created-By: 1.8.0_102-b14 (Oracle Corporation)
Main-Class: Detection
```

Entry for execution

Manifest

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.9.4
X-COMMENT: Main-Class will be added automatically by build
Class-Path:
Created-By: 1.8.0_102-b14 (Oracle Corporation)
Main-Class: Detection
```

Java packages

java.io

java.lang

java.lang.reflect

java.security

java.util

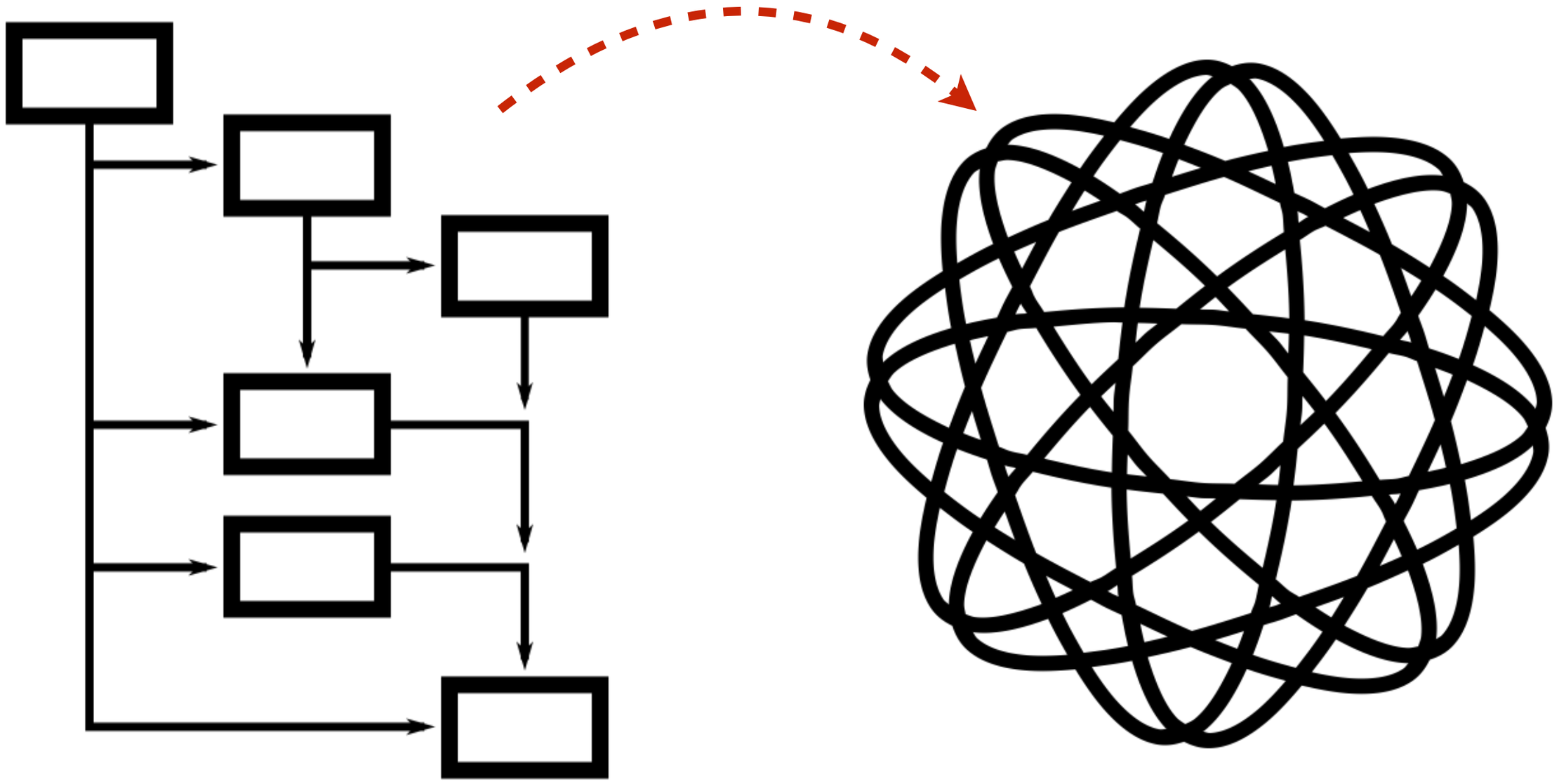
java.util.jar

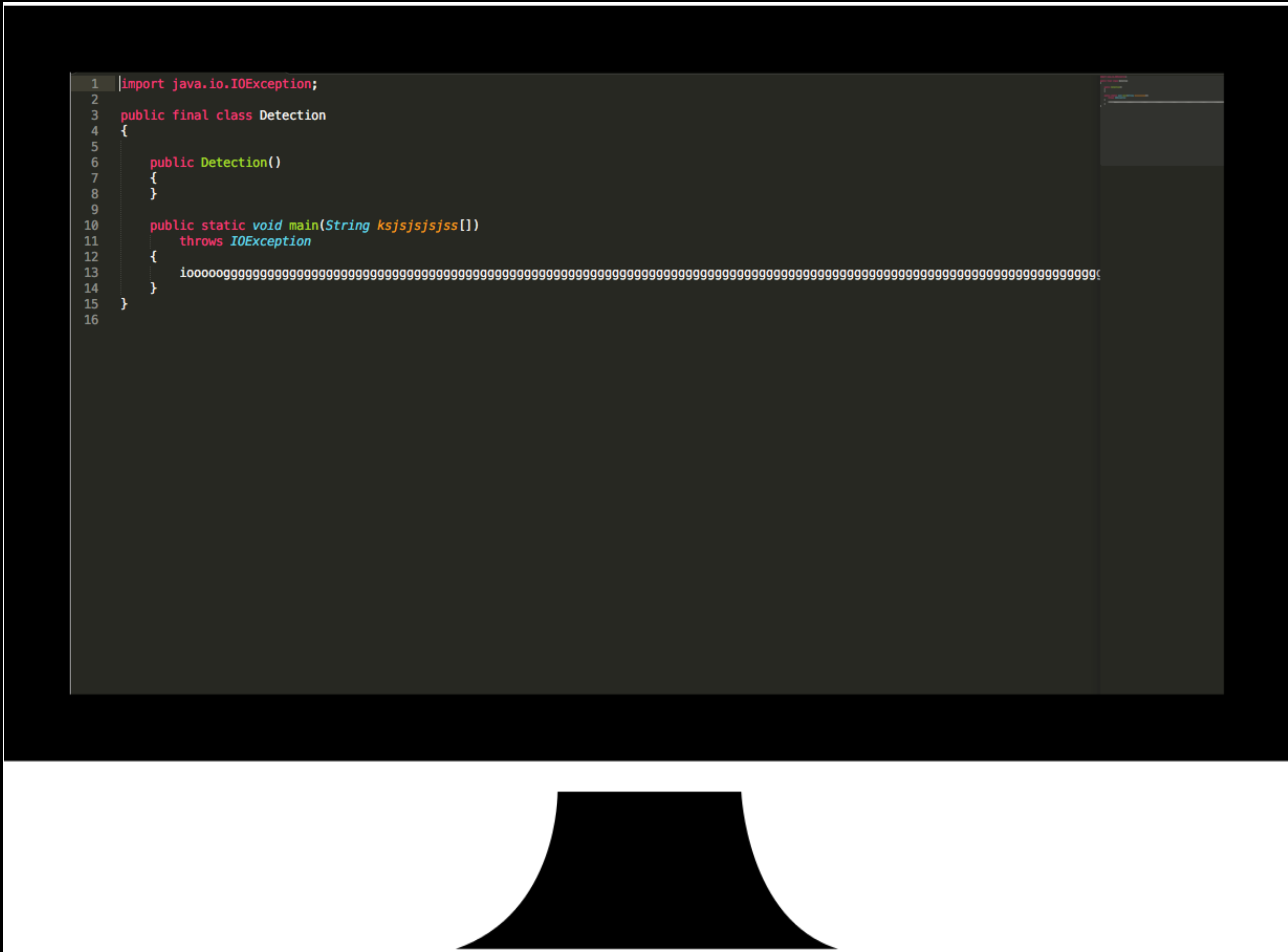
java.util.zip

javax.crypto

javax.crypto.spec

Java Static Attributes: Obfuscation





import java.io.IOException;
public final class Detection
{
public Detection()
{
}
public static void main(String ksjsjsjsjss[])
throws IOException
{
iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg
}
}

Contained files

This file is a compressed stream containing 26 files.

[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	6281 Bytes	✖
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	3784 Bytes	✖
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	7216 Bytes	✖
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	1556 Bytes	✖
[+] META-INF/MANIFEST.MF	unknown	201 Bytes	✔
[+] rWkDTJ/gmABnbS.JUM	unknown	114704 Bytes	✔
[+] av.list	unknown	94384 Bytes	✔
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	1539 Bytes	✔
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	1846 Bytes	✔
[+] iooooogggggggggggggggggggggggggggggggggggggggggggggggggggggg...	Java Bytecode	1092 Bytes	✔

Show all

Compression metadata

Contained files	26
Uncompressed size	255556
Highest datetime	2016-10-07 00:20:02
Lowest datetime	2016-10-07 00:20:02

JUST DO IT!!!!!

Workshop

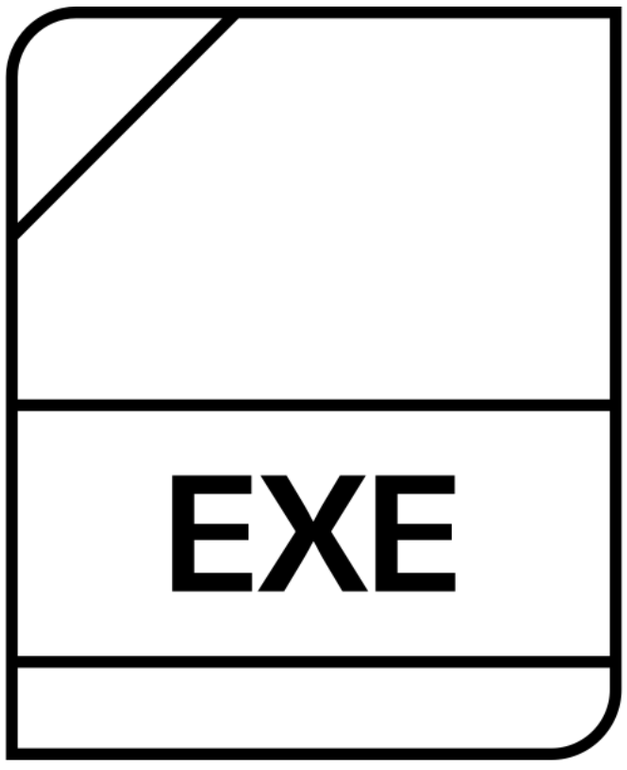
Details in your workbook.

Analysis
Step 3: Dynamic Attributes

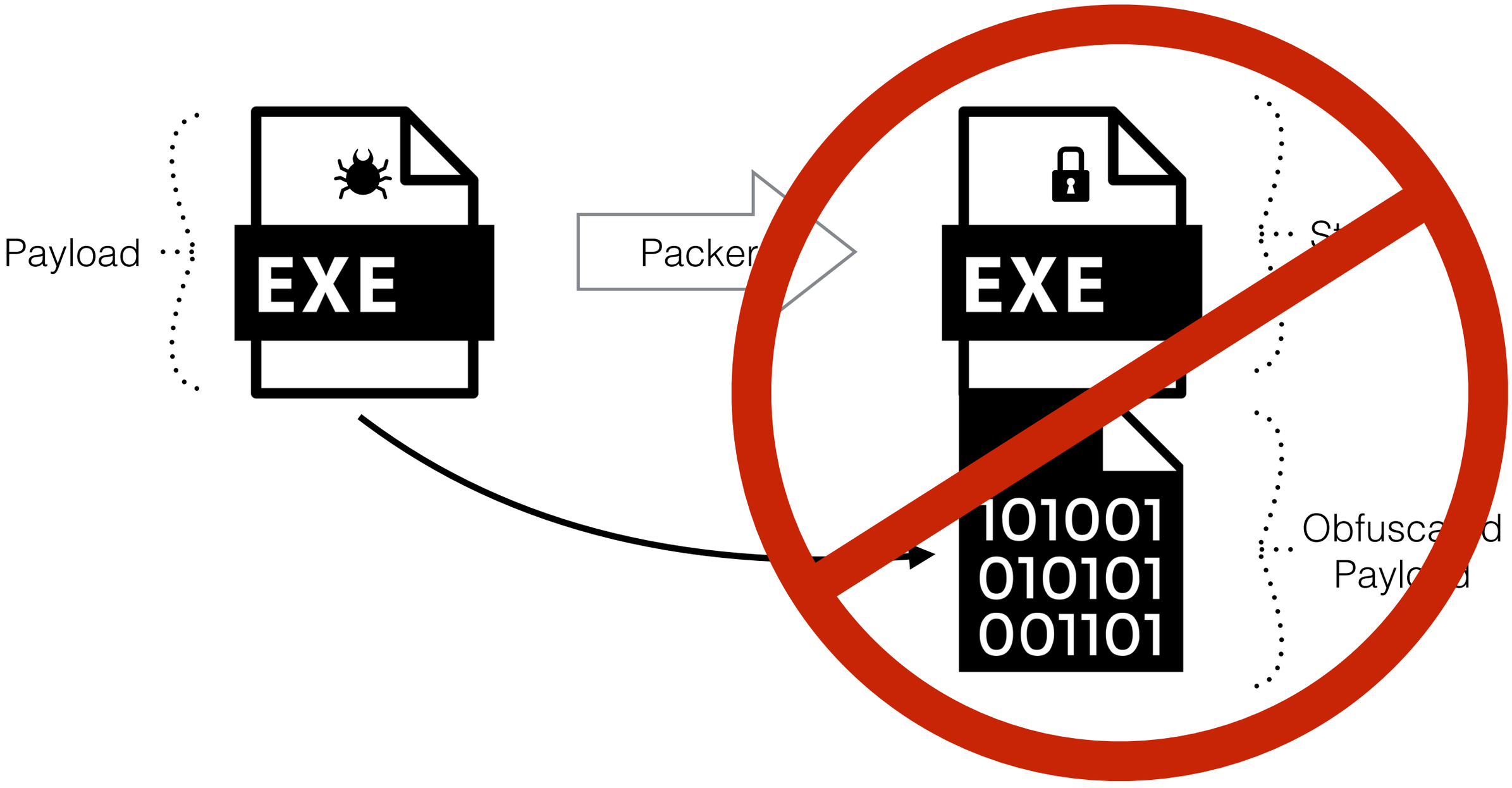
1. Use dynamic analysis tools to analyze the sample.

2. Collect dynamic attributes for the sample.

PE



Packer/Crypter Basics



Low Quality Static Attributes

PE:
Packers vs. Static Attributes

- Stub may not contain any strings
- Stub may not contain all Imports used by payload
- Stub metadata may be altered
- **Cannot trust the static attributes to represent the payload!**
- Possible to use static attributes to identify stub

FileVersionInfo properties

Product	The easiest way for individuals to pay their subscription is by PayPal using the buttons on this page. You can sign up to pay a subscription annually or just this once
Original name	E34PNvR1.exe
Internal name	E34PNvR1
File version	1.00.0030
Description	Individual members can pay subscriptions in three ways: by PayPal, from links on this webpage, by credit or debit card, or by a cheque in pounds
Comments	Members of the Early English Text Society receive each year the editions published by the Society in the Ordinary Series for that year

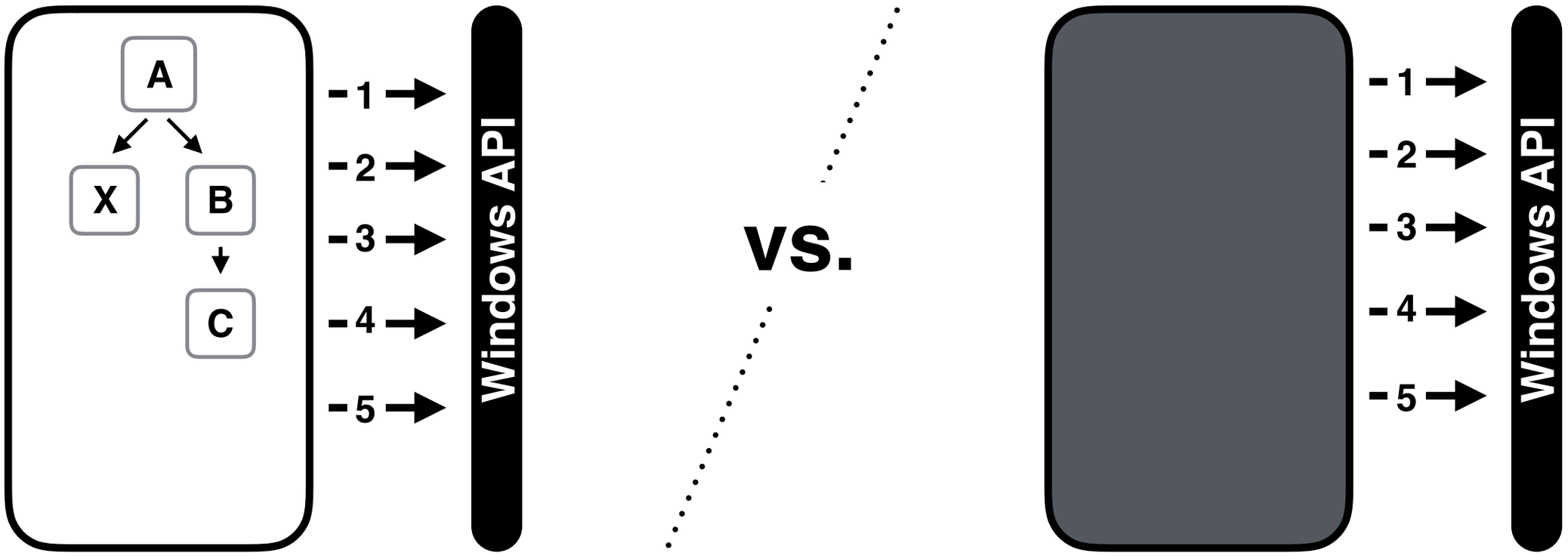
PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2016-09-29 09:56:20
Entry Point	0x000010E4
Number of sections	3

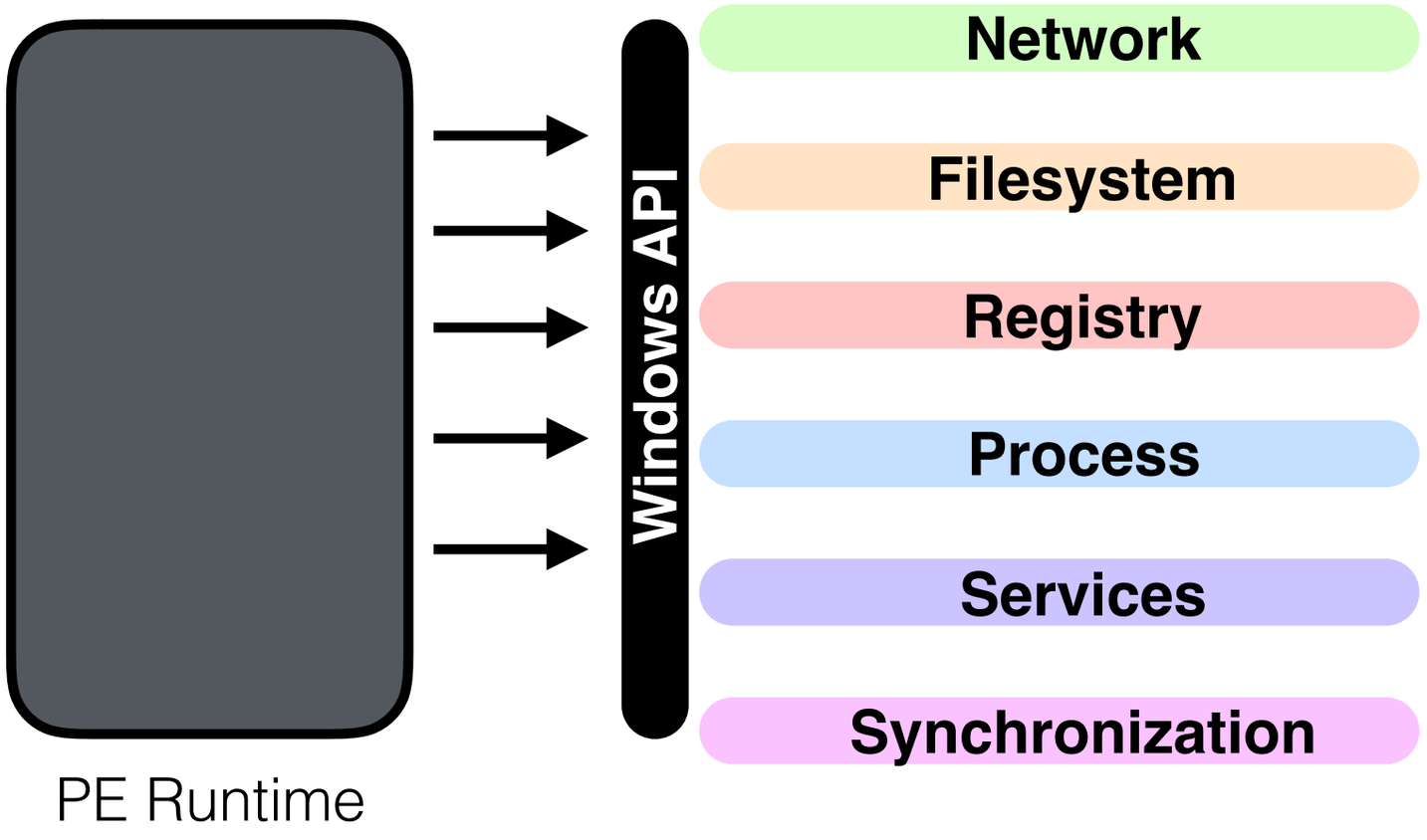
PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	43912	45056	4.59	37fbf8e2fccd2219273765c11b1caa79
.data	49152	12492	0	0.00	d41d8cd98f00b204e9800998ecf8427e

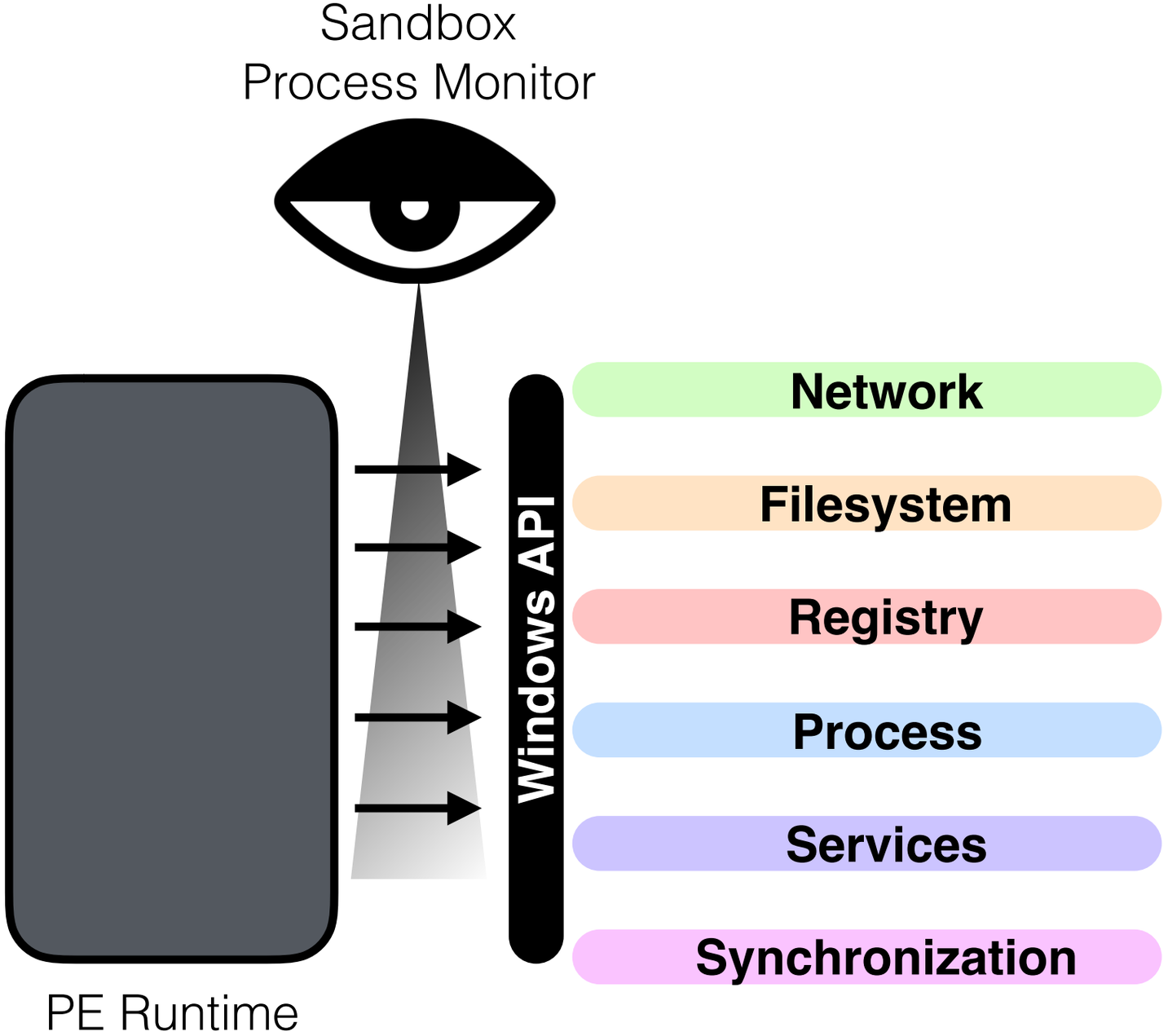
PE Runtime:
The Packer Weakness



The Windows API



Sandbox Basics



PE Dynamic Attributes: Process Overview

- Are any subprocesses created?
- What types of subprocess?
- Do you recognize any unpacker behaviour?

malwr

- 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

PE Dynamic Attributes: Strings From Memory

Strings that have been obfuscated (or strings in packed payloads) may be written to memory as plaintext during execution.

- Registry keys
- File names
- Network artifacts
- Text

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 RSA and AES can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem) http://en.wikipedia.org/w

!!! Your personal identification ID: 32C0D883E1644D0A !!!

!!! Your personal identification ID: 32C0D883E1644D0A !!! !!! IMPORTANT INFORMATION !!!!

!!!!

!!!!_

!This program cannot be run in DOS mode.$

%USERPROFILE%\Desktop_Locky_recover_instructions.txt

-{]@&d

/C del /Q /F "%TEMP%\sysB245.tmp"

Incident Response
Indicators
File Details
Screenshots (12)
Hybrid Analysis (4)
Network Data
Extracted Strings
Extracted Files (13)
Notifications
Community (0)

Back to top

PE Dynamic Attributes:

Process Handles / Mutex

Processes use handles as a way to track/access resources. However a special handle called a “mutex” is often used to signal the presence of the malware and avoid overlapping infections.

- NtCreateMutant

2016-02-16 15:54:39,213	**NtCreateMutant**	Handle: 0x000000d8 InitialOwner: 0 MutexName: CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-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: 0xffffffff	success	0x00000000	

PE Dynamic Attributes:

Accessed / Created Files

- NtCreateFile
- NtOpenFile
- NtQueryInformationFile
- NtReadFile
- NtWriteFile
- DeleteFileW

2016-02-16 15:54:38,783	**NtCreateFile**	ShareAccess: 0 FileName: C:\Documents and Settings\User\Desktop_Locky_recover_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.wikipe	success	0x00000000	

PE Dynamic Attributes:

Registry Keys

- RegCreateKey
- RegDeleteKey
- RegQueryValue
- RegDeleteValue
- RegEnumKey
- RegEnumValue
- RegSetValue
- …

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	

PE Dynamic Attributes:

Network Traffic

- DNS lookup
- GET
- POST

- WSAStartup
- socket
- gethostbyname
- connect
- send
- recv

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

Performs some HTTP requests

The binary likely contains encrypted or compressed data.

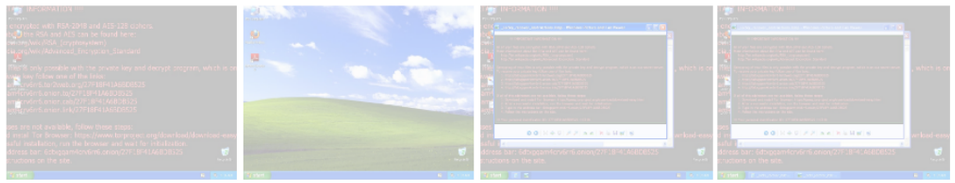
A process attempted to delay the analysis task by a long amount of time.

Steals private information from local Internet browsers

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Installs itself for autorun at Windows startup

Screenshots



Hosts

IP
109.234.38.35

Domains

No domains contacted.

malwr

- 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

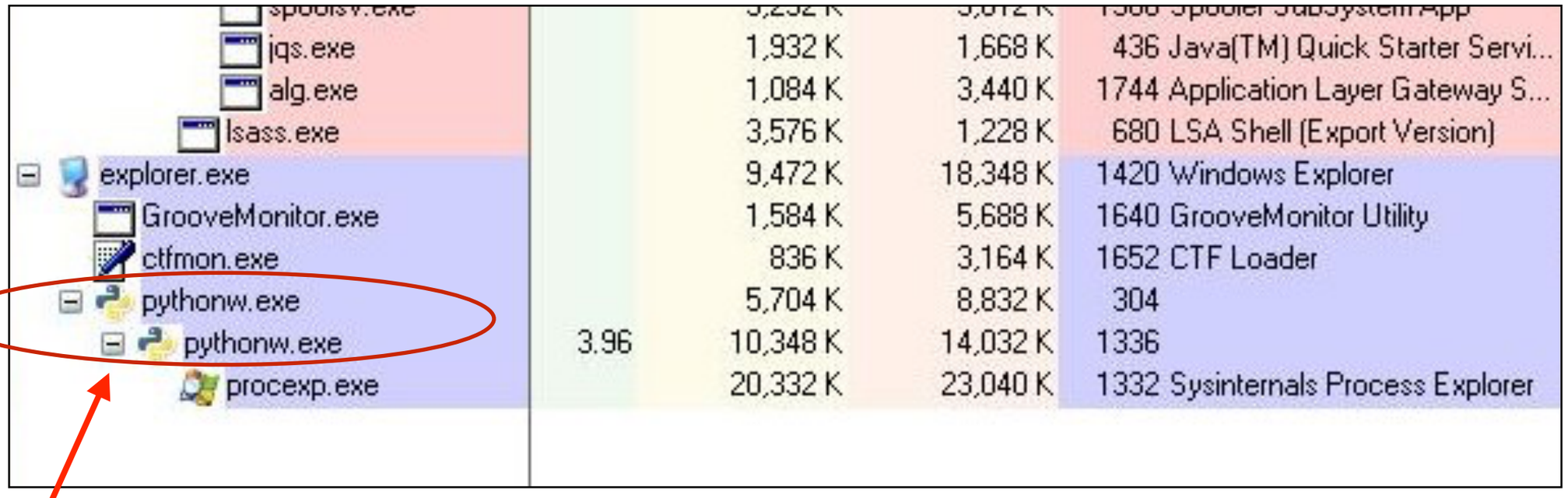
http://109.234.38.35/main.php	`POST /main.php HTTP/1.1`
	`Host: 109.234.38.35`
	`Content-Length: 163713`
	`Connection: Keep-Alive`
	`Cache-Control: no-cache`

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\x0e\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.{\`
	`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\x0f`

Sandboxes We Recommend

Sandbox Warning!



jqs.exe		1,932 K	1,668 K	436 Java(TM) Quick Starter Servi...
alg.exe		1,084 K	3,440 K	1744 Application Layer Gateway S...
lsass.exe		3,576 K	1,228 K	680 LSA Shell (Export Version)
explorer.exe		9,472 K	18,348 K	1420 Windows Explorer
GrooveMonitor.exe		1,584 K	5,688 K	1640 GrooveMonitor Utility
ctfmon.exe		836 K	3,164 K	1652 CTF Loader
pythonw.exe		5,704 K	8,832 K	304
pythonw.exe	3.96	10,348 K	14,032 K	1336
procexp.exe		20,332 K	23,040 K	1332 Sysinternals Process Explorer

????

Sandboxes can be tricked!

Sandbox Warning!

```
VOID AntiCuckoo()
{
        LPDWORD pOld, pFake;

        pFake = (LPDWORD) malloc(4096*100);
        memset(pFake, 1, 4096*100);
        __asm
        {
                mov eax, fs:[0x44]              // save old value
                mov pOld, eax

                mov eax, pFake                  // replace with fake value
                mov fs:[0x44], eax
        }

        // this will not be logged nor executed.
        CreateThread(NULL, 0, (LPTHREAD_START_ROUTINE) Sleep, (LPVOID) 1000, 0, NULL);

        __asm
        {
                mov eax, pOld           // restore old value, not reached if cuckoo
                mov fs:[0x44], eax
        }

        free(pFake);
}
```

Sandboxes can be tricked!

Sandbox Warning!

```
MOV    EAX,564D5868    ; 'VMXh'
MOV    EBX,0           ; Any value but not the MAGIC VALUE
MOV    ECX,0A          ; Get VMWare version
MOV    EDX,5658        ; 'VX' (port number)
IN     EAX,DX          ; Read port
CMP    EBX,564D5868    ; Is there a reply from VMWare?
```

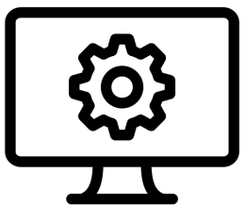
Sandboxes can be tricked!

Sandbox Warning!

```
v7 = v2;
v13 = &v7;
v21 = sub_4011A0(L"VBOX");
v12 = v21;
v26 = 2;
v6 = v3;
v11 = &v6;
*(_DWORD *)v20 = sub_4011A0(L"0");
v10 = *(_DWORD *)v20;
LOBYTE(v26) = 3;
v5 = *(_DWORD *)v20;
v9 = &v5;
v8 = sub_4011A0(L"SYSTEM\\ControlSet001\\Services\\Disk\\Enum");
v26 = -1;
v24 = sub_404AA0(HKEY_LOCAL_MACHINE, v5, v6, v7);
if ( !v24 )
  result = 0;
```

Sandboxes can be tricked!

Document Based Sandbox Evasion

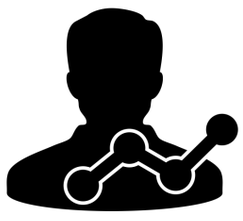


Environment

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

Network

- ASN Details
- Source IP
- Ping as time delay



Anti-Analysis

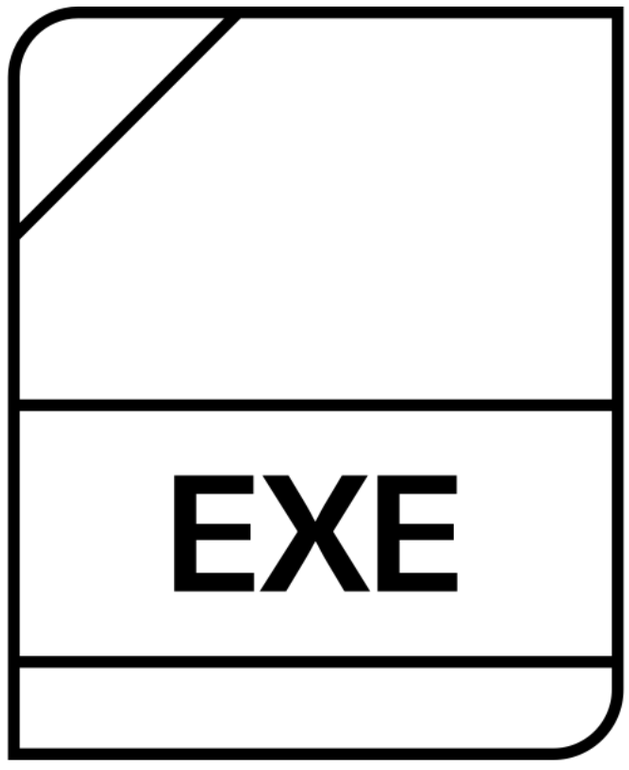
- Specific functionality OO vs Microsoft Office Objects
- Obfuscated payloads
- Payload launch Arguments

Ghetto Runtime Analysis

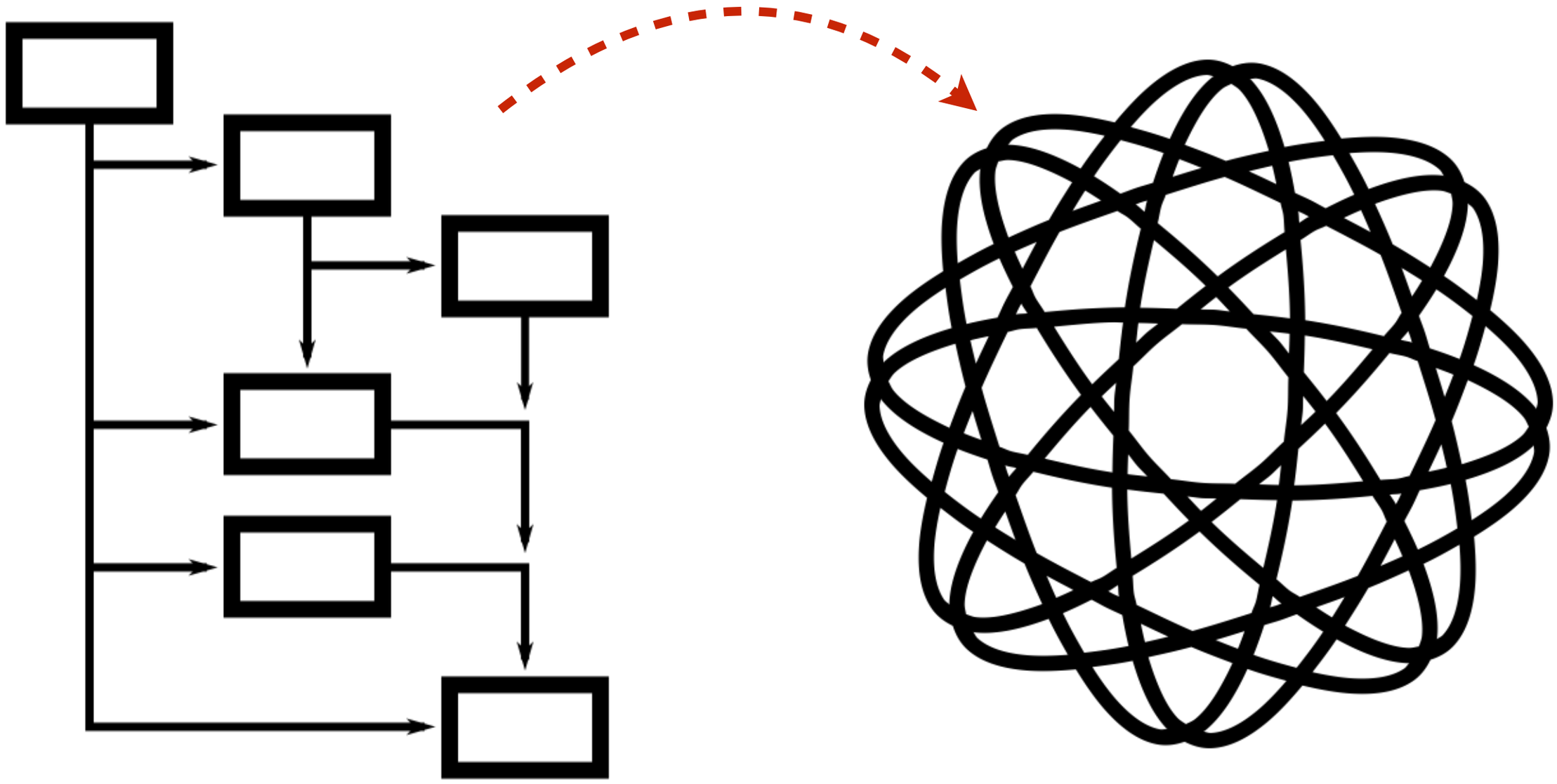
OR

+

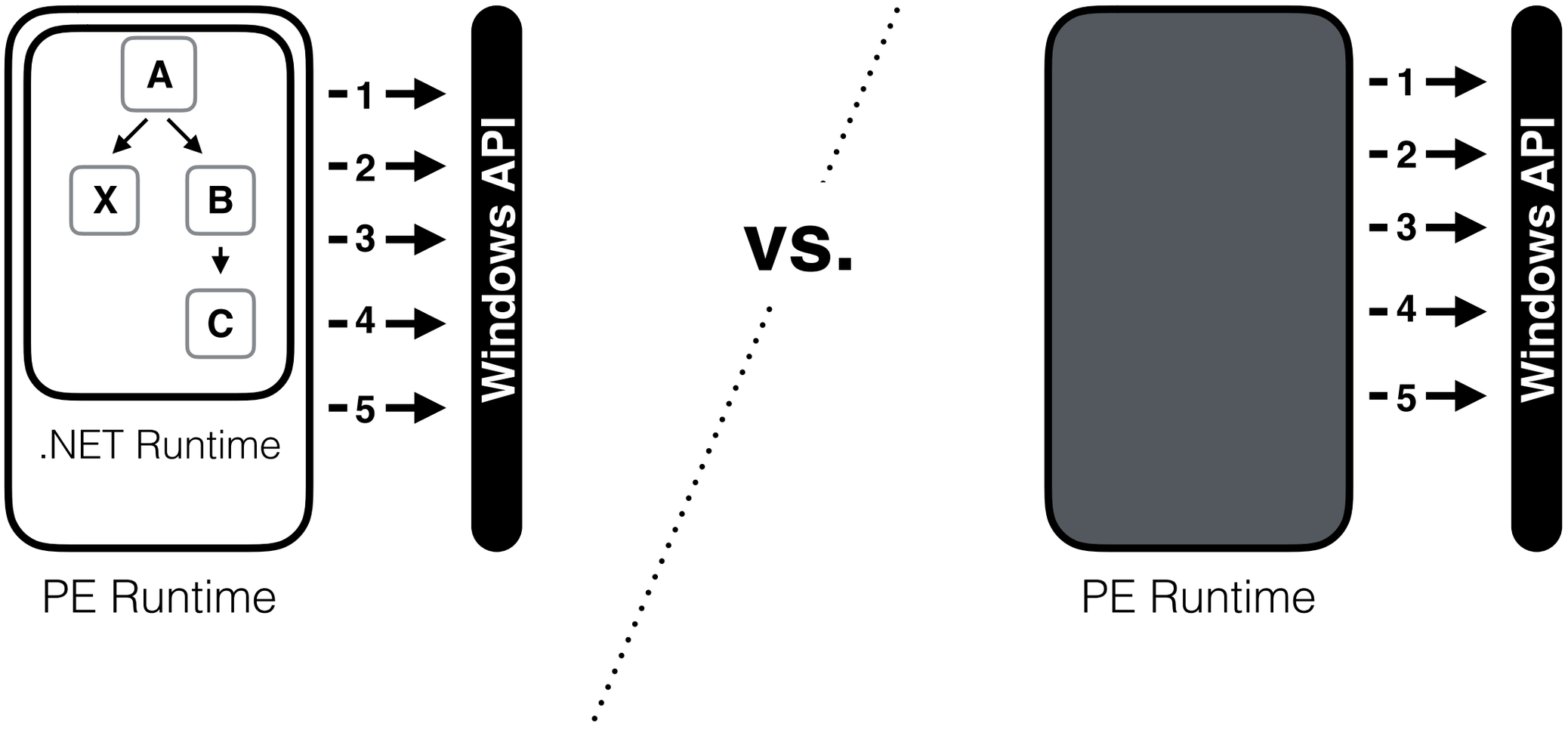
PE (.NET)



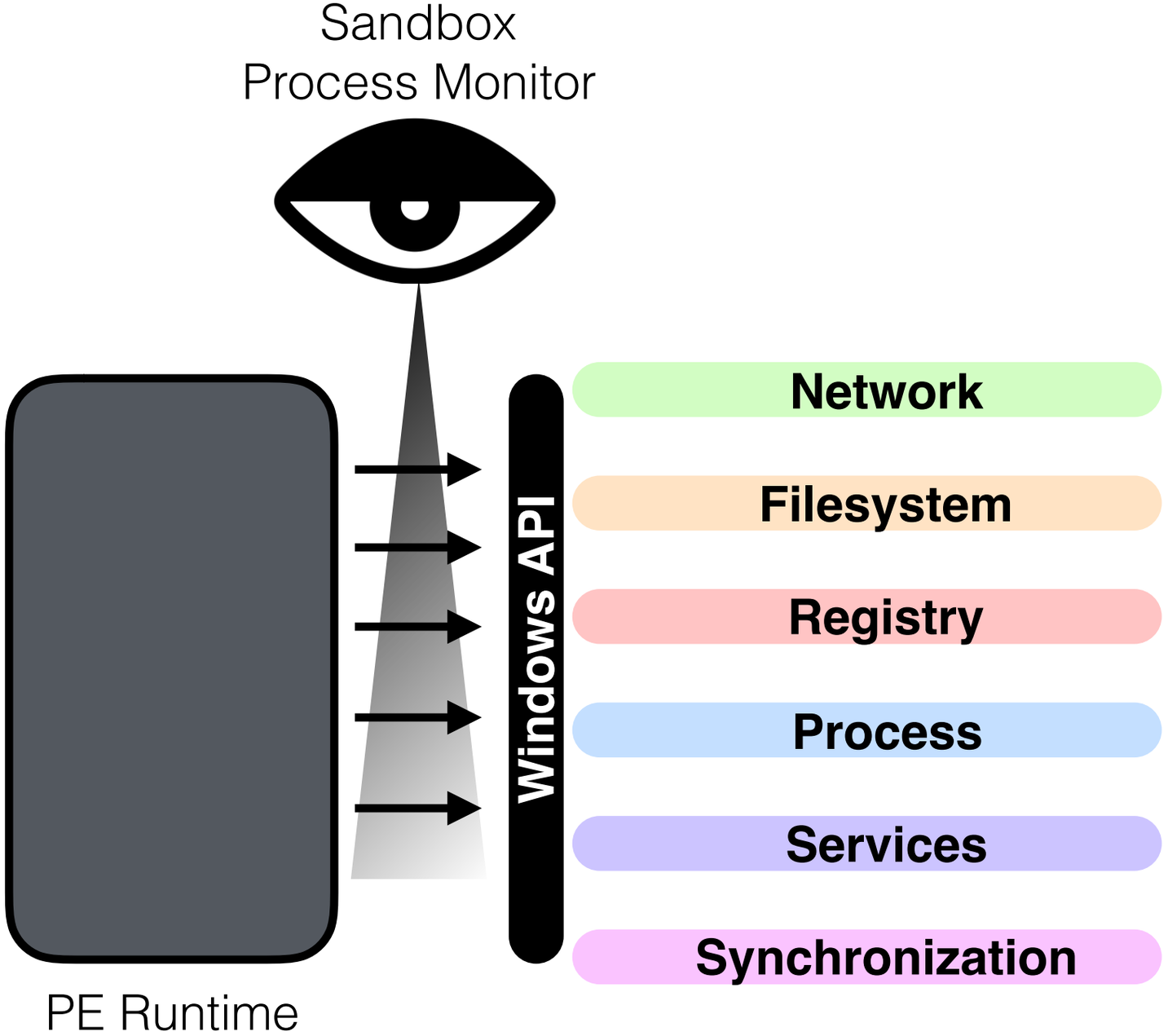
.NET Static Attributes: Obfuscation



.NET Runtime is PE Runtime: Obfuscation Weakness



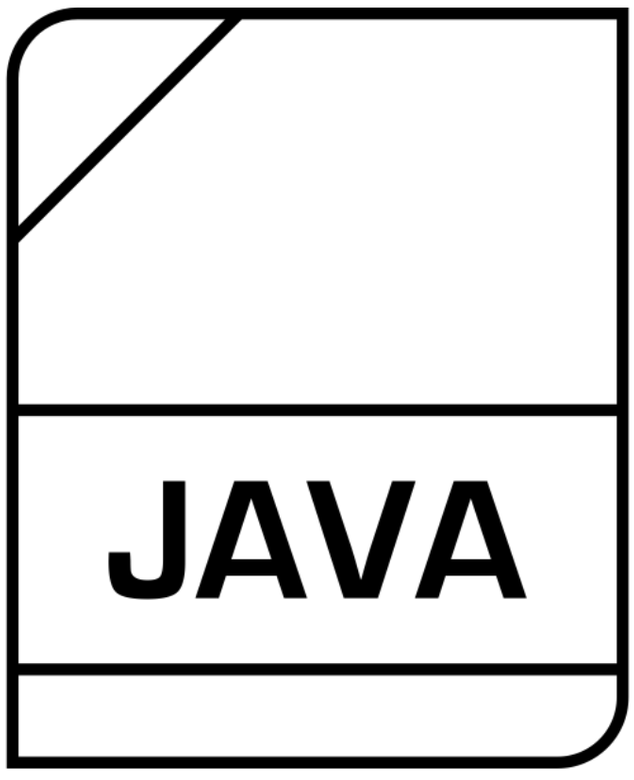
Same Sandbox Basics Apply for .NET



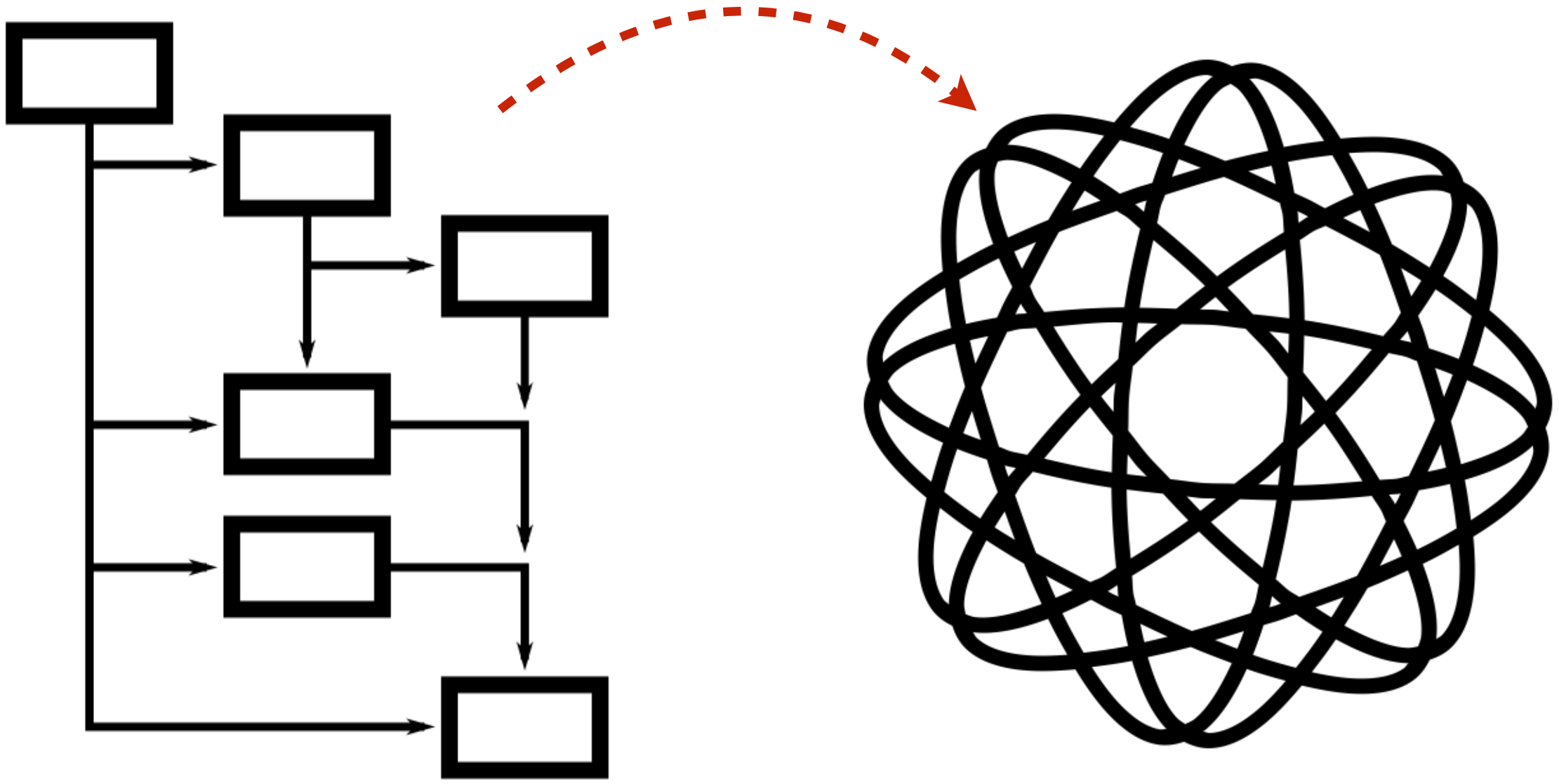
.NET Dynamic Attributes

- strings from memory
- process handles / mutex
- files dropped
- registry keys
- network traffic

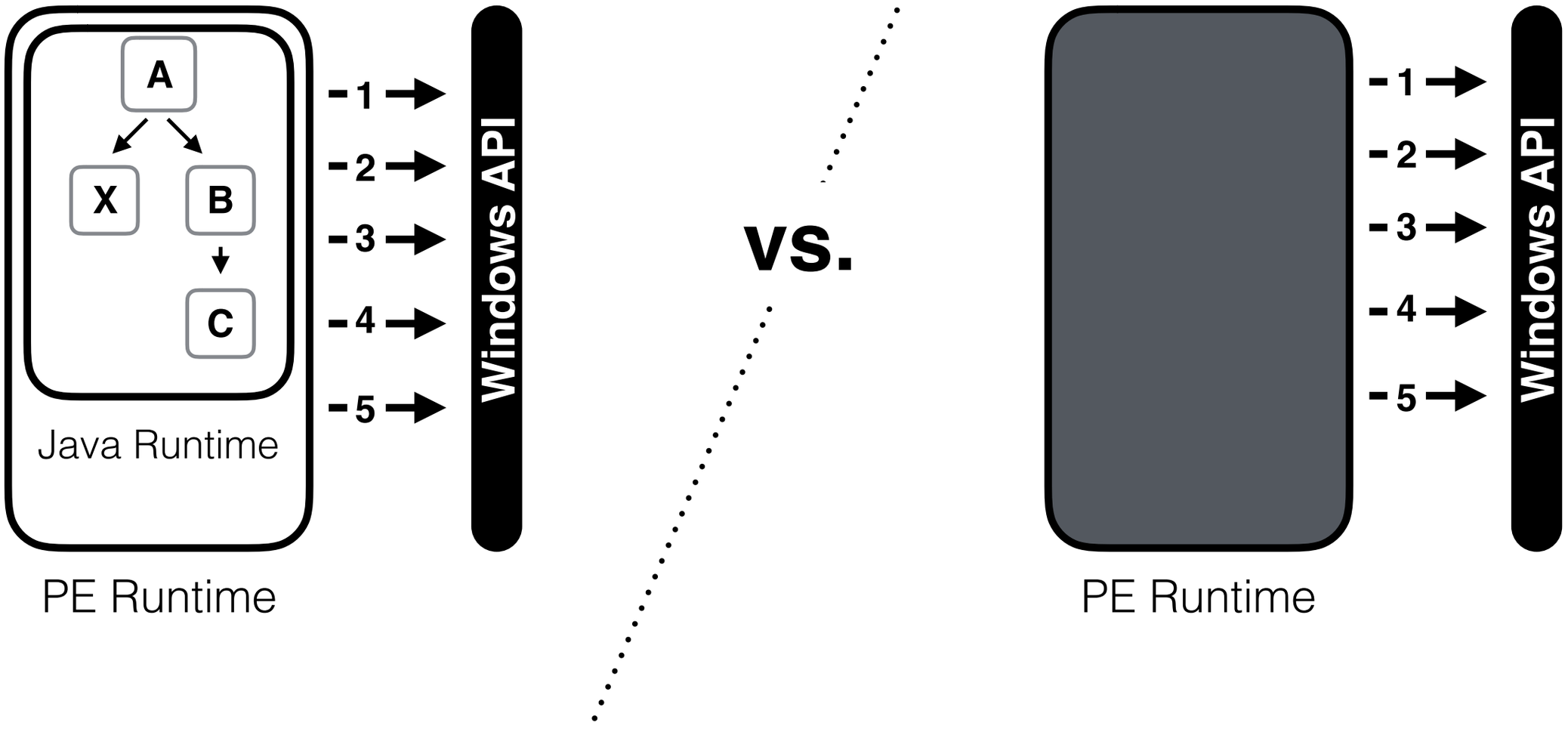
Java



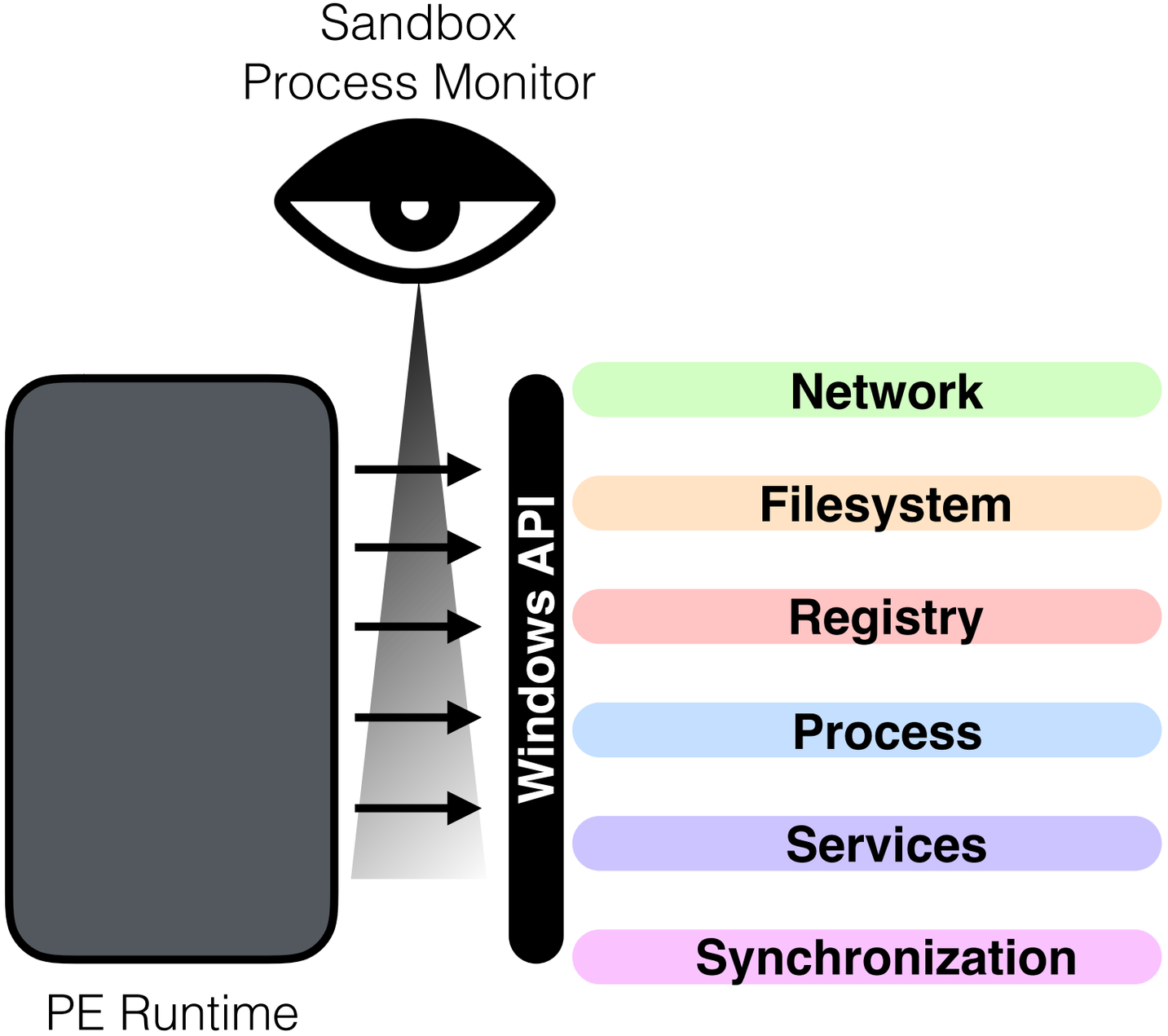
Java Static Attributes: Obfuscation



Java Runtime is PE Runtime: Obfuscation Weakness



Same Sandbox Basics Apply for Java



Java Dynamic Attributes

- strings from memory
- process handles / mutex
- files dropped
- registry keys
- network traffic

Analysis -> Indicators

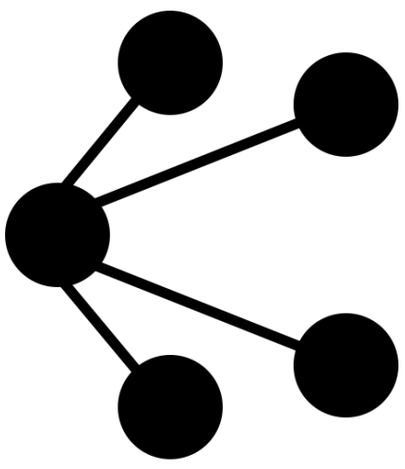
1. Identify the file.

2. Use static analysis tools to collect static attributes

3. Use dynamic analysis tools to collect dynamic attributes

4. Compare dynamic and static attributes to determine the best set of indicators.

Develop Primary IOCs



Collect Your Notes

Choose IOC Format (If Needed)

Prepare To Hunt

Rough Notes Are OK

VS.

Evernote Basic

+ New Note in Traige | New Chat | Search notes

All Notes | Traige

APRIL 2016 1

Maybe Locky

Today MD5: 7d69f3934be22a9bdcf0e20059d6c0a8.zip 109.234.38.35 ==URLS== http://109.234.38.35/main.php _Locky_recover_instruction...

Traige | click to add tags | Share

Created: Apr 29, 2016 Updated: Apr 29, 2016

Maybe Locky

MD5: 7d69f3934be22a9bdcf0e20059d6c0a8.zip

109.234.38.35

==URLS==
http://109.234.38.35/main.php

_Locky_recover_instructions.txt

\\\\?\\Volume{<guid>}\\\

HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Run

Locky" = “%TEMP%\.exe”

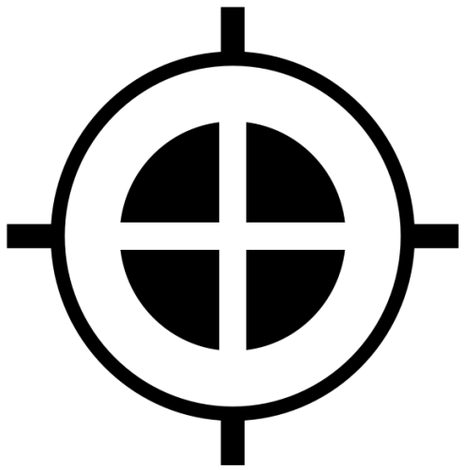
===ref==
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26383/en_US/McAfee_Labs_Threat_Advisory-Ransomware-Locky.pdf

JUST DO IT!!!!!

Workshop

Details in your workbook.

Discovery (Hunting)



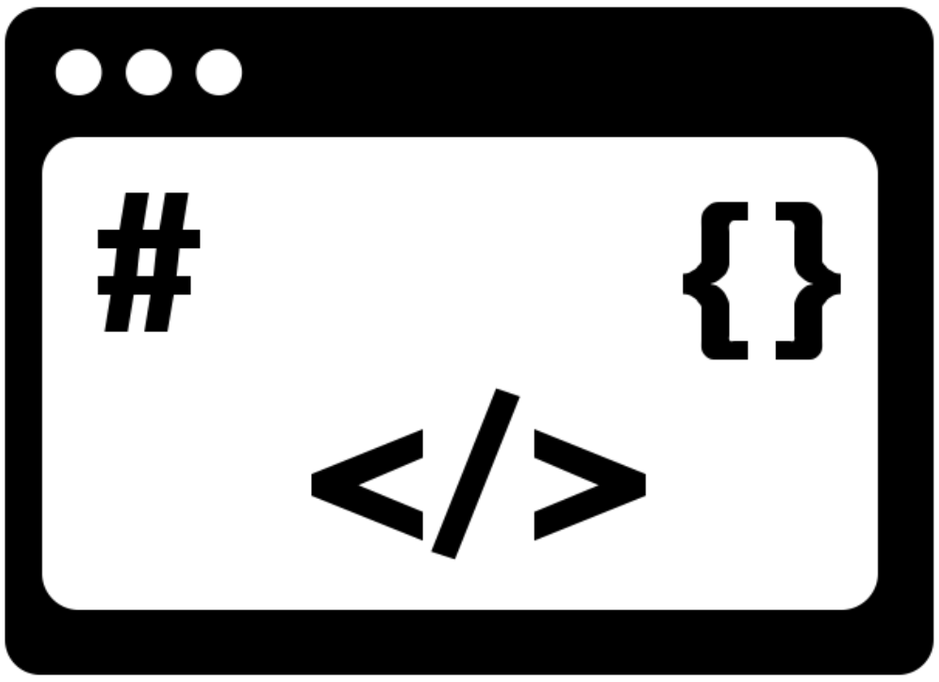
Static Pivots

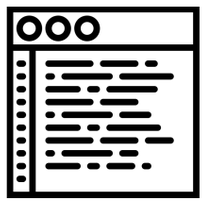
Dynamic Pivots

Sandboxes

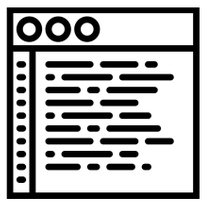
Acquiring Samples

Static Pivots

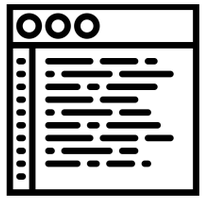




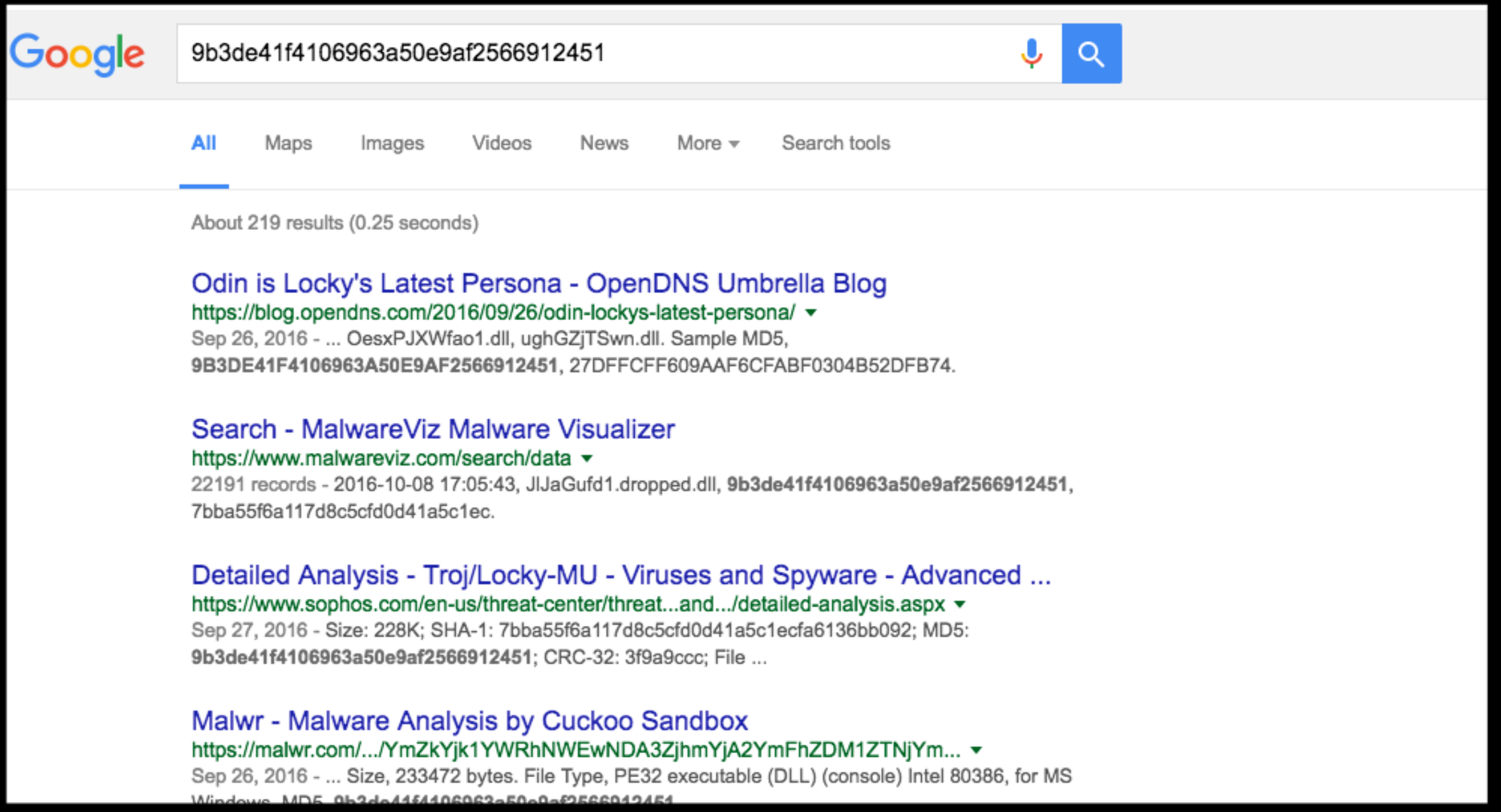
Metadata



Hashing



Strings


Google
9b3de41f4106963a50e9af2566912451
All
Maps
Images
Videos
News
More
Search tools
About 219 results (0.25 seconds)
Odin is Locky's Latest Persona - OpenDNS Umbrella Blog
https://blog.opendns.com/2016/09/26/odin-lockys-latest-persona/
Sep 26, 2016 - ... OesxPJXWfao1.dll, ughGZjTSwn.dll. Sample MD5,
9B3DE41F4106963A50E9AF2566912451, 27DFFCFF609AAF6CFABF0304B52DFB74.
Search - MalwareViz Malware Visualizer
https://www.malwareviz.com/search/data
22191 records - 2016-10-08 17:05:43, JlJaGufd1.dropped.dll, 9b3de41f4106963a50e9af2566912451,
7bba55f6a117d8c5cfd0d41a5c1ec.
Detailed Analysis - Troj/Locky-MU - Viruses and Spyware - Advanced ...
https://www.sophos.com/en-us/threat-center/threat...and.../detailed-analysis.aspx
Sep 27, 2016 - Size: 228K; SHA-1: 7bba55f6a117d8c5cfd0d41a5c1ecfa6136bb092; MD5:
9b3de41f4106963a50e9af2566912451; CRC-32: 3f9a9ccc; File ...
Malwr - Malware Analysis by Cuckoo Sandbox
https://malwr.com/.../YmZkYjk1YWRhNWEwNDA3ZjhmYjA2YmFhZDM1ZTNjYm...
Sep 26, 2016 - ... Size, 233472 bytes. File Type, PE32 executable (DLL) (console) Intel 80386, for MS

virustotal

SHA256: 86d229d219a21ab8092839a4361d30977e56c78f0ada10b6d68363b2834dd1dc

File name: DEVRTL.dll

Detection ratio: 47 / 56

Analysis date: 2016-10-11 09:16:01 UTC (21 hours, 26 minutes ago)

Analysis | File detail | Additional information | Comments 5 | Votes

The file being studied is a Portable Executable file! More specifically, it is a Win32 DLL file for the Windows command line subsystem.

FileVersionInfo properties

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Original name	DEVRTL.DLL
Internal name	DEVRTL.dll
File version	6.1.7601.17621 (win7sp1_gdr.110523-2108)
Description	Device Management Run Time Library

Malware Indicator & Sandbox Search

"Device Management Run Time Library"

About 251 results (0.20 seconds)

Sort by: Date

powered by Google™ Custom Search

Did you mean: "Device Management ***Runtime*** Library"

Servicio gratuito automatizado de análisis de malware, con ...
https://www.hybrid-analysis.com/.../ 54665e8c581183bbc4bedf9ead343fa2be1167ce3d...
Oct 2, 2016 ... ... Operating System; ProductVersion: 6.1.7601.17621; FileDescription: **Device Management Run Time Library**; OriginalFilename: DEVRTL.

TBAR80616.wsf - Free Automated Malware Analysis Service ...
https://www.hybrid-analysis.com/.../ fef71cfb495dc6c9a2e91138590aa3f0f37028292802d5a17794734411864...
Sep 28, 2016 ... ... Operating System; ProductVersion: 6.1.7601.17621; FileDescription: **Device Management Run Time Library**; OriginalFilename: DEVRTL.

Document No 4358794733.zip - Free Automated Malware Analysis ...
https://www.hybrid-analysis.com/.../ 7b6ca17b613e3771dbfd8db7576a577467312bfa0a0909015980edc48de2...
Sep 27, 2016 ... ... Operating System; ProductVersion: 6.1.7601.17621; FileDescription: **Device Management Run Time Library**; OriginalFilename: DEVRTL.

RFS41809.wsf
https://www.hybrid-analysis.com/.../ 80623b5f72c21faa5fdcc4e6fa937dc4c28f24cd100ff08bac42b1ec8a1079e...
Sep 27, 2016 ... ... Operating System; ProductVersion: 6.1.7601.17621; FileDescription: **Device Management Run Time Library**; OriginalFilename: DEVRTL.

... VxStream خدمة تحليل البرامج الضارة المؤتمتة المجانية - مشغلة بواسطة
https://www.hybrid-analysis.com/.../ 0e0cef2fdbccf410e238dc4a9fa7c5b04e674d76a2e78708854ffa5e1...
Sep 27, 2016 ... ... Operating System; ProductVersion: 6.1.7601.17621; FileDescription: **Device Management Run Time Library**; OriginalFilename: DEVRTL.

Malwr - Malware Analysis by Cuckoo Sandbox

Locky Rannoh Trojan renames files to .odin

Posted 2 weeks ago by stuza

#malware

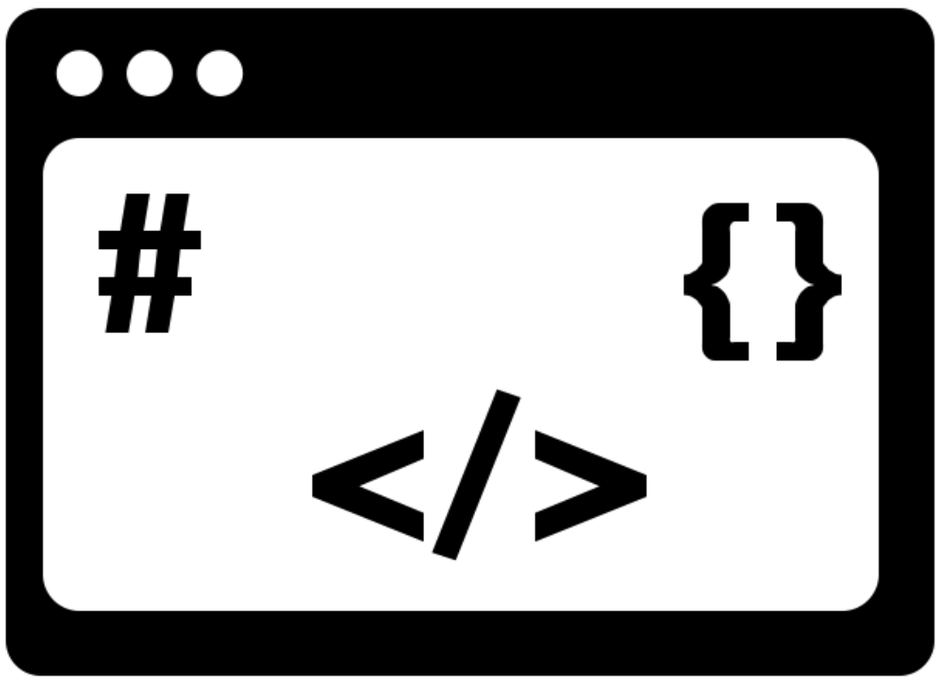
Posted 2 weeks ago by paulch

submitname:"86d229d219a21ab8092839a4361d30977e56c78f0ada10b6d68363b2834dd1dc"
vxstream-threatscore:58/100
memurl:"Pattern match: http://msdl.microsoft.com/download/symbols"
memip:"Heuristic match: 6.1.7601.17621 (win7sp1_gdr.110523-2108),Heuristic match: 6.1.7601.17621"
source:https://www.hybrid-analysis.com/sample/86d229d219a21ab8092839a4361d30977e56c78f0ada10b6d68363b2834dd1dc?environmentId=100

Posted 2 weeks, 1 day ago by PayloadSecurity

https://myonlinesecurity.co.uk/locky-ransomware-changed-now-a-odin-extension/

Dynamic Pivots



- Persistence
- Communication
- Runtime Characteristics

Dynamic Pivots Common

Persistence

- Registry
- Services
- Tasks
- Handler

Communication

- Hostnames
- URL Paths & Parameters
- Characteristics (TCP, HTTP(s) …)

Runtime

- Mutex
- Functionality
- Pipes
- Process Hooks

A process attempted to delay the analysis task by a long amount of time.

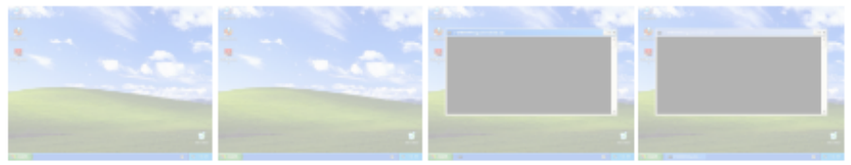
Steals private information from local Internet browsers

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Installs itself for autorun at Windows startup

process: None
signs: [{u'type': u'registry', u'value': u'HKEY_USERS\\S-1-5-21-1547161642-507921405-839522115-1004\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon'}]
process: None
signs: [{u'type': u'registry', u'value': u'HKEY_LOCAL_MACHINE\\system\\CurrentControlSet\\services\\RDPNP\\NetworkProvider'}]
process: None
signs: [{u'type': u'file', u'value': u'c:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Startup'}]

Screenshots

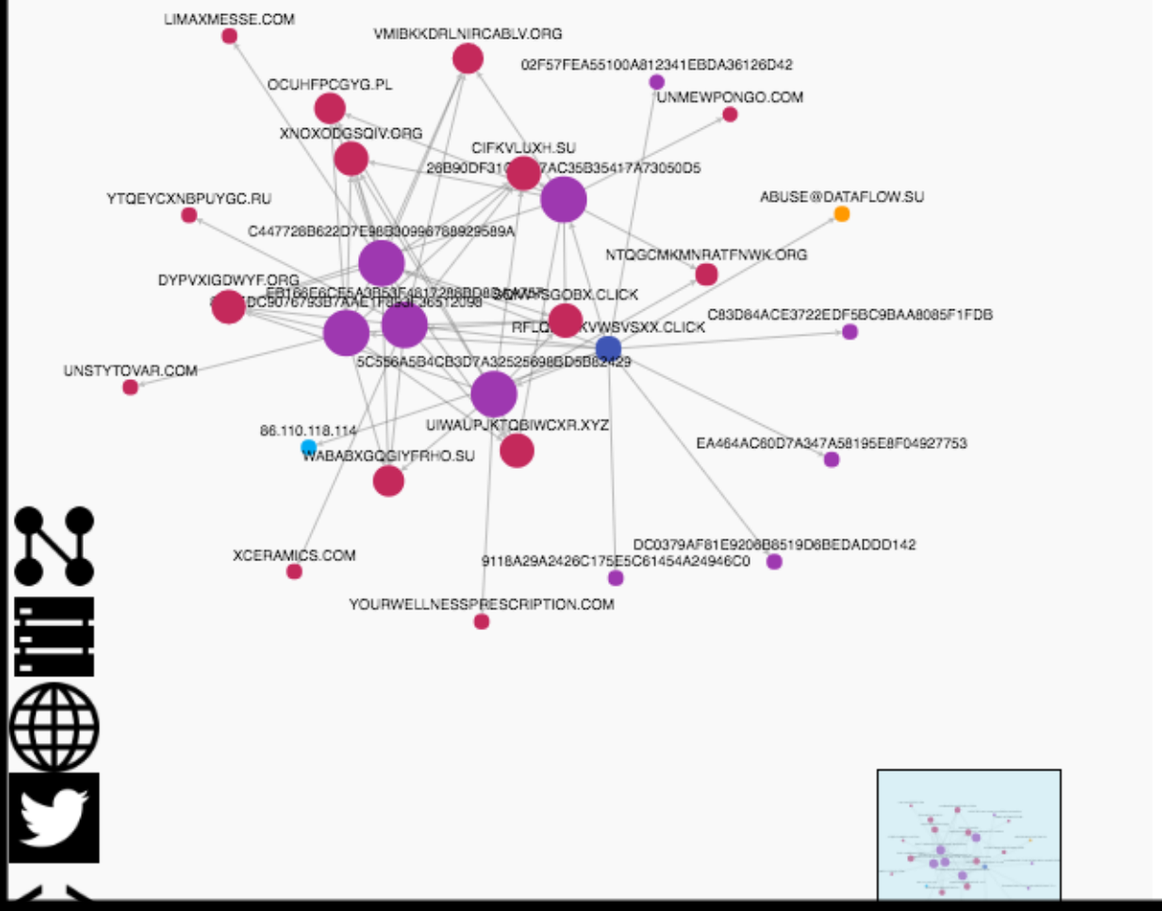


Hosts

IP
46.22.145.37
210.1.58.21
5.133.180.130
62.173.154.240
5.196.200.247
86.110.118.114

Domains

DOMAIN	IP
ict-net.com	46.22.145.37
www.ict-net.com	46.22.145.37
networkthai.org	210.1.58.21
residencyradio.com	5.133.180.130
wababxgqgiyfrho.su	
yxmagrdetpr.biz	
cifkvluxh.su	
rflqjuckvwsvsxx.click	86.110.118.114



DOMAIN > RFLQJUCKVWSVSXX.CLICK

Is this malicious? Yes No

FILES THAT TALK TO RFLQJUCKVWSVSXX.CLICK

MD5	A/V
eb166e6ce5a3b53f4817288bd8daa757	
c447728b622d7e98b30996788929589a	
5c556a5b4cb3d7a32525698bd5b82429	
8d9edc9076793b7aae1f893f36512098	
26b90df31c1b87ac35b35417a73050d5	
02f57fea55100a812341ebda36126d42	
9118a29a2426c175e5c61454a24946c0	
c83d84ace3722edf5bc9baa8085f1fdb	
dc0379af81e9206b8519d6bedaddd142	
ea464ac60d7a347a58195e8f04927753	
bf0a2782445804372b22242f0259a83c	
c23efc3e2e98c65562c375bda261c433	
4f2259013e37110ad0c2fe9fdab41b74	

RISKIQ

PASSIVE TOTAL | BULK UPLOAD | HELP | CONTACT US

API | Solutions | Learn | Blog | My Account | Logout

Search for a domain, IP, email, SSL certificate hash or tag...

rflqjuckvwsvsxx.click

ATTRIBUTES

First Seen	2016-09-26 11:35:44
Last Seen	2016-10-10 12:28:11
Resolutions	1
Primary	rflqjuckvwsvsxx.click
TLD	
Ever Compromised?	true / false
Dynamic DNS	true / false
Classify	malicious / suspicious / non-malicious / unknown
Monitor	

TAGS

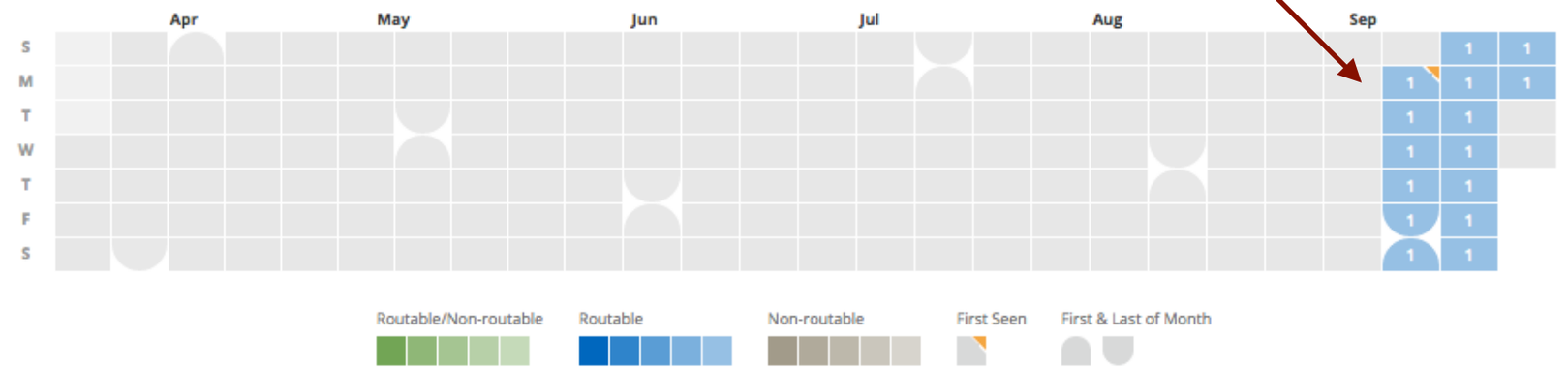
Consider tagging domains and IPs in order to remember small details like if it were suspicious or compromised!

recently-registered | hashes | active

Add tag... +

UNIQUE (1) COPY

Heatmap | WHOIS | OSINT 5 | Hashes 3



Select a date or dates *(shift-click)* on the Heatmap to filter results.

copy

Resolve	Location	Network	First	Last	Source	Tags
86.110.118.114	RU	86.110.116.0/22	2016-09-26 11:35:44	2016-10-10 12:28:11	mnemonic, emerging_threats, virustotal, kaspersky, riskiq	

malicious | suspicious | non-malicious | unknown | add tag... +

« 1 »

1 of 1

* some sources failed to respond to our query request

Search for a domain, IP, email, SSL certificate hash or tag...

rflqjuckvwsvsxx.click

ATTRIBUTES

First Seen	2016-09-26 11:35:44
Last Seen	2016-10-10 12:28:11
Resolutions	1
Primary	rflqjuckvwsvsxx.click
TLD	
Ever Compromised?	true / false
Dynamic DNS	true / false
Classify	malicious / suspicious / non-malicious / unknown
Monitor	

TAGS

Consider tagging domains and IPs in order to remember small details like if it were suspicious or compromised!

recently-registered hashes active

Add tag... +

UNIQUE (1) copy

Heatmap WHOIS OSINT 5 Hashes 3

Source	Link	Tags
malware-traffic-analysis.net	http://malware-traffic-analysis.net/2016/09/26/index4.html	search-engine, malware-traffic-analysis
blog.dynamoo.com	http://blog.dynamoo.com/2016/09/malware-spam-attachedscan70-and-others.html	search-engine, dynamoo
hosts-file.net	https://hosts-file.net/hphosts-partial.txt	search-engine, hosts-file
blog.dynamoo.com	http://blog.dynamoo.com/	search-engine, dynamoo
blog.dynamoo.com	http://blog.dynamoo.com/2016_09_01_archive.html	search-engine, dynamoo

Select a date or dates *(shift-click)* on the Heatmap to filter results.

copy

Resolve	Location	Network	First	Last	Source	Tags
86.110.118.114	RU	86.110.116.0/22	2016-09-26 11:35:44	2016-10-10 12:28:11	mnemonic, emerging_threats, virustotal, kaspersky, riskiq	

malicious suspicious non-malicious unknown add tag... +

« 1 »

1 of 1

* some sources failed to respond to our query request

RISKIQ

PASSIVE TOTAL BULK UPLOAD HELP CONTACT US

API Solutions Learn Blog My Account Logout

Search for a domain, IP, email, SSL certificate hash or tag...

rflqjuckvwsvsxx.click

ATTRIBUTES

First Seen	2016-09-26 11:35:44
Last Seen	2016-10-10 12:28:11
Resolutions	1
Primary	rflqjuckvwsvsxx.click
TLD	
Ever Compromised?	true / false
Dynamic DNS	true / false
Classify	malicious / suspicious / non-malicious / unknown
Monitor	

TAGS

Consider tagging domains and IPs in order to remember small details like if it were suspicious or compromised!

recently-registered hashes active

Add tag... +

UNIQUE (1) copy

Heatmap WHOIS OSINT 5 Hashes 3

Source	Sample	copy
Emerging Threats (Proofpoint)	f979f3be3c83224dde216d68e397e16d	
Emerging Threats (Proofpoint)	e3b75ac09ecff8285afd0a02eddd2c9e	
Emerging Threats (Proofpoint)	335544e4d437281be533bbf7712c57fa	

Select a date or dates *(shift-click)* on the Heatmap to filter results.

copy

Resolve	Location	Network	First	Last	Source	Tags
86.110.118.114	RU	86.110.116.0/22	2016-09-26 11:35:44	2016-10-10 12:28:11	mnemonic, emerging_threats, virustotal, kaspersky, riskiq	

malicious suspicious non-malicious unknown add tag... +

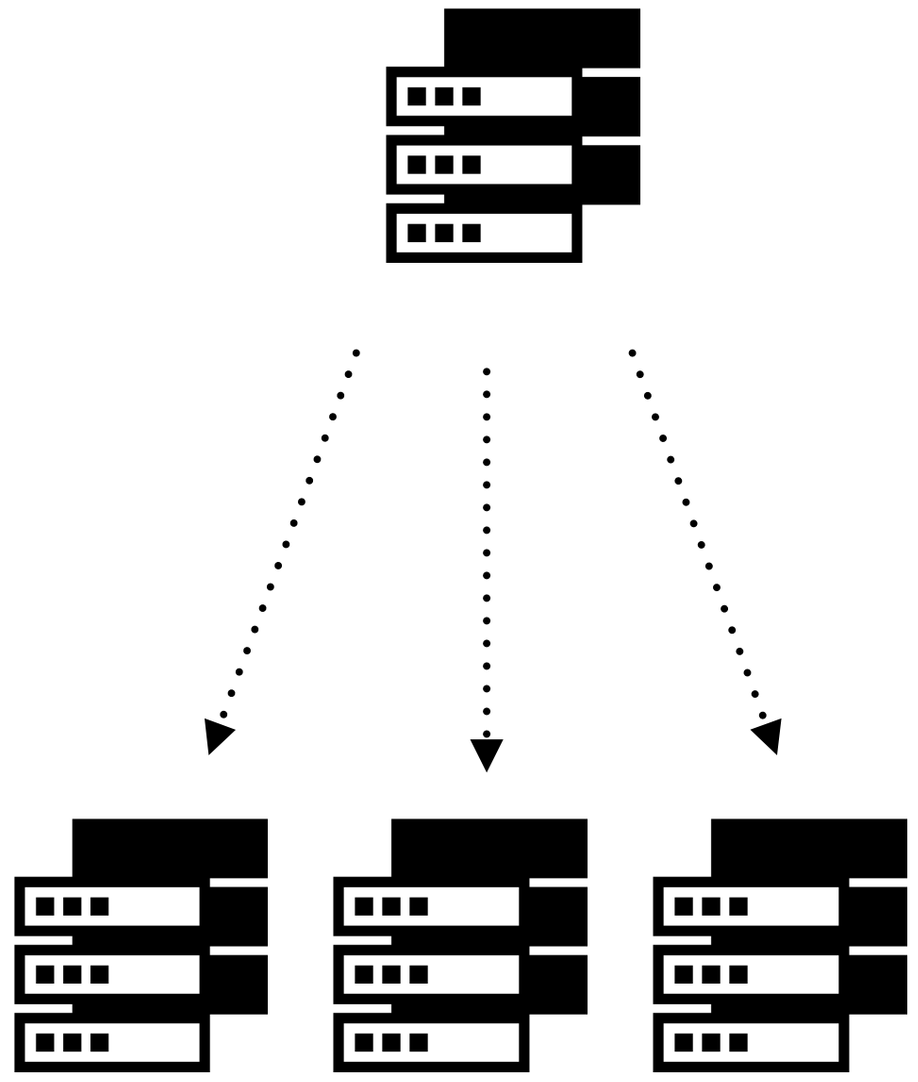
« 1 »

1 of 1

* some sources failed to respond to our query request

~~Online~~ SandBoxes

- Shared Virtualization Infrastructure
- Shared Templates
- Hunting using computed Values



dV8K7R5hEh8Mb6

About 5 results (0.22 seconds)

Sort by: **Relevance**

powered by Google™ Custom Search

[Malwr - Malware Analysis by Cuckoo Sandbox]
https://malwr.com/.../ MDQwZDBmYTZkODllNDYwMWFjNTJiNWVlODhkMWExNTM...
1 hour ago **...** ... AntiVirus on VirusTotal as malicious. Performs some HTTP requests. process: None. signs: [{u'type': u'http', u'value': {u'count': 1, u'body': ...

[Malwr - Malware Analysis by Cuckoo Sandbox]
https://malwr.com/.../ YWViOGIyMGZkZWY0NDVlZThjMmE2ODhiNDAwZjRmNTk/

Mar 28, 2016 **...** signs: [{u'type': u'http', u'value': {u'count': 1, u'body': u'', u'uri': u'http:// pockettypewriter.co.uk/765f46vb.exe', u'user-agent': u'Mozilla/4.0 ...

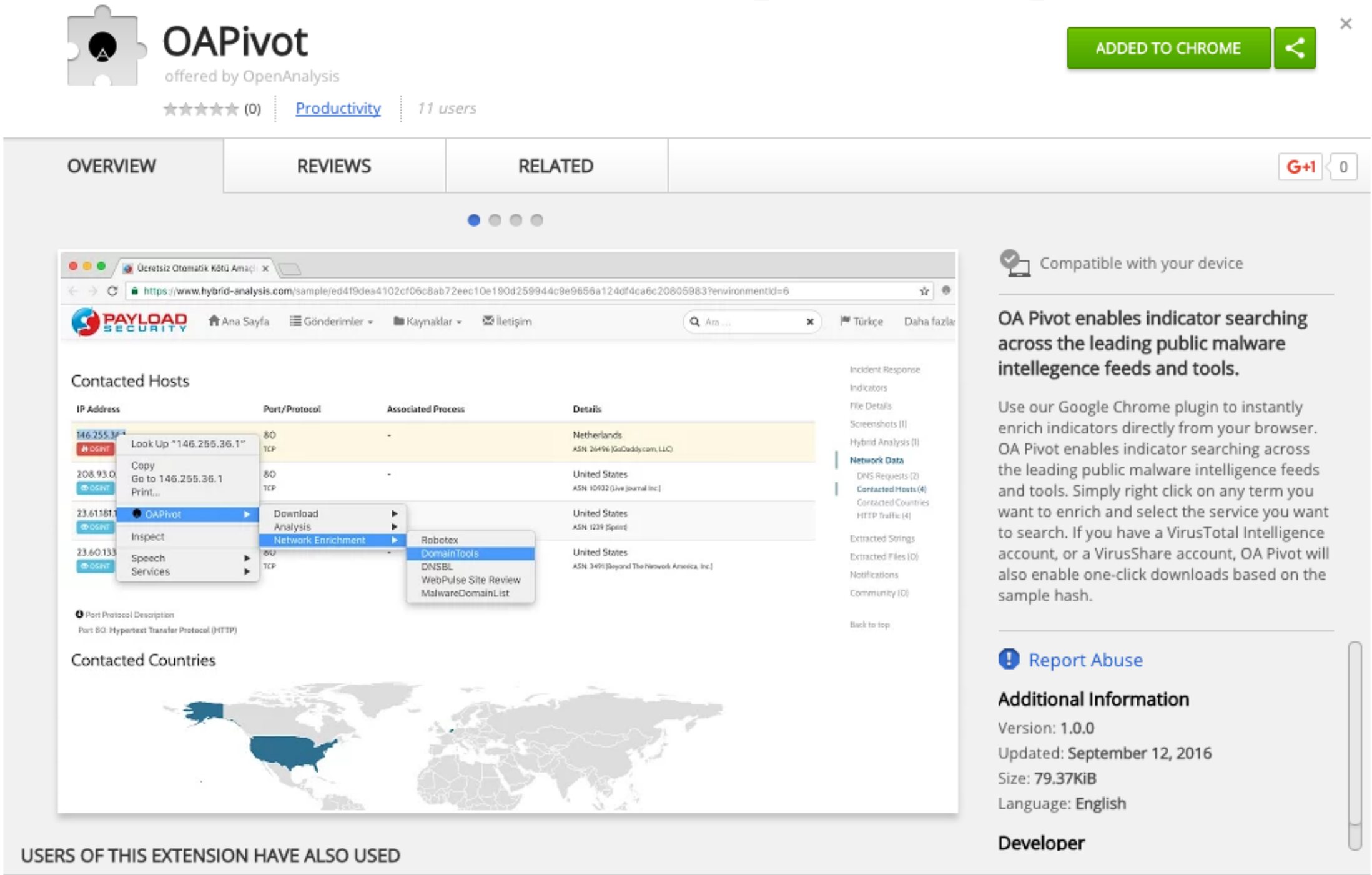
[Malwr - Malware Analysis by Cuckoo Sandbox]
https://malwr.com/.../ MTQ0YmFlNmYyYjMwNGI1OGI5MDc1MzI5NjM1ZDg2ZDY/
Mar 22, 2016 **...** signs: [{u'type': u'http', u'value': {u'count': 1, u'body': u'', u'uri': u'http://mmworld.eu/ op3z8e', u'user-agent': u'Mozilla/4.0 (compatible; MSIE 6.0; ...

[Analysis]
https://malwr.com/.../ ZjUxYmUwMGFlNDJlNGMxNTkwNDkzZjE0YjcxNTNjZTQ/
Mar 29, 2016 **...** signs: [{u'type': u'api', u'value': {u'category': u'filesystem', u'status': True, u'return': u' 0x00000000', u'timestamp': u'2016-03-29 12:02:55,788', ...

[23]
https://malwr.com/.../ ODYzMWY5ZTVmMDhiNGUyNGEzOWJlOTJmMDg5OGJjNjM/

Mar 24, 2016 **...** HKEY_CURRENT_USER\Software**dV8K7R5hEh8Mb6**. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName

Mining Open Data The Easy Way



Discovery (Pivots)

Search Engines - Google!	AlienVault OTX
PassiveTotal	ThreatMiner
ThreatCrowd	HybridAnalysis
malc0de	ShadowServer
VirusTotal	TotalHash

Discovery (Network Enrichment)

DomainTools

Robotex

DNSBL

WebPulse Site Review

MalwareDomainList

URLQuery

Downloading Samples

Discovery (Downloading)

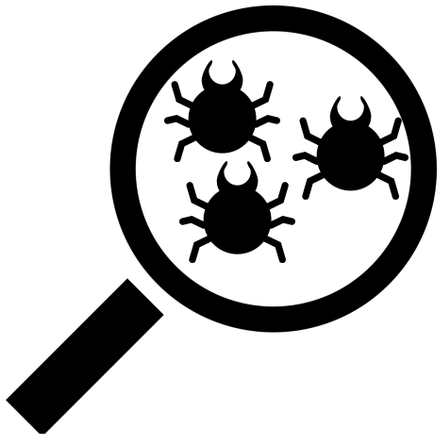
Malwr	Requires Registration (free)	Requires Uploader Shares Sample
HybridAnalysis	Requires Registration (free)	Requires Uploader Shares Sample
VirusShare	Requires Registration (free)	Requires Sample has been indexed
VirusTotal	Requires Account (Paid)	Need Account

JUST DO IT!!!!!

Workshop

Details in your workbook.

Comparative Analysis

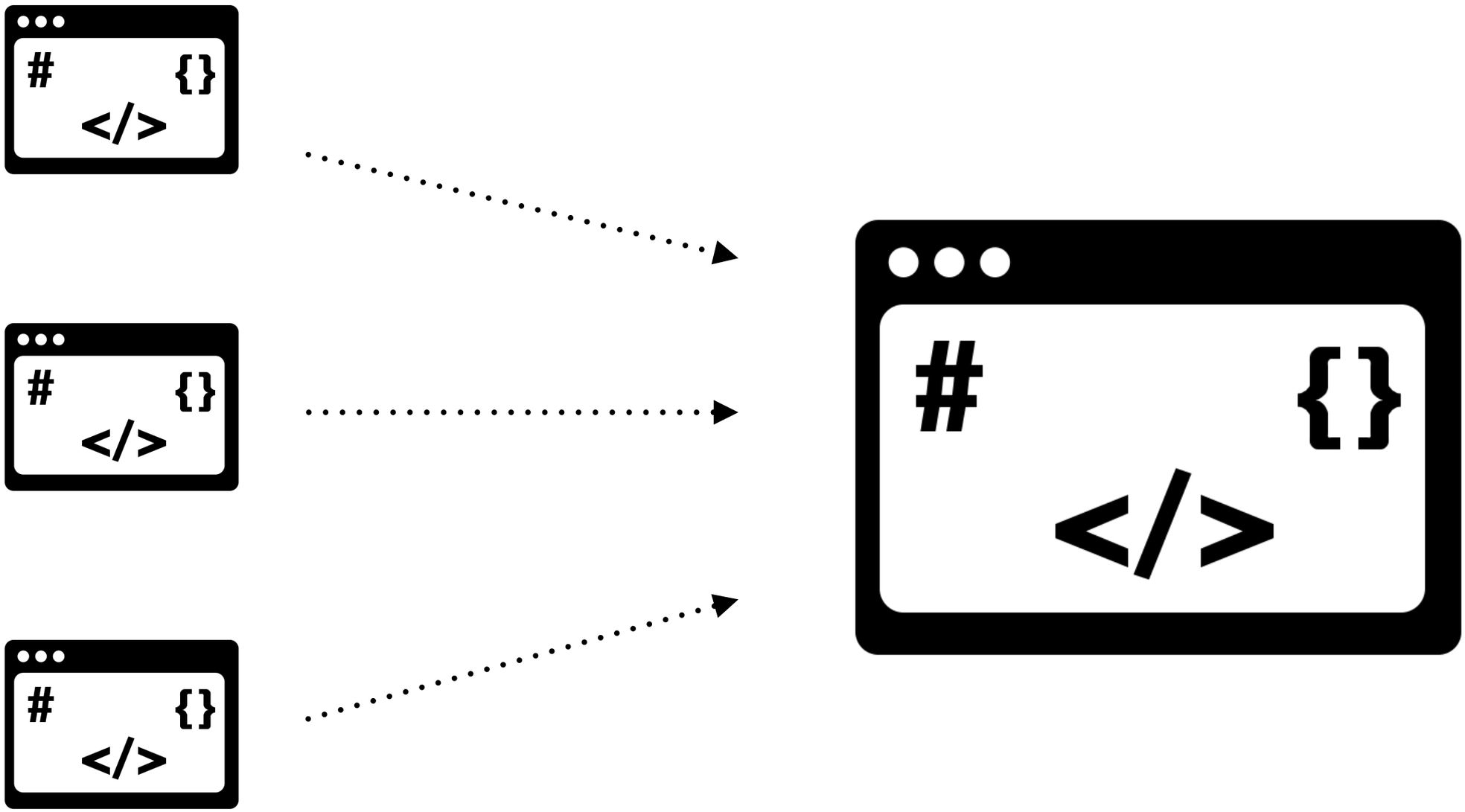


Identify common characteristics

Common Properties

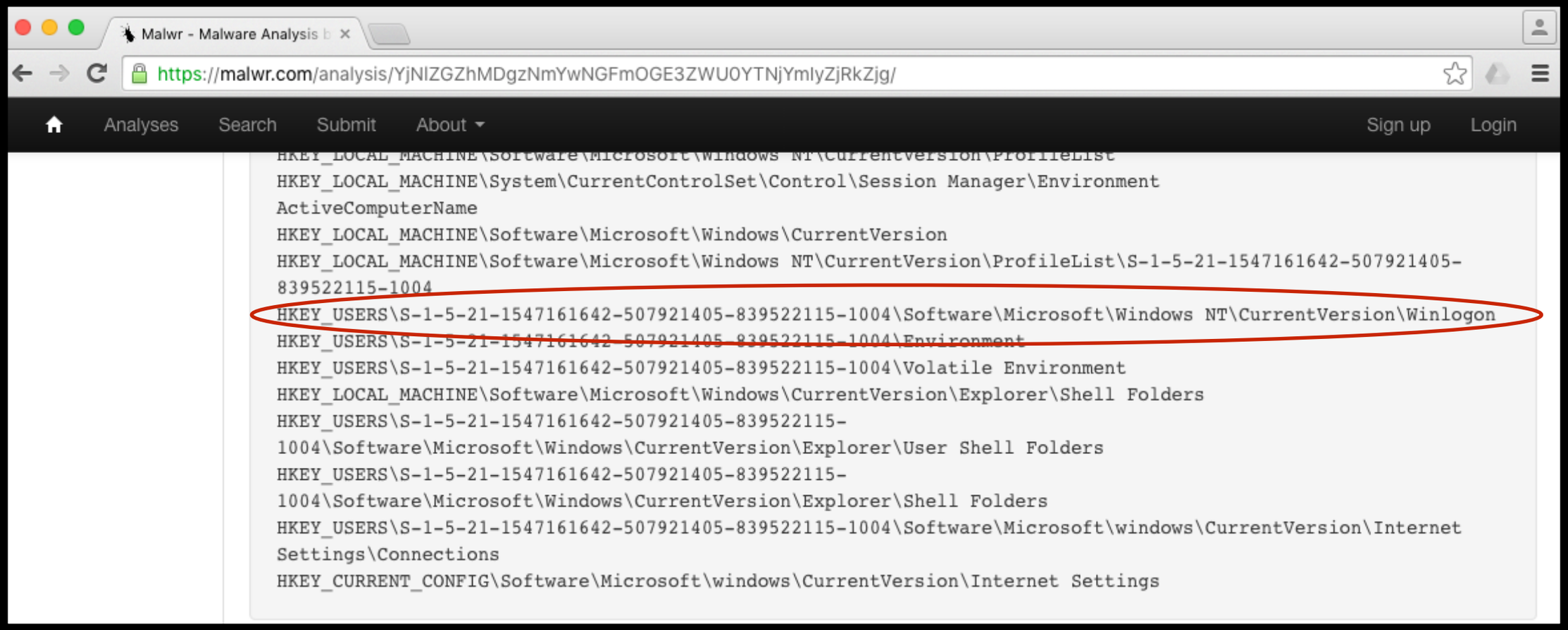
Common Behaviour

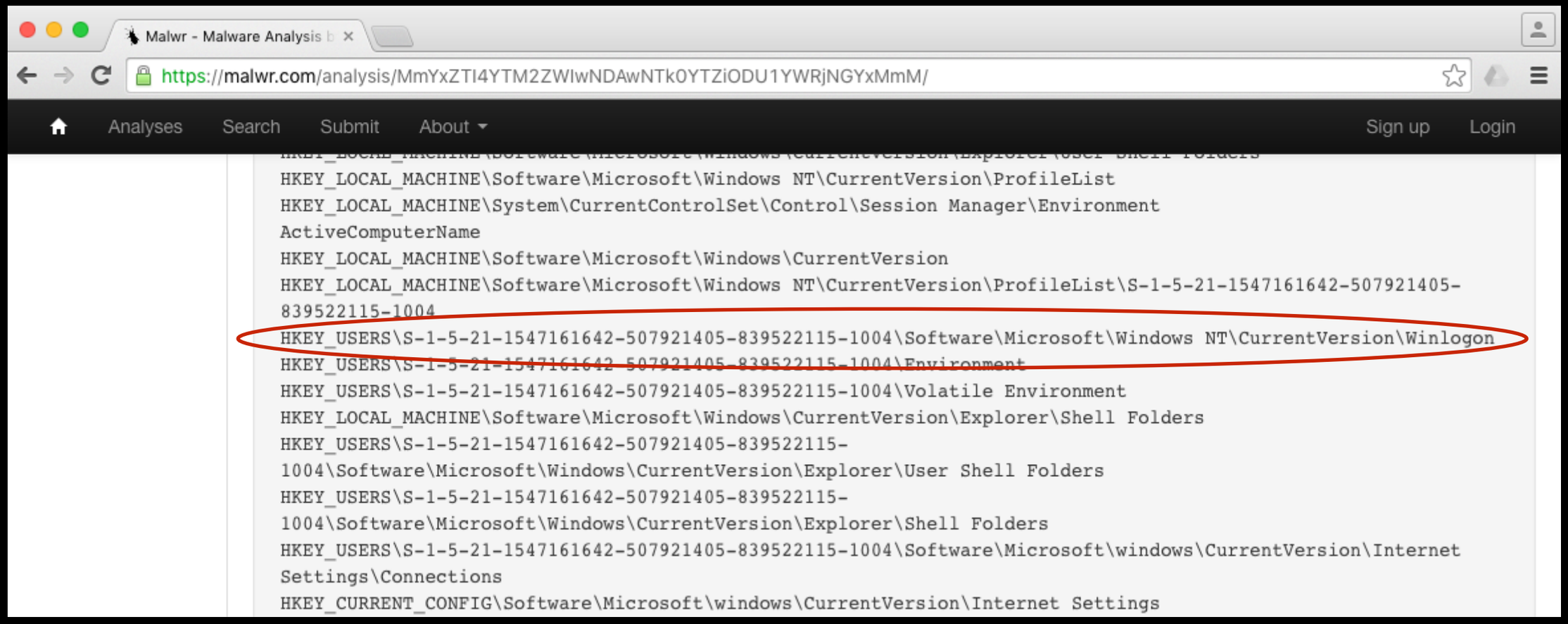
Identify Common Properties



Comparison

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


Malwr - Malware Analysis b
https://malwr.com/analysis/YjNlZGZhMDgzNmYwNGFmOGE3ZWU0YTNjYmIyZjRkZjg/
Analyses
Search
Submit
About
Sign up
Login
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment
ActiveComputerName
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1547161642-507921405-839522115-1004
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Environment
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Volatile Environment
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections
HKEY_CURRENT_CONFIG\Software\Microsoft\windows\CurrentVersion\Internet Settings


Malwr - Malware Analysis
https://malwr.com/analysis/MmYxZTI4YTM2ZWIwNDAwNTk0YTZiODU1YWRjNGYxMmM/
Analyses
Search
Submit
About
Sign up
Login
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment
ActiveComputerName
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1547161642-507921405-839522115-1004
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Environment
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Volatile Environment
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections
HKEY_CURRENT_CONFIG\Software\Microsoft\windows\CurrentVersion\Internet Settings

Malwr - Malware Analysis b

https://malwr.com/analysis/YjNlZGZhMDgzNmYwNGFmOGE3ZWU0YTNjYmIyZjRkZjg/

Analyses Search Submit About Sign up Login

IP
146.185.155.126
139.59.166.196
176.114.3.173
107.170.20.33

DOMAIN	IP
vfskhymctwrudey.work	
olpwaaqa.pw	
jbepeasvjy.work	
mdrrheffduavmv.pl	
rjrrgbagydjtae.pl	
edtlvnqnrfdi.ru	
irmfftepdwqflu.xyz	
nbjmamvhbmvweu.info	

Malwr - Malware Analysis b

https://malwr.com/analysis/MmYxZTI4YTM2ZWIwNDAwNTk0YTZiODU1YWRjNGYxMmM/

Analyses Search Submit About Sign up Login

IP
176.114.3.173
139.59.166.196
107.170.20.33
146.185.155.126

DOMAIN	IP
pndboqlwiwsoh.su	
wxepifrf.ru	
dvjnmwwvhx.ru	
wblcngccarxa.work	
enfnhbvhwd.ru	
wvjeiajyibr.ru	
igyrcvcpvdwlbnaph.su	
dmpulwux.xyz	

Malwr - Malware Analysis b ×

https://malwr.com/analysis/MmYxZTI4YTM2ZWIwNDAwNTk0YTZiODU1YWRjNGYxMmM/

Analyses Search Submit About Sign up Lo

vioral Analysis

ork Analysis

oed Files

ment Board (0)

HTTP Requests

URI	DATA
http://107.170.20.33/userinfo.php	POST /userinfo.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0. 506.648; .NET CLR 3.5.21022) Host: 107.170.20.33 Content-Length: 275 Connection: Keep-Alive Cache-Control: no-cache \x18v>\xd0\xd4UE\x9Z\x93n\xa7\xa1 \xda7\xaf8\x94b\xdf\xf1\x04\xe1%\x1ao\xd7\xeeR\x9c\xba\ f\x01\xe1jb\xd0\x9d\x1d\x0ZH\xce1\xb7_\xe8\x8fn)B\xcf\x

Malwr - Malware Analysis b

https://malwr.com/analysis/YjNlZGZhMDgzNmYwNGFmOGE3ZWU0YTNjYmIyZjRkZjg/

Analyses Search Submit About Sign up Login

Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

HTTP Requests

URI	DATA
http://107.170.20.33/userinfo.php	POST /userinfo.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04 506.648; .NET CLR 3.5.21022) Host: 107.170.20.33 Content-Length: 266 Connection: Keep-Alive Cache-Control: no-cache \xfe)M\x7f\xd1\xb61y\xec\xa1\xf6q\x0c\x8e\x0c\xa6\x06\xd 0"\x9bw\xeeZwa\xaa\xfe\x89\xd6\x12\x03\xc0\x83\xf8\x19\x8 5\x88]Q\xcd\xa7\xb8\xd3\xd0\x9c\x1av\xf9\xee\x91\x96\xaf

Evernote Basic

New Note in Traige | New Chat | Search notes

All Notes | Traige

APRIL 2016 1

Maybe Locky

Today MD5:
7d69f3934be22a9bdcf0e2
0059d6c0a8.zip
109.234.38.35 ==URLS==
http://109.234.38.35/
main.php
_Locky_recover_instruction...

Traige | click to add tags | Share

Helvetica Neue 14

Comparative Analysis

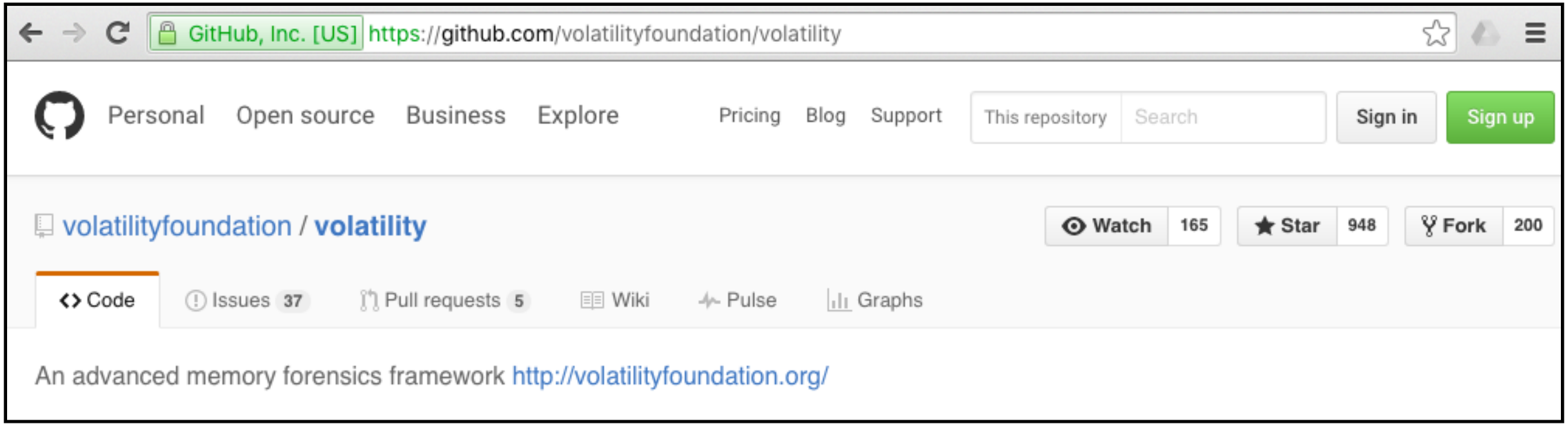
```
POST /userinfo.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Host: 107.170.20.33
Content-Length: 266
Connection: Keep-Alive
Cache-Control: no-cache
```

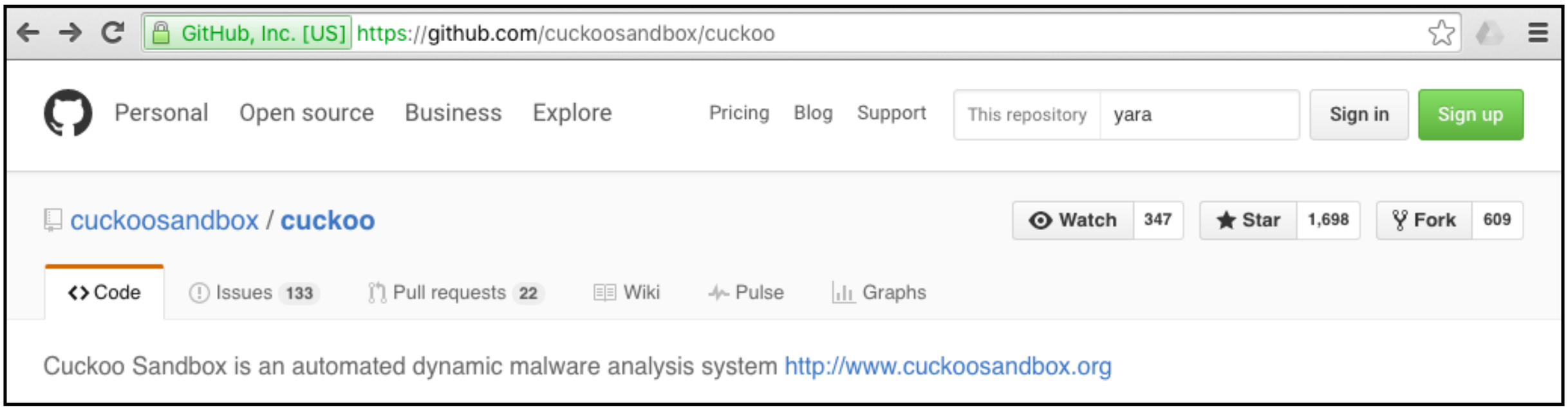
IP
146.185.155.126
139.59.166.196
176.114.3.173
107.170.20.33

No Common Static Attributes

Yara Cannot Proceed

Yara “2.0” is Memory!





https://www.reverse.it/sample/7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142?environmentId=100

reverse.it Home Submissions Contact FAQ Search (MD5, SHA256, English More

Deepviz_b39091b1ae870525b7c26e4c8b4658af_201

Submitted on May 9th 2016 14:37:19 (CDT) running the *Kernelmode* monitor
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pac
Report generated by VxStream Sandbox v4.10 © Payload Security

Sample not shared | Downloads | VirusTotal Report | Metadefe Report | Re-analyze

malicious

Threat Score: 100/100
AV Multiscan: 63%
Trojan.GenericKD

Tweet E-Mail

Incident Response

Risk Assessment

Spyware/Leak	POSTs files to a webserver
Fingerprint	Reads the cryptographic machin UID Reads the active computer name
Network Behavior	Contacts 7 domains and 2 hosts. View network section for more details.

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Incident Response
Indicators
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Data
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

https://www.reverse.it/sample/7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142?environmentId=100

rsverse.it Home Submissions Contact FAQ Search (MD5, SHA256, English More

Extracted Strings

Download All Memory Strings (12KiB)

All Details: Off

Interesting (256) | All Strings (991) | 7d69f3934be22a9bdcf0e2... | 7d69f3934be22a9bdcf0e2... | PCAP (5) | cmd.exe (1) | svchost.exe:2116 (177)

- .class
- .djvu
- .java
- .locky
- .ms11 (Security copy)
- .potx
- .pptx
- .qcow2
- .SQLITEDB
- .tar.bz2
- .vmdk
- .xlsb

Incident Response
Indicators
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Data
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

Extracted Files

https://www.reverse.it/sample/7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142?environmentId=100

Extracted Strings

Download All Memory Strings (12KiB)

All Details: Off

Interesting (256) | All Strings (991) | 7d69f3934be22a9bdcf0e2... | 7d69f3934be22a9bdcf0e2... | PCAP (5) | cmd.exe (1) | svchost.exe:2116 (177)

@_Locky_recover_instructions.bmp

_Locky_recover_instructions.bmp

_Locky_recover_instructions.txt

\Sessions\1\Windows\ApiPort

__based(

__cdecl

__clrcall

__eabi

__fastcall

__pascal

__ptr64

__restrict

Incident Response
Indicators
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Data
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

Extracted Files

https://www.reverse.it/sample/7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142?environmentId=100

Extracted Strings

Download All Memory Strings (12KiB)

All Details: Off

Interesting (256) All Strings (991) 7d69f3934be22a9bdcf0e2... 7d69f3934be22a9bdcf0e2... PCAP (5) cmd.exe (1) svchost.exe:2116 (177)

SHGetFolderPathW

Sleep

Software\Locky

Software\Microsoft\Windows\CurrentVersion\Run

string too long

Sunday

svchost.exe

SystemParametersInfoW

Tahoma

TerminateProcess

text&lang=

Thursday

Incident Response
Indicators
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Data
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

Extracted Files

https://www.reverse.it/sample/7d69f3934be22a9bdcf0e20059d6c0a851218abe9aa07b83795c54e696be6142?environmentId=100

Extracted Strings

Download All Memory Strings (12KiB)

All Details: Off

Interesting (256) | All Strings (991) | 7d69f3934be22a9bdcf0e2... | 7d69f3934be22a9bdcf0e2... | PCAP (5) | cmd.exe (1) | svchost.exe:2116 (177)

CryptReleaseContext

D$''I'$L)&O)'Q)'R)'T*'V)&W(&X)&W(&S'$P&$M%#J$''G#!F#!F#!H#!J#''L#!N#''Q#''Q''''Q''''Q#''R#''R##R$#R$$R$#R$#Q$#Q%$Q%$Q&$S'%T(&V('W('X))X))X))W))V))U)(T((S('R('Q('R"Q"P"P&'P%&P$%P''#Q!''Q!''Q!!Q!!R''#S''#T##T$$T%$U%$U%#T$''R#''Q#!Q#!O#!P$''R%#S&$T'%U)&V+'W+(V+(U+(U+(U+(T+)T*)T('R'&Q&%O%N''M$''M%#O&%R('S('V)(Y*([*([*)\.*].-_0.b2/d20f10f/-e/,d-*a+)^)'['&X'$U&$R&S'S(%S(%S)'U+(W,)W+(U*)S)(R(&Q%%O$#N%#P'%U)(\,*a-+a-+`/-d41k;6v>9|@;

D:\2d4\1x20e\s6m32\q\v02\8mzewd\xq1fw.pdb

dbOOOOOOOO

dBXOY/

DefWindowProcA

dii i`

dLqtqtqtq

dLttttttt-ttttttXEdKooooooooooooooo

dLXXXXXXXXXXXX

Extracted Files

Incident Response
Indicators
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Data
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

All Notes Traige

MAY 2016 1

Maybe Locky

Today MD5:
7d69f3934be22a9bdcf0e2
0059d6c0a8.zip
109.234.38.35 ==URLS==
http://109.234.38.35/
main.php
_Locky_recover_instruction...

Traige click to add tags

Share

Cabin 14

Potential In-Memory Yara Strings

D:\2d4\1x20e\s6m32\q\v02\8mzewd\xq1fw.pdb

.class
.djvu
.java
.locky
.ms11 (Security copy)
.potx
.pptx
.qcow2
.SQLITEDB
.tar.bz2
.vmdk
.xlsb
.xlsx
.xltx

_Locky_recover_instructions.bmp
_Locky_recover_instructions.txt

Software\Locky
Software\Microsoft\Windows\CurrentVersion\Run

Develop IOC

Choose IOC Format(s)

Develop Yara Rule

Develop OpenIOC Rule

Practical Yara

```
rule Locky_Memory
{
    meta:
        desc = "Locky in memory strings"
        family = "Locky Ransomeware"

    strings:
        $a1 = ".locky"
        $a2 = "Locky_recover_instructions.bmp"
        $a3 = "Locky_recover_instructions.txt"
        $a4 = "Software\Lock"
        $b1 = ".djvu"
        $b2 = ".java"
        $b3 = ".ms11"
        $b4 = ".tar.bz2"
        $b5 = ".SQLITEDB"
        $b6 = ".qcow2"


    condition:
        $a2 or $a3 or ($a1 and $a4) or ($a1 and $b1 and $b2 and $b3 and $b4 and $b5 and $b6)
}
```

Meta: information about the IOC. This is all optional but the bare minimum is advised.

Practical Yara

```
rule Locky_Memory
{
    meta:
        desc = "Locky in memory strings"
        family = "Locky Ransomeware"

    strings:
        $a1 = ".locky"
        $a2 = "Locky_recover_instructions.bmp"
        $a3 = "Locky_recover_instructions.txt"
        $a4 = "Software\Lock"
        $b1 = ".djvu"
        $b2 = ".java"
        $b3 = ".ms11"
        $b4 = ".tar.bz2"
        $b5 = ".SQLITEDB"
        $b6 = ".qcow2"

    condition:
        $a2 or $a3 or ($a1 and $a4) or ($a1 and $b1 and $b2 and $b3 and $b4 and $b5 and $b6)
}
```

Strings: List of strings “attributes” that will be used in the rule. Each assigned to a variable. “Wide” is used to denote wide string (unicode).

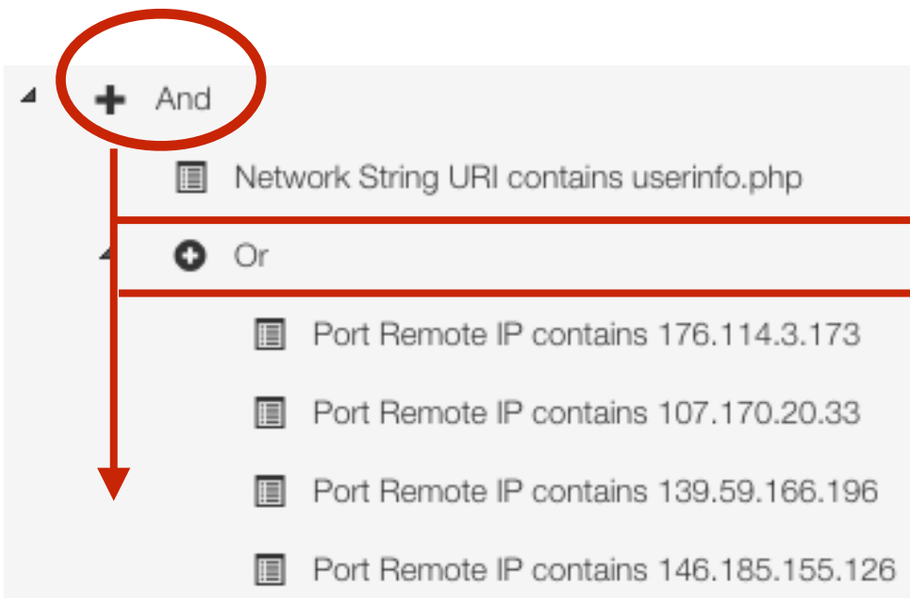
Practical Yara

```
rule Locky_Memory
{
    meta:
        desc = "Locky in memory strings"
        family = "Locky Ransomeware"

    strings:
        $a1 = ".locky"
        $a2 = "Locky_recover_instructions.bmp"
        $a3 = "Locky_recover_instructions.txt"
        $a4 = "Software\Lock"
        $b1 = ".djvu"
        $b2 = ".java"
        $b3 = ".ms11"
        $b4 = ".tar.bz2"
        $b5 = ".SQLITEDB"
        $b6 = ".qcow2"

    condition:
        $a2 or $a3 or ($a1 and $a4) or ($a1 and $b1 and $b2 and $b3 and $b4 and $b5 and $b6)
}
```

condition: The rule that uses the string assigned variables and logic operators. For now we will stick to simple “and” “or” but there are many more!

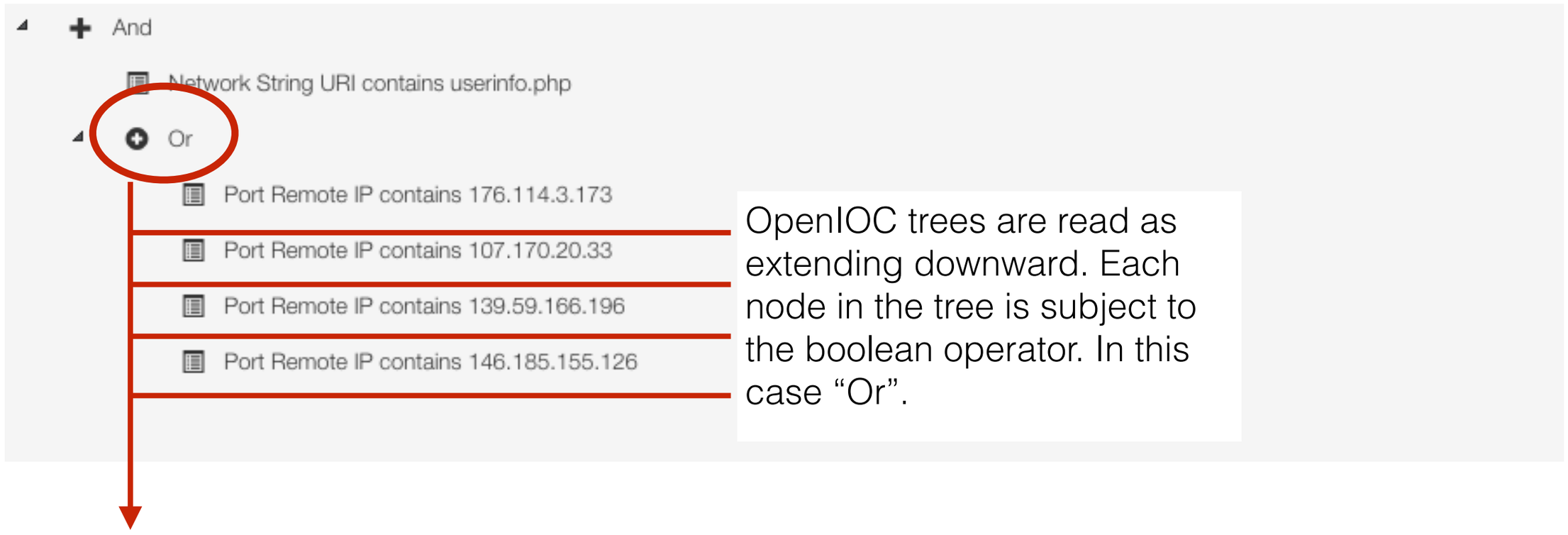
```
rule Locky_Memory
{
    meta:
        desc = "Locky in memory strings"
        family = "Locky Ransomeware"

    strings:
        $a1 = ".locky"
        $a2 = "Locky_recover_instructions.bmp"
        $a3 = "Locky_recover_instructions.txt"
        $a4 = "Software\Lock"
        $b1 = ".djvu"
        $b2 = ".java"
        $b3 = ".ms11"
        $b4 = ".tar.bz2"
        $b5 = ".SQLITEDB"
        $b6 = ".qcow2"


    condition:
        $a2 or $a3 or ($a1 and $a4) or ($a1 and $b1 and $b2 and $b3 and $b4 and $b5 and $b6)
}
```

Practical OpenIOC

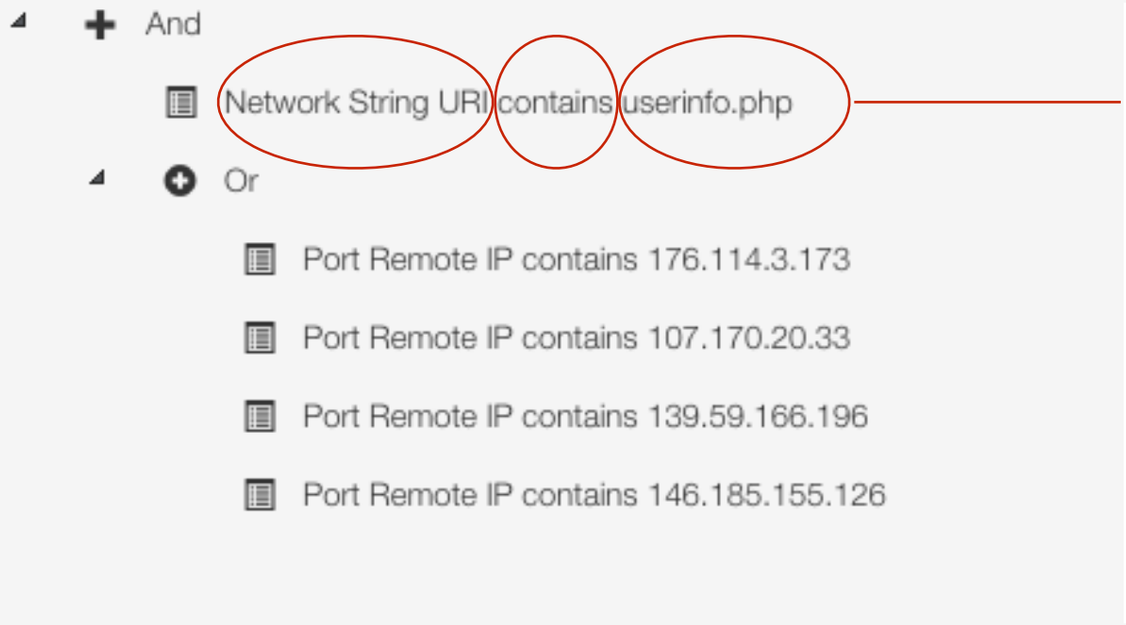


OpenIOC trees are read as extending downward. Each node in the tree is subject to the boolean operator. In this case “And”.

Practical OpenIOC



Practical OpenIOC



OpenIOC entries are composed of a descriptor, an operator, and an attribute.

In this case:
Descriptor: “Network String URI”
Operator:contains
Attribute:userinfo.php

- And
  - Network String URI contains userinfo.php
  - Or
    - Port Remote IP contains 176.114.3.173
    - Port Remote IP contains 107.170.20.33
    - Port Remote IP contains 139.59.166.196
    - Port Remote IP contains 146.185.155.126

JUST DO IT!!!!!

Workshop

Details in your workbook.

Test (Validate)

Test IOCs Against Known Bad

Test IOCs Against Known Good

How To Test

Known Bad

- Test against your sample set just to verify everything still matches.
- Test against your malware collection for the past few weeks, did you get any hits?
- Monitor your new IOCs if one stops matching (especially if it's for a common family) time to investigate!

Known Good

- Run against your standard deployment image, we don't want any false positives!

Known Bad Test

Yara

- Run Yara rule against your directory of samples and verify each sample has been identified.

Memory Yara

- Run sample in Windows VM and take memory capture.
- Use Volatility yarascan to verify the sample is identified.

OpenIOC

- Run sample in Windows VM and take memory capture.
- Use Volatility openioc_scan to verify the sample is identified.

OpenIOC (Windows only)

- Use Mandiant Redline to create an memory acquisition “collector”.
- Run sample in Windows VM and use collector to acquire memory.
- Import IOC into Redline and analyze acquired memory to verify sample is identified.

Administrator: Command Prompt

```
C:\Users\Administrator\Desktop>dump.txt

C:\Users\Administrator\Desktop>DumpIt.exe
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1073741824 bytes (   1024 Mb)
    Free space size:          11712393216 bytes (  11169 Mb)

    * Destination = \??\C:\Users\Administrator\Desktop\WIN-D2AGAN7QSH8-20161012-223227.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing... Success.


C:\Users\Administrator\Desktop>_
```

Administrator: Command Prompt - volatility-2.5.standalone.exe --profile=Win2008SP1x86 -f WIN-D2AGAN7QSH8-20161012-230640.raw yarascan -y Locky.yar

```
C:\Users\Administrator\Desktop>volatility-2.5.standalone.exe --profile=Win2008SP1x86 -f WIN-D2AGAN7QSH8-20161012-230640.raw yarascan -y Locky.yar
Volatility Foundation Volatility Framework 2.5
Rule: Locky_Memory
Owner: Process winlogon.exe Pid 580
0x004eb2ef  37 25 37 2d 37 33 37 3b 37 41 37 49 37 4f 37 57   7%7-737;7A7I7O7W
0x004eb2ff  37 5d 37 65 37 6c 37 71 37 78 37 7d 37 84 37 89   7]7e7l7q7x7}7.7.
0x004eb30f  37 90 37 95 37 9c 37 a1 37 a8 37 ad 37 b4 37 c2   7.7.7.7.7.7.7.7.
0x004eb31f  37 c8 37 d3 37 d8 37 e9 37 f0 37 f6 37 fd 37 0c   7.7.7.7.7.7.7.7.
0x004eb32f  38 13 38 19 38 22 38 2f 38 39 38 d9 38 18 39 2e   8.8.8"8/898.8.9.
0x004eb33f  39 3b 39 44 39 9d 39 bb 39 c5 39 cf 39 e3 39 ed   9;9D9.9.9.9.9.9.
0x004eb34f  39 f7 39 0a 3a 16 3a 22 3a f3 3a f9 3a ff 3a 19   9.9.:.:":.:.:.:.
0x004eb35f  3b 1e 3b 27 3b 2d 3b 37 3b 3d 3b 44 3b 4b 3b 6a   ;.;';-;7;=;D;K;j
0x004eb36f  3b 6f 3b 78 3b 7e 3b 88 3b 8e 3b 95 3b 9c 3b 50   ;o;x;~;.;.;.;.;P
0x004eb37f  3c 62 3c 74 3c 8f 3c a1 3c a7 3c c2 3c cb 3c d2   <b<t<.<.<.<.<.<.
0x004eb38f  3c 0b 3d 12 3d 29 3d 2f 3d 41 3d 54 3d 5b 3d 7c   <.=.=)=/=A=T=[=|
0x004eb39f  3d 8b 3d a9 3d cb 3d e5 3d f2 3d 0f 3e 23 3e 35   =.=.=.=.=.=.=.>#>5
0x004eb3af  3e 56 3e 5d 3e 74 3e 7a 3e 8f 3e 95 3e 9b 3e 00   >V>]>t>z>.>.>.>.
0x004eb3bf  00 00 50 00 00 40 00 00 00 00 30 08 30 0c 30 10   ..P..@....0.0.0.
0x004eb3cf  30 14 30 58 34 68 34 78 34 88 34 98 34 a8 34 b8   0.0X4h4x4.4.4.4.
0x004eb3df  34 c8 34 d8 34 e8 34 f8 34 08 35 18 35 28 35 38   4.4.4.4.4.5.5(58
Rule: Locky_Memory
Owner: Process winlogon.exe Pid 580
0x006eb2ef  37 25 37 2d 37 33 37 3b 37 41 37 49 37 4f 37 57   7%7-737;7A7I7O7W
0x006eb2ff  37 5d 37 65 37 6c 37 71 37 78 37 7d 37 84 37 89   7]7e7l7q7x7}7.7.
0x006eb30f  37 90 37 95 37 9c 37 a1 37 a8 37 ad 37 b4 37 c2   7.7.7.7.7.7.7.7.
0x006eb31f  37 c8 37 d3 37 d8 37 e9 37 f0 37 f6 37 fd 37 0c   7.7.7.7.7.7.7.7.
0x006eb32f  38 13 38 19 38 22 38 2f 38 39 38 d9 38 18 39 2e   8.8.8"8/898.8.9.
0x006eb33f  39 3b 39 44 39 9d 39 bb 39 c5 39 cf 39 e3 39 ed   9;9D9.9.9.9.9.9.
0x006eb34f  39 f7 39 0a 3a 16 3a 22 3a f3 3a f9 3a ff 3a 19   9.9.:.:":.:.:.:.
0x006eb35f  3b 1e 3b 27 3b 2d 3b 37 3b 3d 3b 44 3b 4b 3b 6a   ;.;';-;7;=;D;K;j
0x006eb36f  3b 6f 3b 78 3b 7e 3b 88 3b 8e 3b 95 3b 9c 3b 50   ;o;x;~;.;.;.;.;P
0x006eb37f  3c 62 3c 74 3c 8f 3c a1 3c a7 3c c2 3c cb 3c d2   <b<t<.<.<.<.<.<.
0x006eb38f  3c 0b 3d 12 3d 29 3d 2f 3d 41 3d 54 3d 5b 3d 7c   <.=.=)=/=A=T=[=|
0x006eb39f  3d 8b 3d a9 3d cb 3d e5 3d f2 3d 0f 3e 23 3e 35   =.=.=.=.=.=.=.>#>5
0x006eb3af  3e 56 3e 5d 3e 74 3e 7a 3e 8f 3e 95 3e 9b 3e 00   >V>]>t>z>.>.>.>.
0x006eb3bf  00 00 50 00 00 40 00 00 00 00 30 08 30 0c 30 10   ..P..@....0.0.0.
0x006eb3cf  30 14 30 58 34 68 34 78 34 88 34 98 34 a8 34 b8   0.0X4h4x4.4.4.4.
0x006eb3df  34 c8 34 d8 34 e8 34 f8 34 08 35 18 35 28 35 38   4.4.4.4.4.5.5(58
```

Start your Analysis Session

Review Script Configuration

You have chosen to create a Standard Collector

The standard collector will collect the data necessary to perform a Redline Analysis focused on memory based audits. Note: this will not enable the options for the full range of data that Redline is capable of collecting, reducing the effectiveness of many Indicators of Compromise.

Edit your script

Acquire Memory Image

☑ Checking this option will acquire an image of memory that can be used to accurately acquire process memory and drivers during analysis in Redline

Specify Collector Location

1. Your Collector package will be created and saved to the location you specify below.

2. On the machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.

3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.

A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'

Redline® - C:\Users\Administrator\Desktop\redline_data\Sessions\AnalysisSession1\AnalysisSession1.mans

Home

Analysis Data

- System Information
- Processes
  - Handles
  - Memory Sections
  - Strings
  - Ports
- Hierarchical Processes
- Driver Modules
- Device Tree
- Hooks
- Timeline
- Tags and Comments
- Acquisition History

Start Your Investigation

Show Home Page on Startup

Investigate >

I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

Investigate >

I Want to Search My Data With a Set of Indicators of Compromise

When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select 'Create a New IOC Report' and specify the location on disk that contains your indicator. When the report is finished you will find it underneath the IOC Reports tab to the left. For more information on IOCs visit http://www.openioc.org

Start your Analysis Session

Instructions

Indicators of Compromise are forensic artifacts left

Configuration

Indicators of Compromise Location: Open Folder

C:\Users\Administrator\Desktop\redline_data\iocs

Browse...

Indicators

	Name
☑	Locky

1 Indicators

Indicator Information

Name: Locky

Author: Testing IOCs **Created:** 10/12/2016 10:12:02 PM

Path: C:\Users\Administrator\Desktop\redline_data\iocs\Testing IOCs.ioc

Description: Locky

Not Collected Search Terms:

None

Unsupported Search Terms:

None

Supported Search Terms:

ProcessItem/name (context: mir)

Cancel

OK

Redline® - C:\Users\Administrator\Desktop\redline_data\Sessions\AnalysisSession1\AnalysisSession1.mans

Home ▸ IOC Reports ▸ IOC Report (10/12/2016 10:13:16 PM)

Analysis Data

IOC Report (10/12/2016 10:13:1

Create a New IOC Report

Host | IOC Reports

Not Collected

IOC Report (10/12/2016 10:13:16 PM)

Locky- (UID: 10797c19)

C:\Users\Administrator\Desktop\redline_data\Sessions\AnalysisSession1\Audits\20161012214624_Copy\ForIocReport\00001122334455\mir.w32processes-memory.3q7iazrzTALbzQp7OWR0yf

View Hits +

Details

Report Details

1 out of your **1** Indicators of Compromise have hit against this Session.

Report Location: C:\Users\Administrator\Desktop\redline_data\Sessions\AnalysisSession1\IOCs\IOCReport\index.html

Known Good Test

Yara

- Run Yara rule against a clean standard image and verify there are no hits.
  - Scan %PROGRAMFILES(x86)%
  - Scan %PROGRAMFILES%
  - Scan %SystemRoot%

Memory Yara

- Take memory capture of a clean standard image.
- Use Volatility yarascan to verify there are no hits.

OpenIOC

- Take memory capture of a clean standard image.
- Use Volatility openioc_scan to verify there are no hits.

OpenIOC (Windows only)

- Use Mandiant Redline to create an memory acquisition “collector”.
- Use collector to acquire memory from a clean standard image.
- Import IOC into Redline and analyze acquired memory to verify there are no hits.

Administrator: Command Prompt

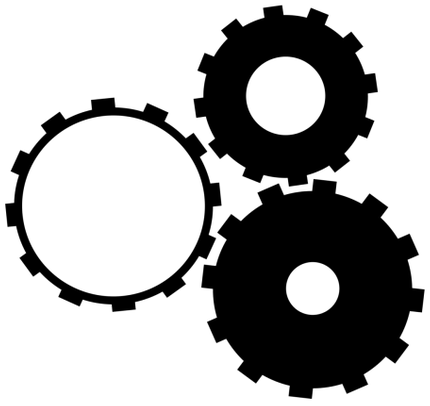
```
C:\Users\Administrator\Desktop>yara32.exe Locky.yar "%SystemRoot%"
error scanning C:\Windows\WindowsUpdate.log: could not open file

C:\Users\Administrator\Desktop>yara32.exe Locky.yar "%PROGRAMFILES%"

C:\Users\Administrator\Desktop>_
```

JUST DO IT!!!!!

Workshop

Details in your workbook.

Automation



Getting API Access

Making API Access

Leveraging OSS

Introduction To Automation

Why Automate

Auto Ignore

- This is where you get true ROI, you remove your expensive analysts from workflows that don't require them.
- When you have analyzed a sample once no need to look at it again; automate decision making in triage.

Auto Find

- With a robust IOC once you have identified a singe compromise you can identify all similar across your enterprise.

Automate The Automation

- Much of the IOC generation process can also be automated. Where there is an API there is a way!

Automating Discovery (Enrichment)

Where there is an API there is a way!

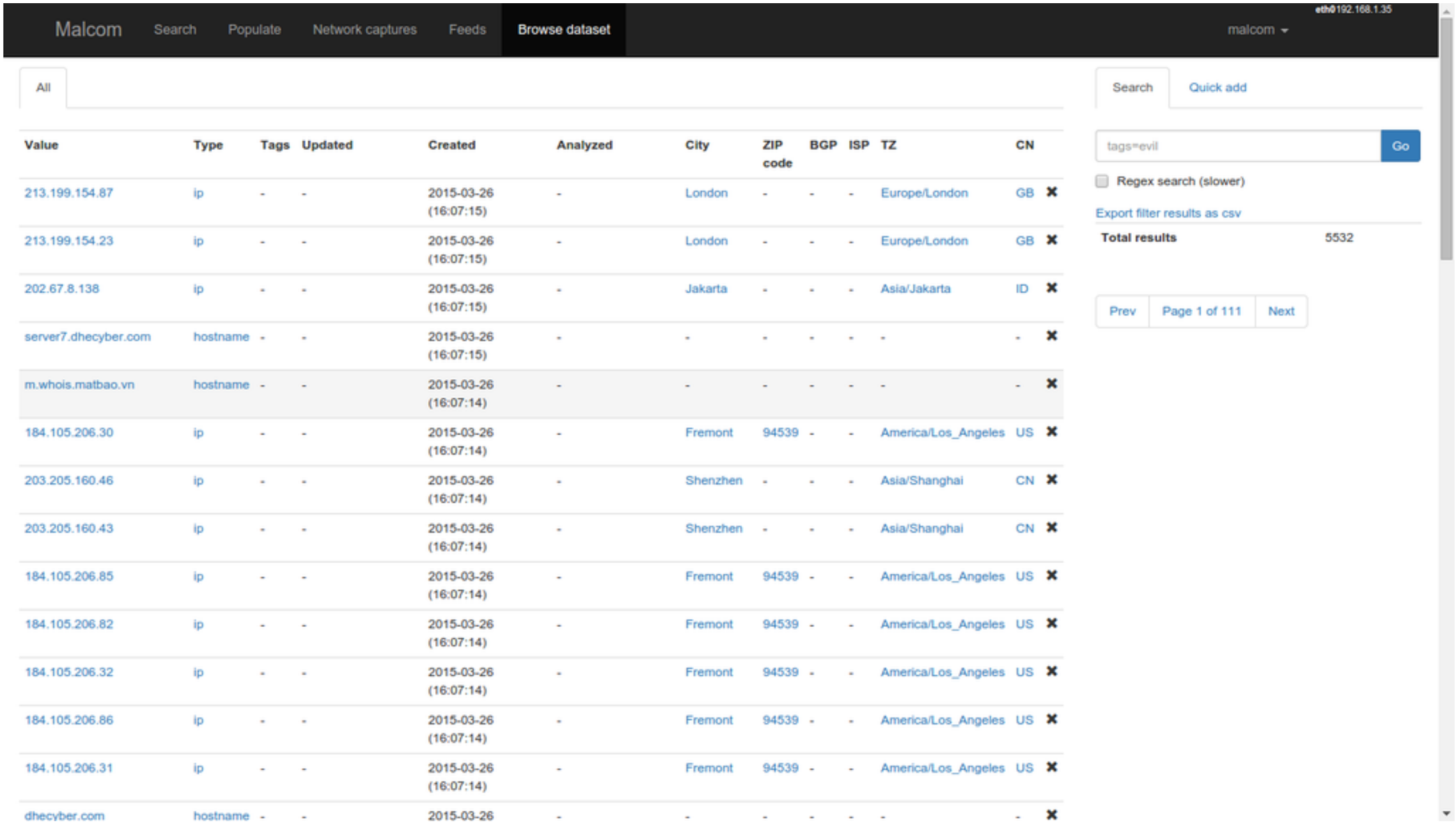
- VirusTotal Intelligence (need a paid membership)
- DomainTools (need paid API key)
- BlueCoat SiteReview
- OTX AlienVault
- PassiveTotal
- ThreatCrowd
- Malc0de

Where there is no API make one!

- Scumblr search anything that can be searched:
  - Malwr
  - Hybrid-analysis
- Web scraper
  - TheatMiner
  - DNSBL
  - urlquery.net

Automating Rule Generation*

Automating Identification Malcom (Network)



Automating Identification
Loki (Host)

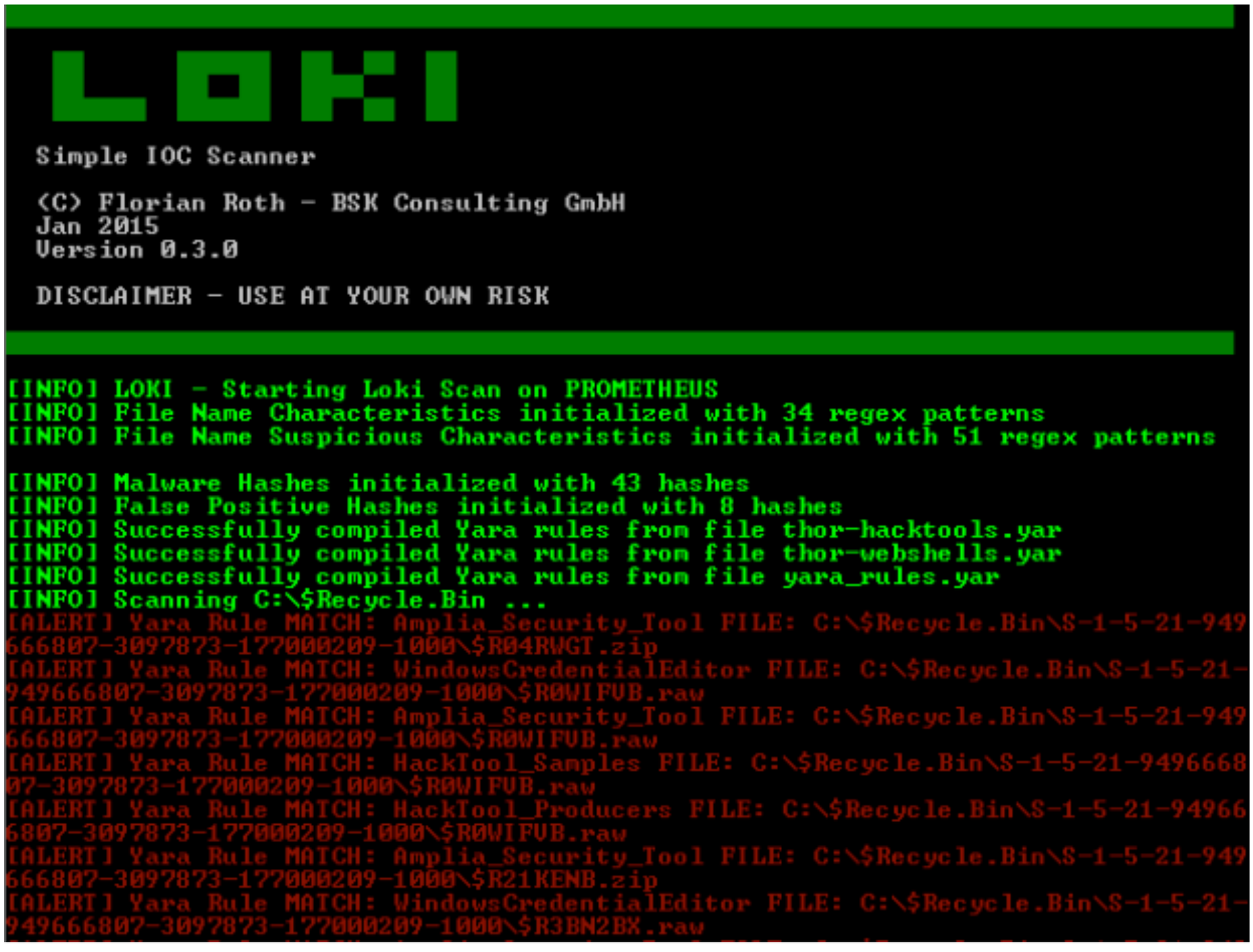


Image Attribution

Network by Rafa Bosch from the Noun Project
Icon made by Freepik from http://www.flaticon.com is licensed under CC BY 3.0
Fingerprint by Daouna Jeong from the Noun Project
Unknown Document by Indygo from the Noun Project
Server by Francesco Terzini from the Noun Project
code by Brennan Novak from the Noun Project
Cloud Download by useiconic.com from the Noun Project
Lemon Liu - Noun Project
Prasad - Noun Project
Exe by corpus delicti (Noun Project)
Lock by Travis Avery (Noun Project)
Binary file by Creative Stall (Noun Project)
File template Created by Alfedo Hernandez (Noun Project)
DOC File by Arthur Shlain (Noun Project)
DOCX File by Arthur Shlain (Noun Project)
Doc File by arjuazka (Noun Project)
Class by Arthur Shlain (Noun Project)
Jar by To Uyen (Noun Project)
Zip by Nut Chant (Noun Project)
Class by Arthur Slain (Noun Project)
Cloud by unlimicon (Noun Project)
Gears by TS Graphics (Noun Project)
Doc by Oliviu Stoian (Noun Project)
Presentation by Alfredo Hernandez (Noun Project)
Error by Rflor (Noun Project)
Embedded by Sergey Demushkin (Noun Project)
Code by Schmidt Sergey (Noun Project)
Cloud Analysis by Delwar Hossain (Noun Project)
Monitor Cog by Aybige Aya (Noun Project)
User by TukTuk Design (Noun Project)