Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Armée suisse**
Base d'aide au commandement BAC


**PUBLIC**

# Applied Cyber Threat Intelligence (CTI)

EPFL, 2019

# Agenda

- **What is Cyber Threat Intelligence (CTI)**
- Sandbox Malware analysis
- Debugger Malware analysis
- Static RE with IDA pro

# What is Cyber Threat Intelligence (CTI) ?

- **A Threat ?**

***"A person or thing likely to cause damage or danger."*** [1]

1.Oxford dictionary

# What is Cyber Threat Intelligence (CTI) ?

- **Intelligence ?**

***"the collection of information of military or political value."*** [1]

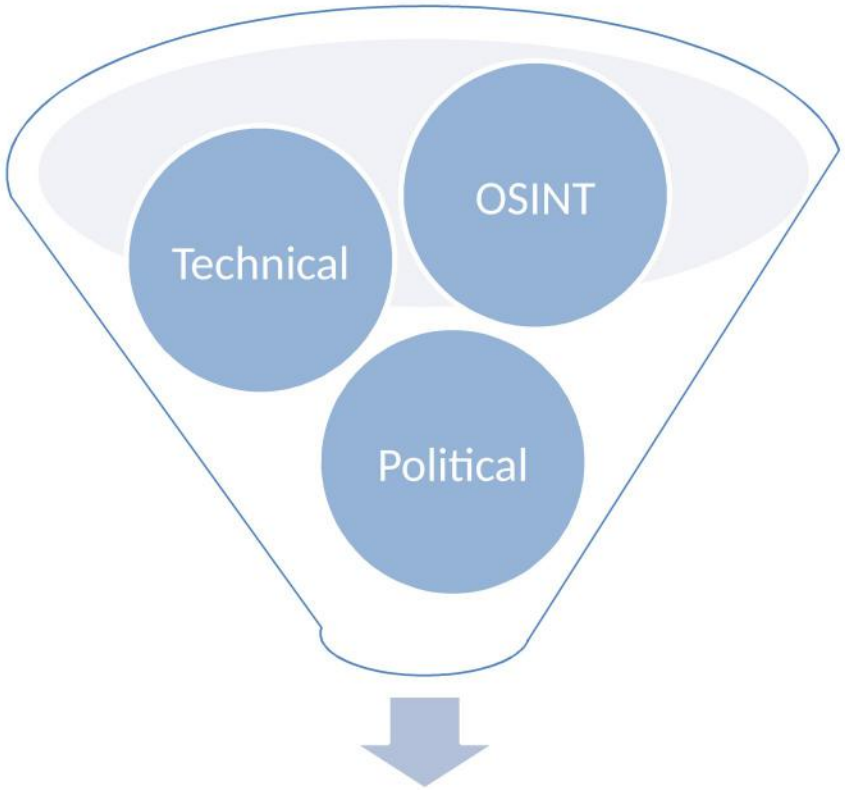
1.Oxford dictionary

# What is Cyber Threat Intelligence (CTI) ?

- **Cyber Threat Intelligence**

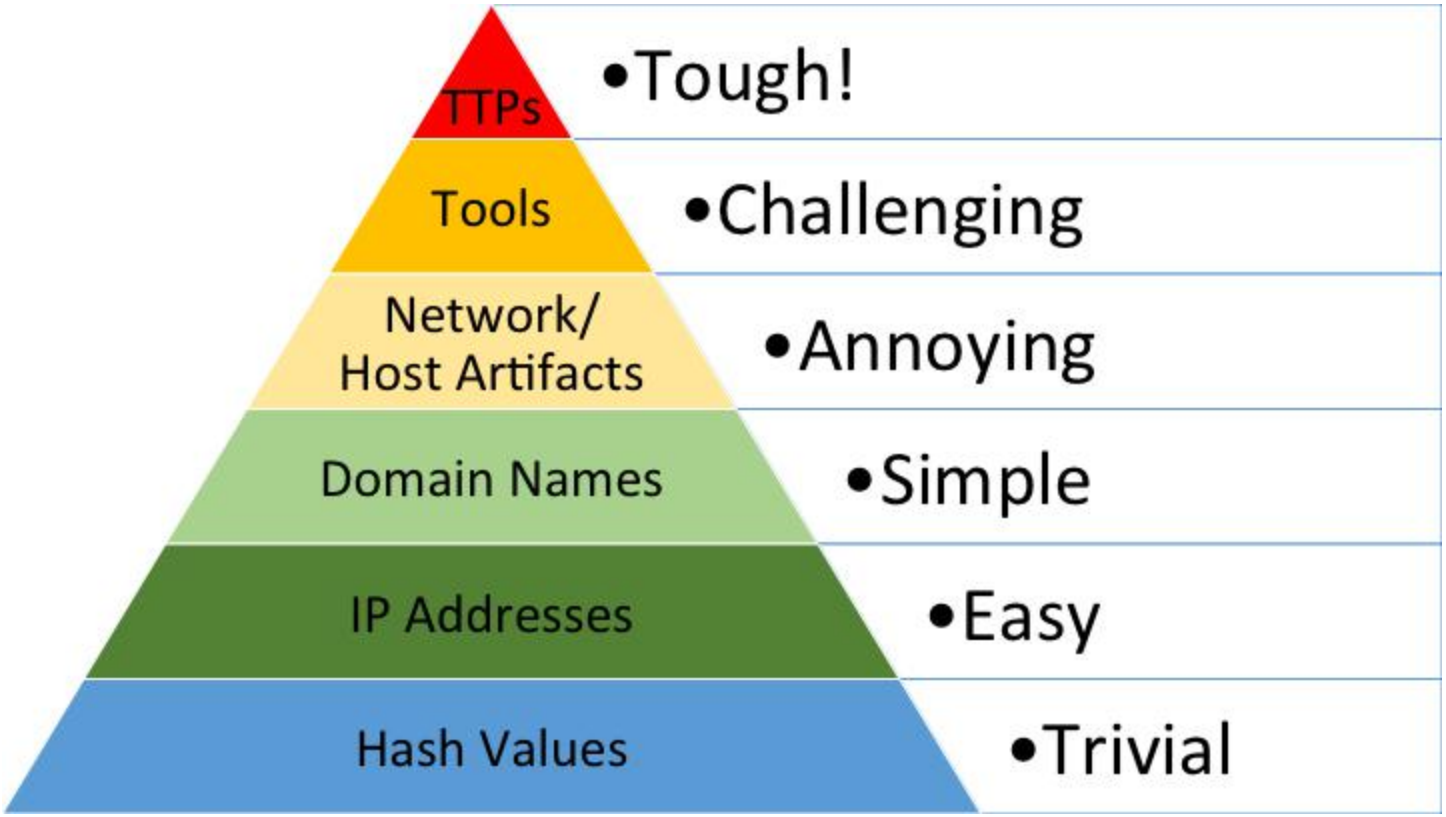
***"Collection and analysis of information (of military or political value) on cyber threats in order to provide actionable information to decision makers"***

# What is Cyber Threat Intelligence (CTI) ?

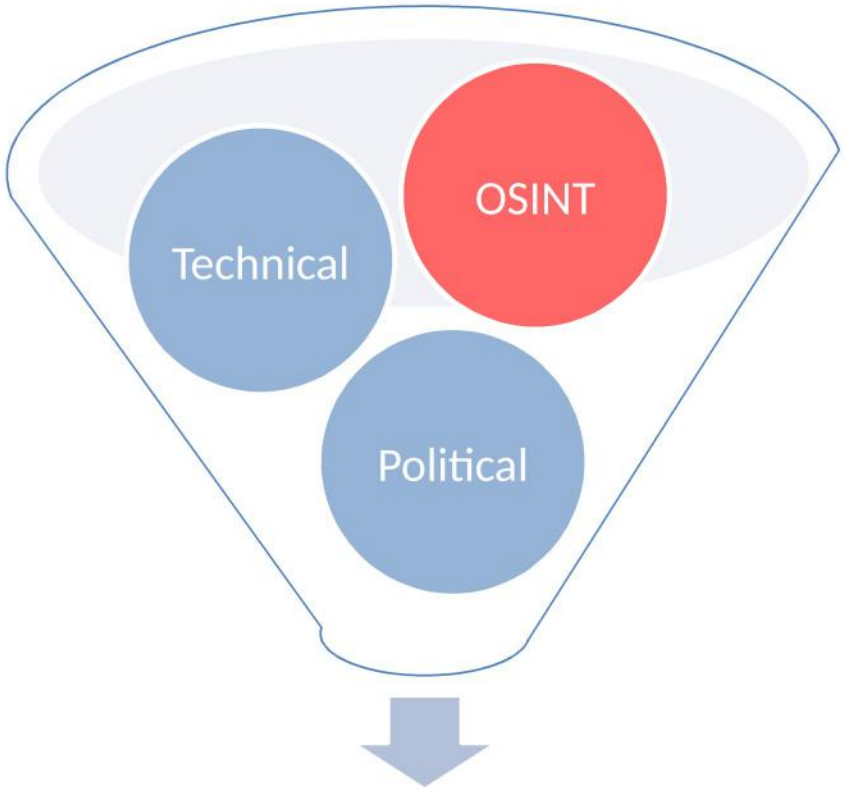


# Why do we do CTI ?
# Introducing the "Pyramid of Pain"

**http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html**



# Let‘s focus on OSINT



# OSINT

- Usefool tools for OSINT:
  - Virustotal.com
  - Passivetotal
  - Censys
  - Shodan
  - https://inteltechniques.com/menu.html
  - Search engines
  - And more …

# OSINT

- Good tool to gather OSINT news and infos:
  - Twitter
  - Twitter lists
  - RSS

# OSINT Exercice

- Find everything that you can on:

"uglygorilla@163.com"

# OSINT Exercice

- Find everything that you can on:

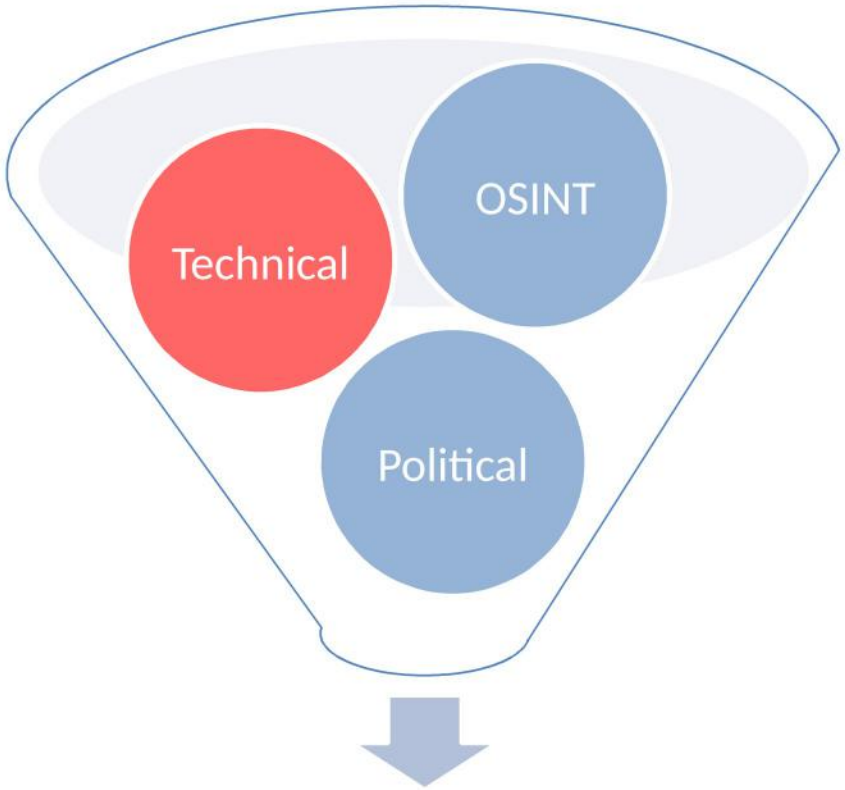
"Kim Hyon Woo"

# OSINT Exercice

- Malware IOCs
  - Find interesting IOCs on:
  - 6884e3541834cc5310a3733f44b38910
  - Ea728abe26bac161e110970051e1561fd51db93b

*You can copy and paste from:*
*https://ghostbin.com/paste/c9qj6*

# What is Cyber Threat Intelligence (CTI) ?



# CTI Technical

## Technical sources

- Incident response / Forensic
- Malware analysis
- External (commercial, researcher, …)
- Honeypots, active defense
- ….

# CTI Technical

## Technical sources

- Incident response / Forensic
- Malware analysis
- External (commercial, researcher, …)
- Honeypots, active defense
- ….

# What is a malware ?

## Different type of malware

- Trojan (from the Trojan war in Greek mythology)
- Worm (self-replicating and spreading)
- Ransomware
- Adware
- Spyware
- RAT (Remote Administration Tool)
- ….

# What is a malware ?

## Output from malware analysis

IOCs ! (indicator of compromises)

- IP addresses
- URL / Domains
- OS specific artifacts (file creation, registry on Windows, …)
- Network artifacts (crypto, typo on http parameters, …)
- Vulnerabilities (network protocol, bad input sanitisation, …)
- ….

# Extract behavioural IOCs

We can have two approaches

- Sandbox
- Emulation

# Extract behavioural IOCs

Example:

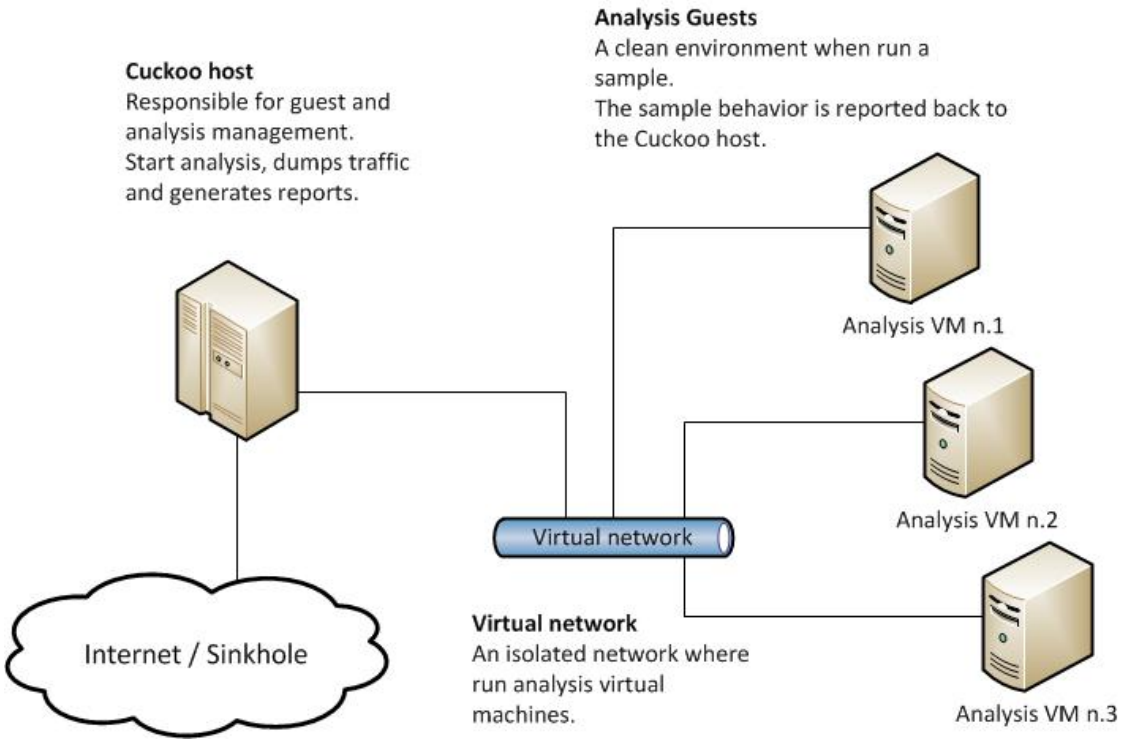
- Cuckoo sandbox (opensource)
- Lastline (emulation)
- Falcon sandbox (hybrid-analysis.com)
- Joe sandbox (based in CH)
- Vmray (ring -1 sandbox)

# Extract behavioural IOCs

- Cuckoo sandbox (https://cuckoosandbox.org/)
- Perfect to start your own
- Opensource
- Easy to setup (pip install -U cuckoo)

# Extract behavioural IOCs

- Cuckoo sandbox (https://cuckoosandbox.org/)



# Extract behavioural IOCs

You can download shadowhammer samples and some exercise: *https://we.tl/t-3YGdkI2Zoi*

**BE CAREFUL, shadowhammer samples are real samples don't run that on a windows machine outside of a specific analysis virtual machine !**

# Extract behavioural IOCs

- Joe sandbox reports examples
  *(https://www.joesecurity.org/joe-sandbox-reports)*
- How to read a sandbox report
- Let's have a look at the "ShadowHammer" supply chain attack sample
  *(https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/)*

# Extract behavioural IOCs

**What is "ShadowHammer" ?**

*“sophisticated supply chain attack involving ASUS Live Update Utility”*

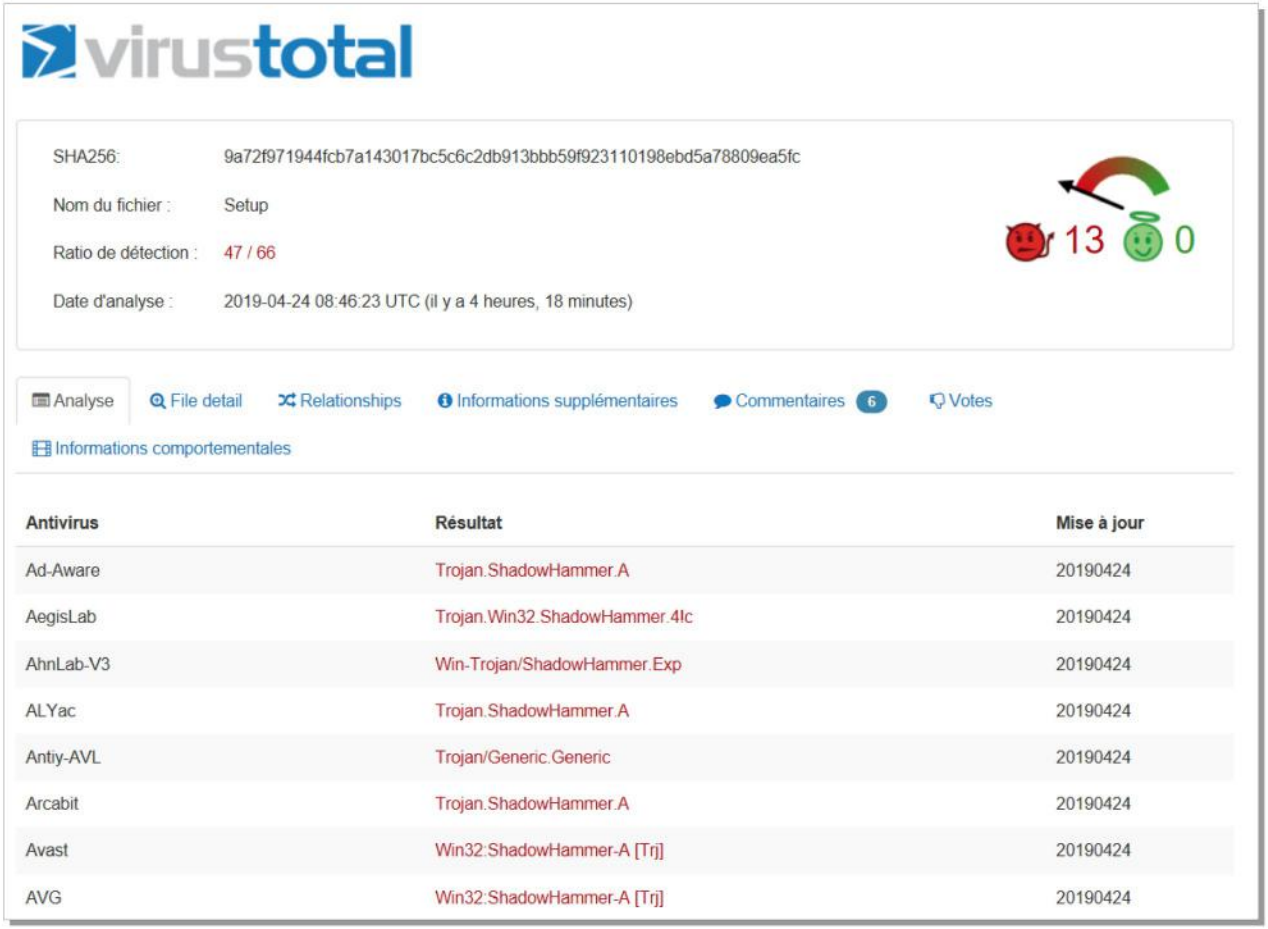
*“The research started upon the discovery of a trojanized ASUS Live Updater file (setup.exe), which contained a digital signature of ASUSTeK Computer Inc. and had been backdoored using one of the two techniques explained below.”*

*Let's start with static analysis*

# Extract behavioural IOCs

- Virustotal report:

"ShadowHammer" supply chain attack



virustotal

SHA256: 9a72f971944fcb7a143017bc5c6c2db913bbb59f923110198ebd5a78809ea5fc

Nom du fichier : Setup

Ratio de détection : 47 / 66

Date d'analyse : 2019-04-24 08:46:23 UTC (il y a 4 heures, 18 minutes)

13 0

Analyse | File detail | Relationships | Informations supplémentaires | Commentaires 6 | Votes

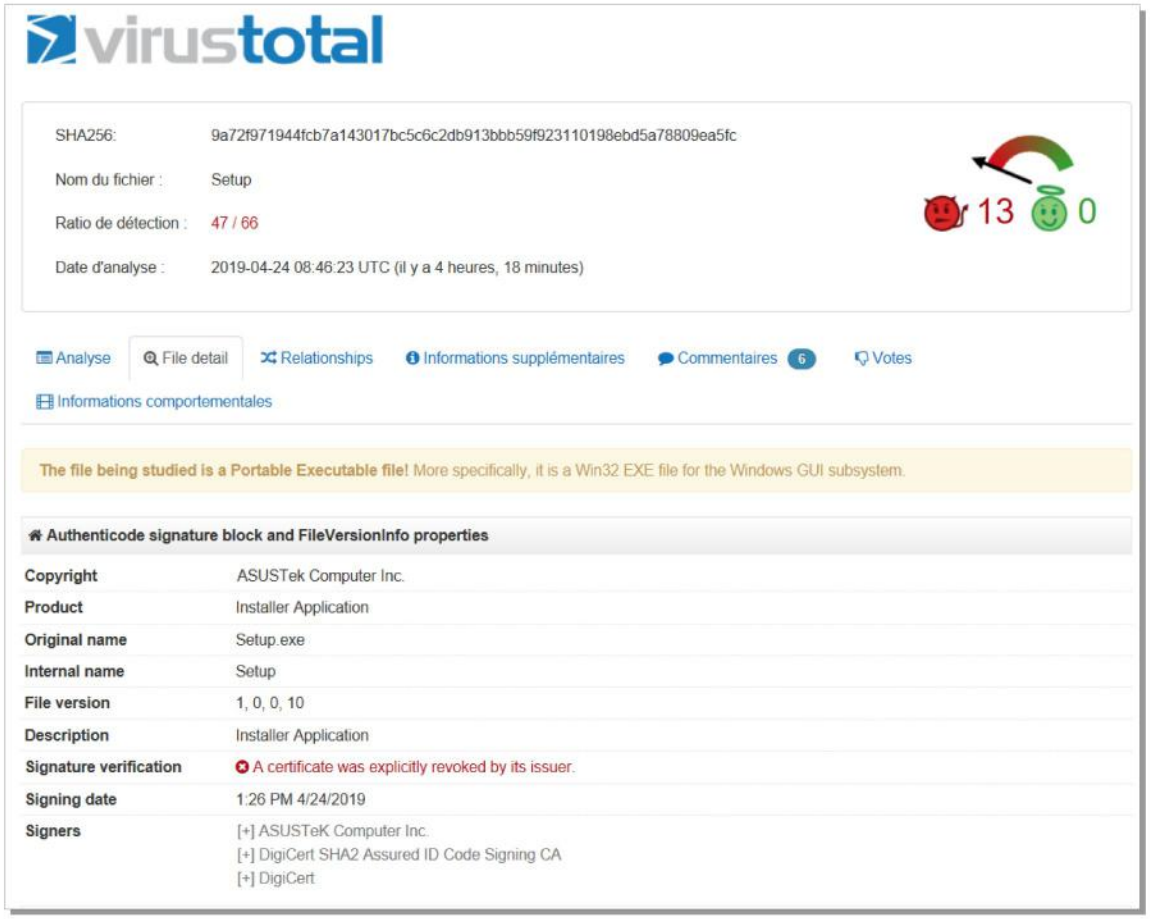
Informations comportementales

| Antivirus | Résultat | Mise à jour |
|---|---|---|
| Ad-Aware | Trojan.ShadowHammer.A | 20190424 |
| AegisLab | Trojan.Win32.ShadowHammer.4!c | 20190424 |
| AhnLab-V3 | Win-Trojan/ShadowHammer.Exp | 20190424 |
| ALYac | Trojan.ShadowHammer.A | 20190424 |
| Antiy-AVL | Trojan/Generic.Generic | 20190424 |
| Arcabit | Trojan.ShadowHammer.A | 20190424 |
| Avast | Win32:ShadowHammer-A [Trj] | 20190424 |
| AVG | Win32:ShadowHammer-A [Trj] | 20190424 |

# Extract behavioural IOCs

- Virustotal report:

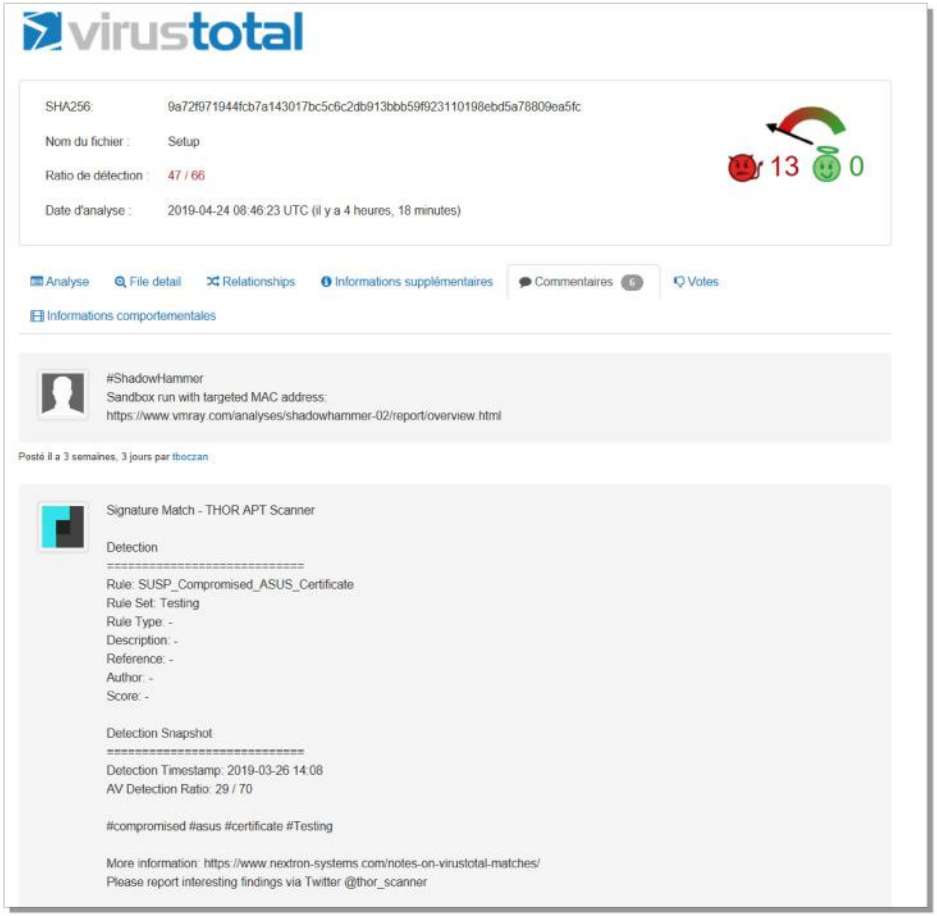
"ShadowHammer" supply chain attack



# Extract behavioural IOCs

- Virustotal report:

"ShadowHammer" supply chain attack



# Extract behavioural IOCs

Interesting tools for static analysis

- Pestudio (https://winitor.com/)
- Cff explorer
- Hxd (hex editor)

# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

## Analysis Report Setup.exe

### Overview

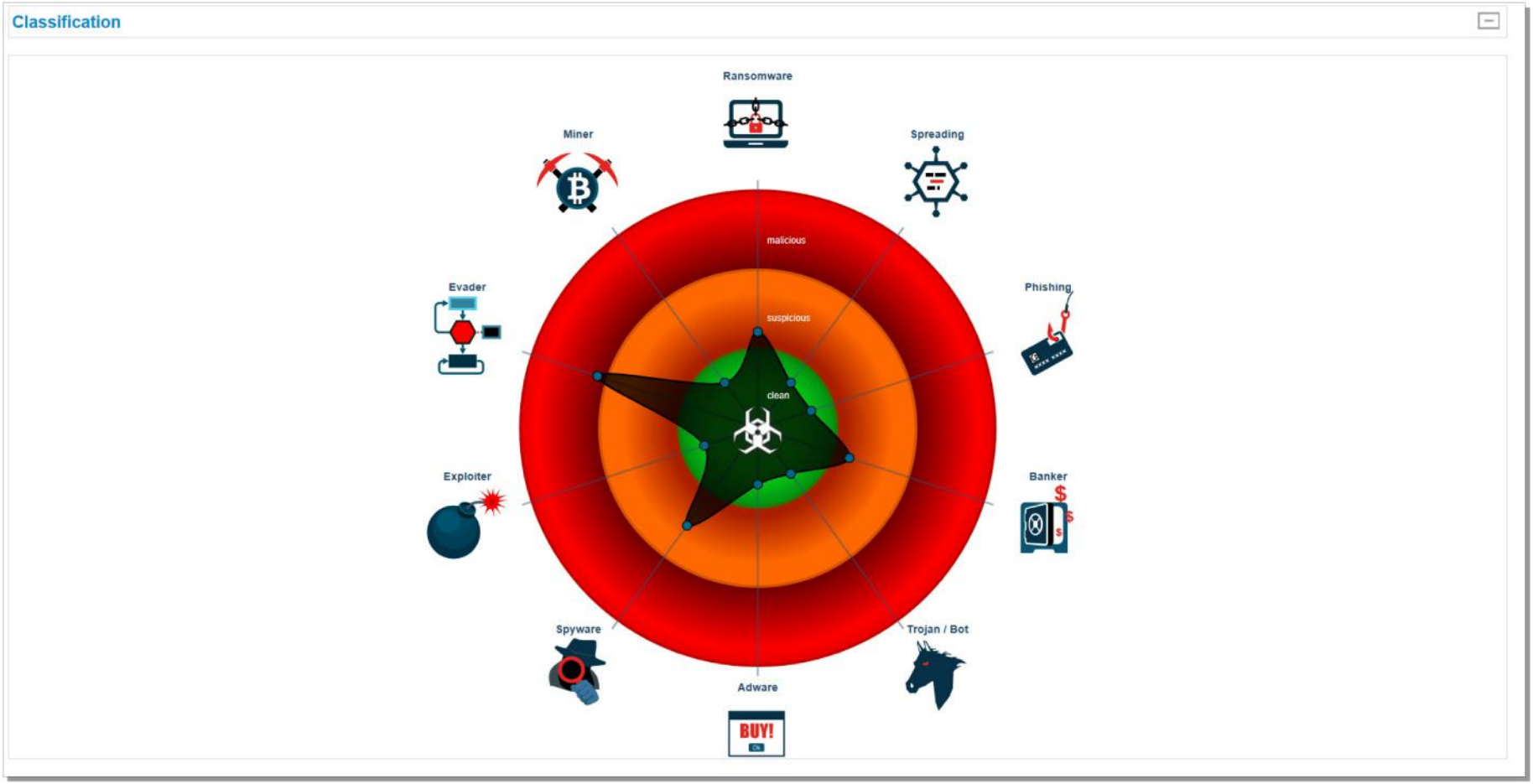
**General Information**

| | |
|---|---|
| Joe Sandbox Version: | 25.0.0 Tiger's Eye |
| Analysis ID: | 825331 |
| Start date: | 26.03.2019 |
| Start time: | 15:20:32 |
| Joe Sandbox Product: | Cloud |
| Overall analysis duration: | 0h 12m 5s |
| Hypervisor based Inspection enabled: | false |
| Report type: | full |
| Sample file name: | Setup.exe |
| Cookbook file name: | defaultwindowsinteractivecookbook.jbs |
| Analysis system description: | Windows 7 x64 (Office 2003 SP3, Java 1.8.0_40, Flash 16.0.0.305, Acrobat Reader 11.0.08, Internet Explorer 11, Chrome 41, Firefox 36) |
| Number of analysed new started processes analysed: | 19 |
| Number of new started drivers analysed: | 1 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies | • HCA enabled<br>• EGA enabled<br>• HDC enabled |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal68.evad.winEXE@13/20@7/2 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 98.9% (good quality ratio 94.9%)<br>• Quality average: 82.1%<br>• Quality standard deviation: 25.6% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

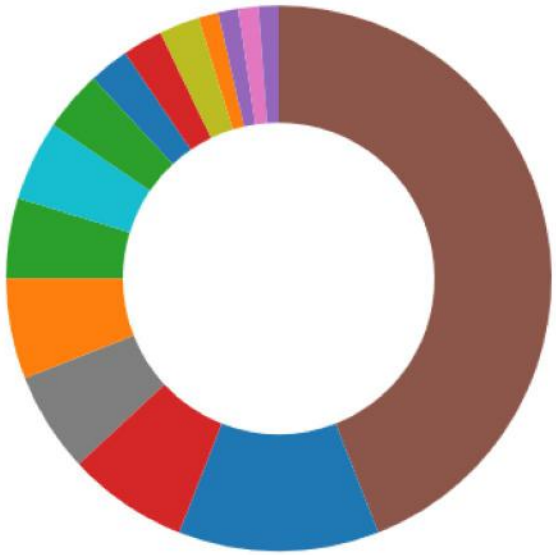


# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

**Signature Overview**

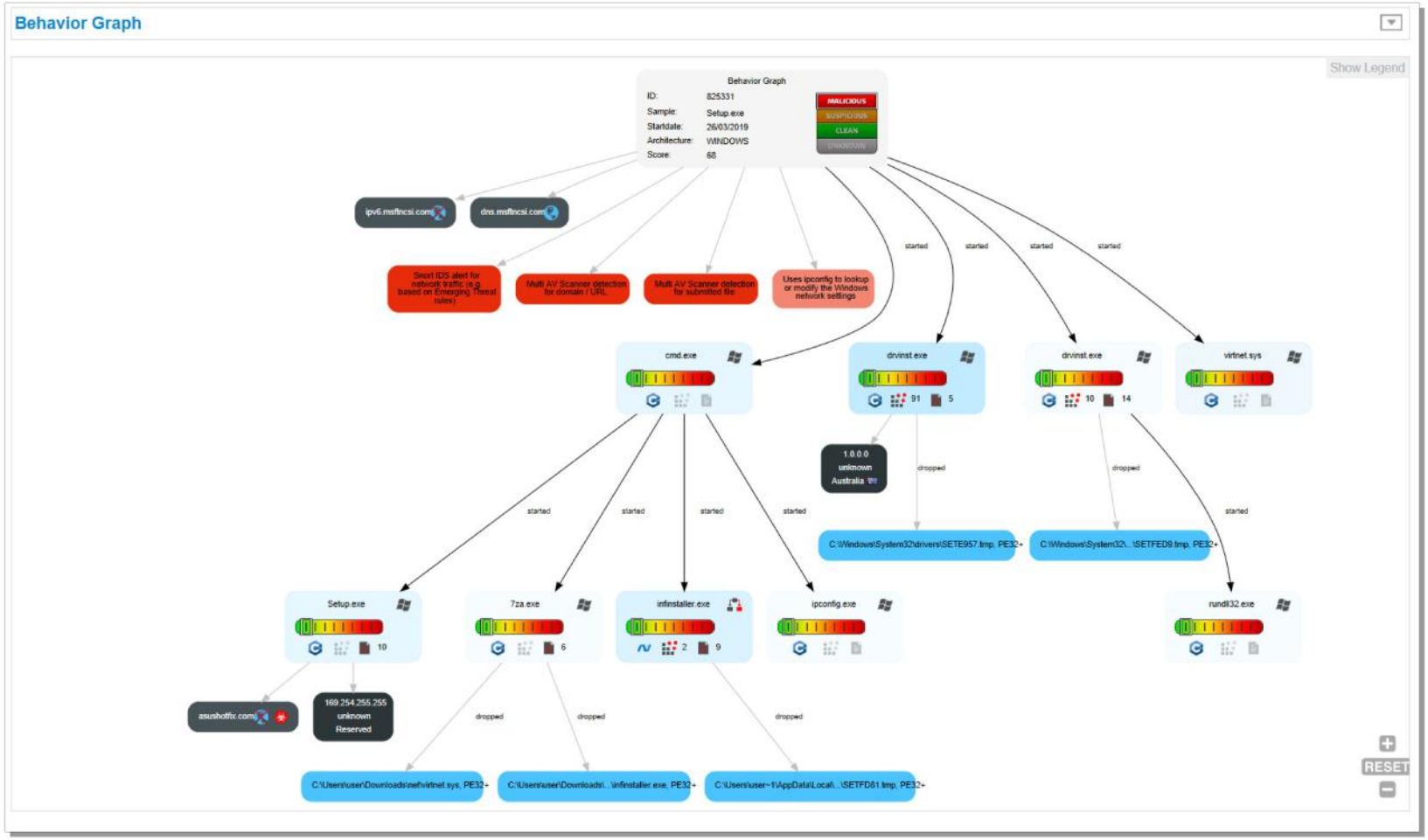


- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings

# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack



# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

**Contacted Domains**

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| dns.msftncsi.com | 131.107.255.255 | true | false | | high |
| ipv6.msftncsi.com | unknown | unknown | false | | high |
| asushotfix.com | unknown | unknown | true | 13%, virustotal, Browse | unknown |

# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

## Created / dropped Files

| C:\System Volume Information\SPP\OnlineMetadataCache\{5a09dc67-7c6a-4b93-a2d6-1d1015663466}_OnDiskSnapshotProp | |
|---|---|
| Process: | C:\Windows\System32\drvinst.exe |
| File Type: | data |
| Size (bytes): | 1680 |
| Entropy (8bit): | 3.794130244868423 |
| Encrypted: | false |
| MD5: | 27447620A1E276F8DB727001513913D7 |
| SHA1: | 1CD0A52CE2726D5C4146F84BC1FF342E02D1789A |
| SHA-256: | 1B2F32656AC3183033F76631C4DA8BF3EAD0C69BC1F8CAE8D8535AC6D1131703 |
| SHA-512: | 4C0C8CB8BF4B34670C6ED7FB35ABBC862D183185D796B5F9DFA3748F42D046942D5CC7250C2061FECEB2CF5EC32462AFDB719968309233D7507ED564681A800F |
| Malicious: | false |
| Reputation: | low |

| C:\System Volume Information\SPP\metadata-2 | |
|---|---|
| Process: | C:\Windows\System32\drvinst.exe |
| File Type: | SysEx File - Twister |
| Size (bytes): | 8697024 |
| Entropy (8bit): | 3.671807434960589 |
| Encrypted: | false |
| MD5: | 3B435A9265689328BC2CDC1AD52F6D52 |
| SHA1: | FAFEFBDB18B1EC565D6FBAF695D99A8F8B75913B |
| SHA-256: | F414D8732194F66C7F8B5B179CC4450754BE0C15D043C5B9F88E63D49C545A8B |
| SHA-512: | 3D7403D80364292088E180733F5F1709E6FB677EE7E9E5F0675F10033BE08CF004FC242756BFCE0747BF45577DA4F48C145D72C6B4C3BBB26BE122A3BB8C8895 |
| Malicious: | false |

# Extract behavioural IOCs

- Joe sandbox report:

"ShadowHammer" supply chain attack

- What IOCs did we extract ?

1. IP / domains
2. Dropped files and their full path
3. Behaviour

# Extract behavioural IOCs

- Never rely on one sandbox only !
- Possible to evade sandboxes
- In fact almost all malware implement some sort of anti-sandbox or antivm

- Example of other report:
- https://www.vmray.com/analyses/shadowhammer-02/report/behavior_grouped.html

# How to hunt for new samples ?

- Let's introduce **YARA**

# Yara

- YARA is an acronym for: YARA: Another Recursive Acronym, or Yet Another Ridiculous Acronym. Pick your choice.
- Pattern matching tool

- http://virustotal.github.io/yara/
- https://github.com/InQuest/awesome-yara

# Yara

- Example dummy rule:

```
rule dummy
 {
condition:
false
 }
```

# Yara

- Yara keywords

| | | | | | | |
|---|---|---|---|---|---|---|
| all | and | any | ascii | at | condition | contains |
| entrypoint | false | filesize | fullword | for | global | in |
| import | include | int8 | int16 | int32 | int8be | int16be |
| int32be | matches | meta | nocase | not | or | of |
| private | rule | strings | them | true | uint8 | uint16 |
| uint32 | uint8be | uint16be | uint32be | wide | | |

# Yara

- Comments

```
/*
    This is a multi-line comment ...
*/

rule CommentExample   // ... and this is single-line comment
{
    condition:
       false  // just an dummy rule, don't do this
}
```

# Yara

- Rule example

```
rule ExampleRule
{
    strings:
        $my_text_string = "text here"
        $my_hex_string = { E2 34 A1 C8 23 FB }

    condition:
        $my_text_string or $my_hex_string
}
```

# Yara

- Rule example

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

# Yara

- Let's write the yara rule for a sample of "shadowhammer"

- strings binary on linux or strings from "sysinternals" (https://docs.microsoft.com/en-us/sysinternals/downloads/strings)
  - Be careful with strings on linux and encoding !

From man strings:

```
… --encoding=encoding
Select the character encoding of the strings that are to be found. Possible values for encoding are: s = single-7-bit-byte characters ( ASCII , ISO 8859, etc., default), S = single-8-bit-byte characters, b = 16-bit bigendian, l = 16-bit littleendian, B = 32-bit bigendian, L = 32-bit littleendian. Useful for finding wide character strings. (l and b apply to, for example, Unicode UTF-16/UCS-2 encodings).
…
```

# Yara

- Let's write the yara rule for a sample of "shadowhammer"

**DEMO**

# Yara

```
rule ShadowHammer {
   meta:
      description = "shadowhammer detection"
      date = ""
      author = ""
      license = ""
      hash1 = "ac0711afee5a157d084251f3443a40965fc63c57955e3a241df866cfc7315223"
      reference = "https://securelist.com/operation-shadowhammer/89992/"
   strings:
      $x1 = "\\AsusShellCode\\Release" ascii
      $x2 = "\\AsusShellCode\\Debug"
   condition:
      uint16(0) == 0x5a4d and 1 of them
}
```

# Yara

- Nice tool written by Florian Roth to help starting a yara rule:

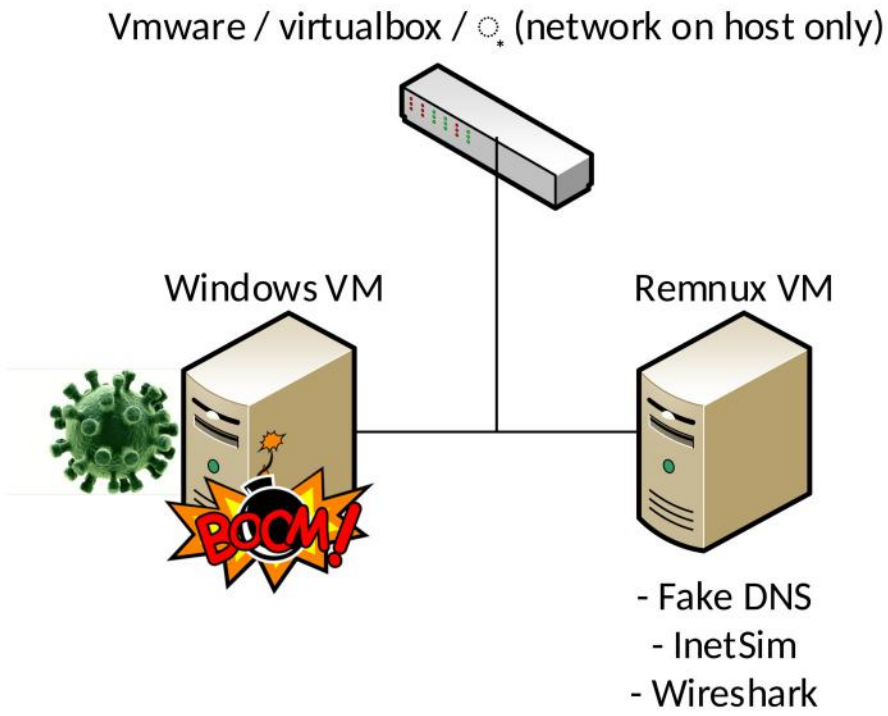
https://github.com/Neo23x0/yarGen

*"The main principle is the creation of yara rules from strings found in malware files while removing all strings that also appear in goodware files. Therefore yarGen includes a big goodware strings and opcode database as ZIP archives that have to be extracted before the first use."*

# Malware dynamic analysis

- We can implement or own network setup for dynamic analysis
- One victim (get a 90 days windows vm: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/)
- One machine recording traffic and providing network ("remnux" linux distribution, *https://remnux.org/).*

# Malware dynamic analysis



# Malware dynamic analysis

## Remnux side

- Fakedns is a python script that answer to any dns request with the IP of the remnux host (http://code.activestate.com/recipes/491264-mini-fake-dns-server/)
- Inetsim is a software suite for simulating common internet services (https://www.inetsim.org/)
- Wireshark is network protocol analyzer (but you should know that, https://www.wireshark.org/)

# Malware dynamic analysis

## Windows side (“victim”)

- Use “FlareVM” scripts (https://github.com/fireeye/flare-vm)
- Interesting tools like “Regshot”, “procmon”, ...

# Malware dynamic analysis

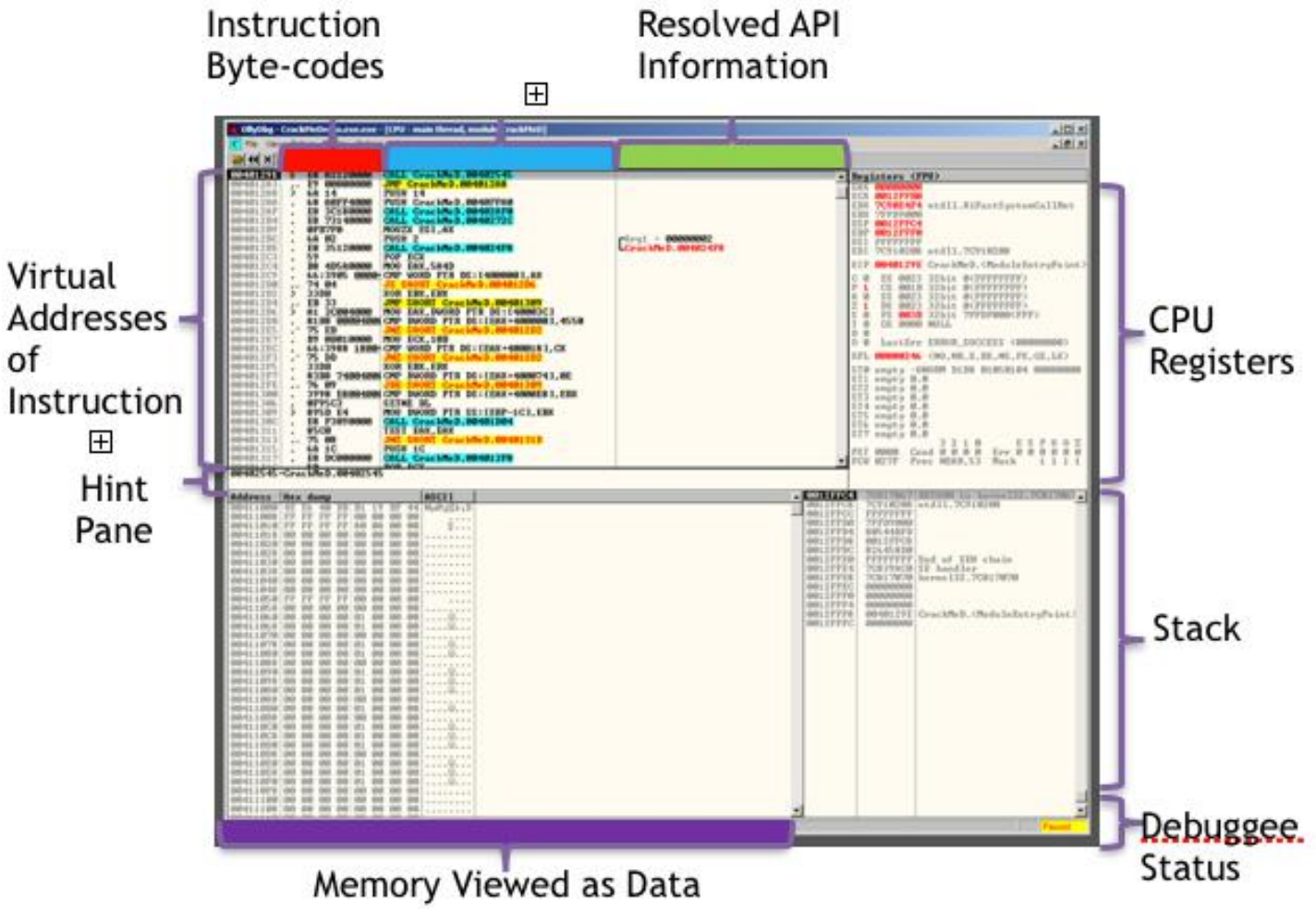
## Remnux and Windows

## DEMO

# Malware dynamic analysis

- Running in a debugger
- ollydbg 32 bits only and old
- X64dbg (https://x64dbg.com/) better, 32 and 64 bits

# Malware dynamic analysis



# Malware dynamic analysis

## Ollydbg or xdbg64 Hotkeys

There are several hotkeys that you will find useful during your debugging session.
They are:

- F7 – the Step Into command. This key single-step traces one instruction at a time
- F8 – the Step Over command. This key single-step traces one instruction except for CALL instructions. When used on a CALL, F8 sets a breakpoint after the CALL and runs the debuggee. This is handy for stepping over C-runtime libraries, such as printf, scanf, etc.
- F9 – Run. Runs the debuggee
- F2 – Set Breakpoint sets a software breakpoint on the currently selected instruction.

# Malware dynamic analysis

- Running the malware in a debugger
- Shadowhammer practical view

**DEMO**

# Malware static analysis

There are multiple tools for disassembly:

- The leader is still IDA pro (closed source and commercial)
- Binary ninja, commercial but cheaper than IDA pro
- Radare, opensource and promising
- Ghidra (NSA tool)

# Malware static analysis

*Pro tip: When you face java or .net binaries, don't try to use IDA pro*

Multiple tools exists to get the high level language (C# or VB):

- ilspy: https://github.com/icsharpcode/ILSpy#ilspy-------
- Dotpeek (based on resharper): https://www.jetbrains.com/decompiler/
- JD-gui: https://java-decompiler.github.io/

# Malware static analysis

Let’s open a shadowhammer sample in IDA pro (sha256: 6aedfef62e7a8ab7b8ab3ff57708a55afa1a2a6765f86d581bc99c738a68fc74)

# Malware static analysis

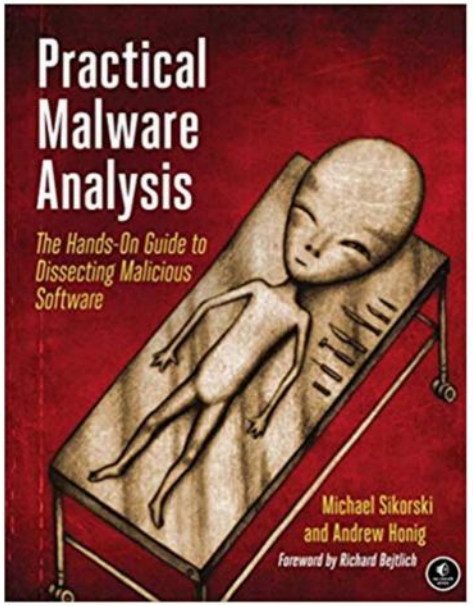
Hybrid Reverse Engineering

- IDA pro
- Debugger

*protip: Disable ASLR of the PE (https://blog.didierstevens.com/2010/10/17/setdllcharacteristics/)*

***DEMO***

# Malware Reverse Engineering




Going further:

- Crackmes
- FlareON challenges (version 1 to 4)
- “Practical Malware Analysis” book

  ( ISBN-13: 978-1593272906, ISBN-10: 1593272901 )

- Practice, practice, practice


Questions?