Automated Malware Analysis

Alessandro **@jekil** Tanasi

MALWARE?

Malicious soft**ware**: software utilizzato a fini malevoli, per danneggiare, rubare, abusare o accedere in modo fraudolento e non autorizzato.

- Virus, Worm, Trojan
- Cryptolocker
- Spyware
- Malware di Stato

HACKINBO

WHY?

Perché scrivere malware?

- Fama
- Business ($$$)
- Spionaggio
- Red team

Perché analizzare malware?

- Incident response
- Defensive security
- Identificare vulnerabilità
- Investigazione e Intelligence

HackInBo

ANALISI MALWARE

Static Analysis: analizzare il malware senza eseguirlo.

- File identification, analisi header, strings, ecc.
- Dissassembler

Dynamic Analysis: analizzare il malware eseguendolo in modo controllato.

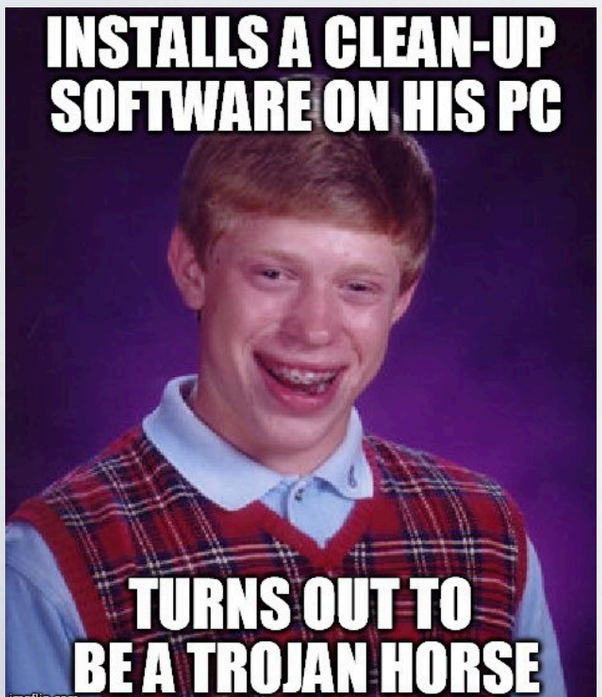
- Memory forensics, network monitoring, etc.
- Debuggers

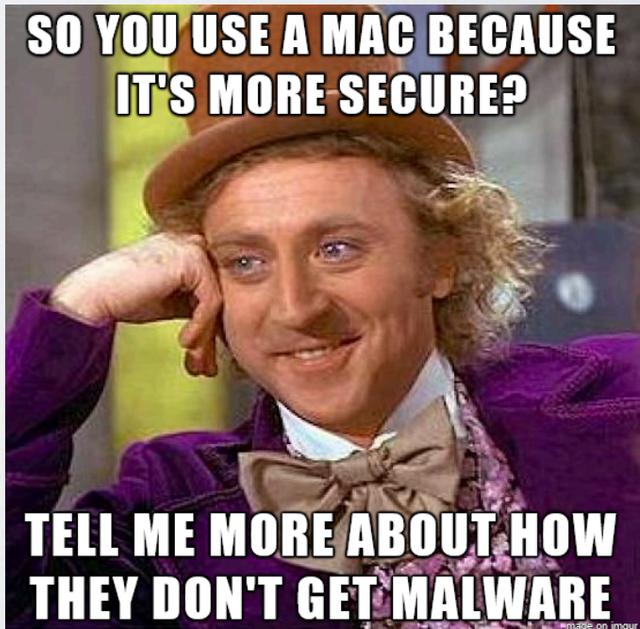
BIG FAT WARNING!!

✓**Segregazione** fra rete per l'analisi malware e le altre.

✓Macchine **dedicate** all'analisi malware.

✓**Igiene** nella gestione dei malware.





HACKINBO

TOOLS

(LIMITED SET OF…)

Network Monitoring
Wireshark
SmartSniff
Bro
InetSim

Process Monitoring
Process Explorer
Process Hacker

File System & Registry Monitoring
Process Monitor
Capture BAT
RegShot

Disassembler & Debugger
OllyDbg
Immunity Debugger
IDA Pro
Radare2

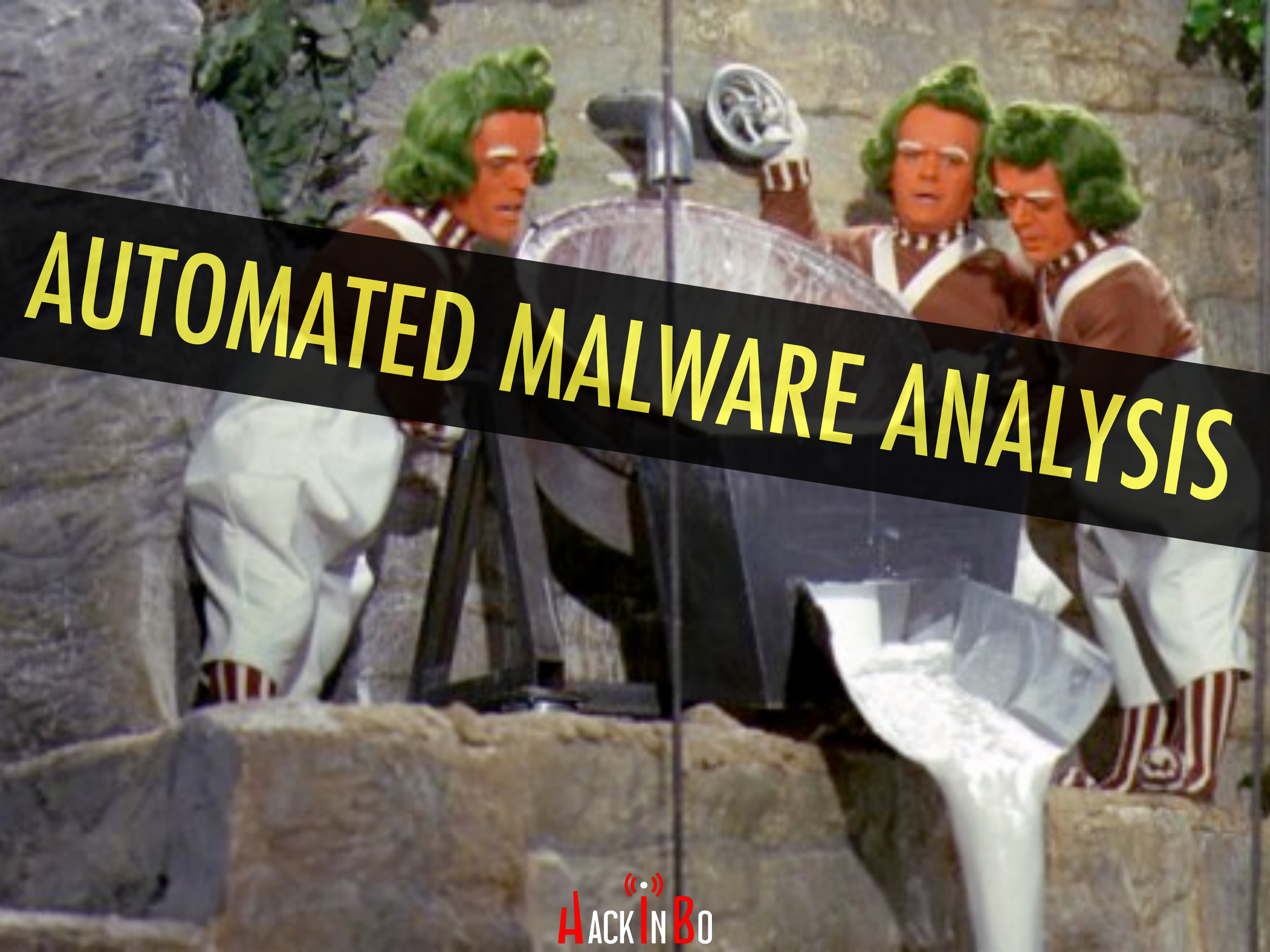
Memory Dumper
LordPE
OllyDump

Memory Analysis
Volatility
Rekall

Documents
Peepdf
PDF Tools

OSINT
Virustoral
Maltego
Intel / IOC resources

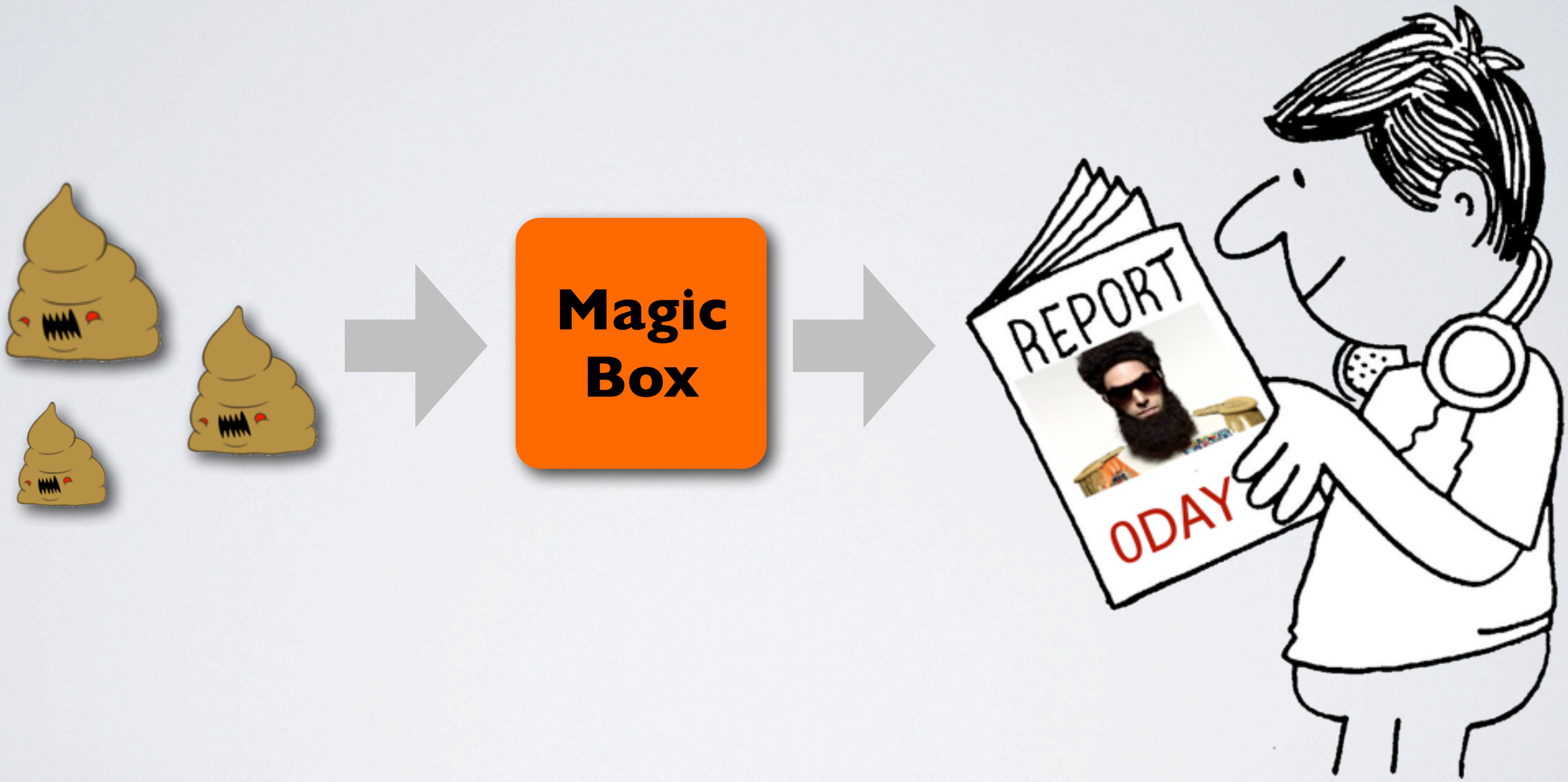
HACKINBO



AUTOMATED MALWARE ANALYSIS

HackInBo

IDEA?!



SANDBOX

- Meccanismo per **isolare** l'esecuzione del software.
- Mette a disposizione un set limitato e **controllato** di **risorse** hardware e software.
- Usato per eseguire software **non fidato**.
- Paradigma utilizzato in security e **malware analysis**.

SANDBOX & MALWARE

- Esecuzione del malware in ambiente **isolato**.
- Monitoraggio del suo **funzionamento**.
- Monitoraggio delle **interazioni** con le risorse HW/SW.
- Software o hardware.

SANDBOX VS MALWARE

- Grandi **quantità** di malware.
- **Automazione** totale e flessibilità.
- Integrazione con altri strumenti di sicurezza.
- Analisi con risultati comparabili con quella manuale.

HACKINBO

SCOPI

- **Analisi** Malware.
- **Ricerca** di minacce.
- **Forensics** e incident response.
- Sistemi integrati per la sicurezza.

WANTED!

HACKINBO

MA..

- Prodotti commerciali **costosi** e **closed** source.
- Setup complessi.
- Nessuna o poco flessibilità.
- Svantaggiosi per studenti, **ricercatori**, ecc.

HackInBo

CUCKOO SANDBOX

- Sandbox per **analisi automatizzata** di malware.
- Progettata per essere **facile** da usare.
- Progettata per essere totalmente **personalizzabile**.

Free as in Freedom

HACKINBO

FUNZIONALITÀ

- Completamente **automatizzata**.
- **Personalizzabile** in ogni sua parte: tutto è modulare.
- Analisi parallela, analisi distribuita.
- Tracciamento **API calls**.
- Memory dump.
- Analisi traffico di **rete**.
- Dump file.
- Screenshots.
- **Signature**.

HACKINBO

TEAM

Claudio *nex* Guarnieri
Lead developer
@botherder

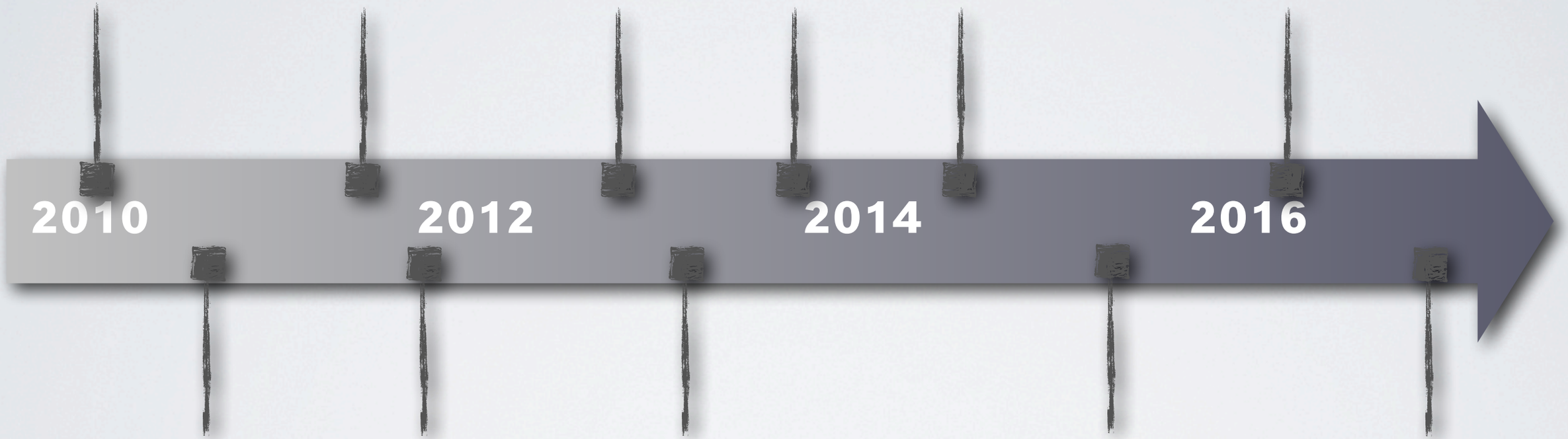
Alessandro jekil Tanasi
Core developer
@jekil

Mark rep Schloesser
Core developer
@repmovsb

Jurriaan skier Bremer
Core developer
@skier_t

HACKINBO

MAJOR RELEASES

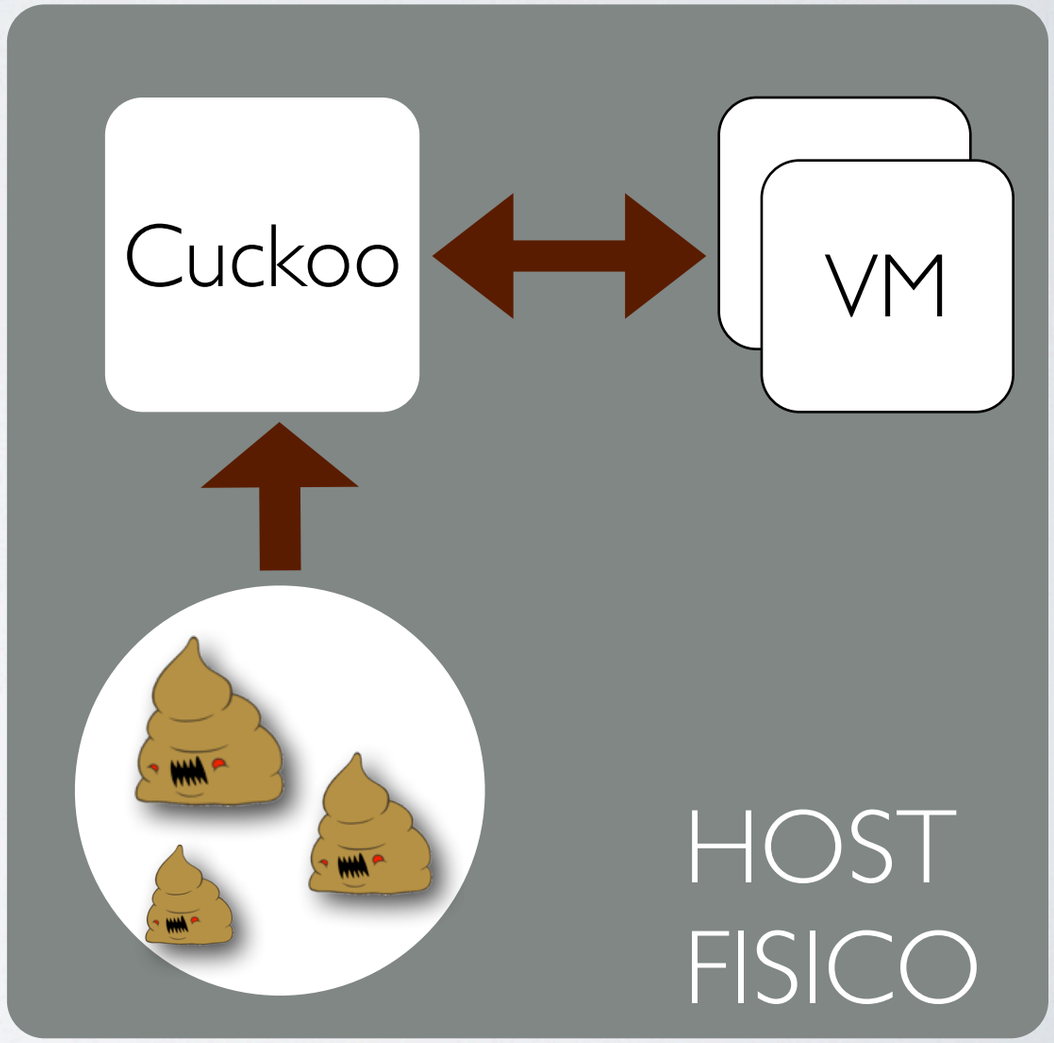


HACKINBO

ARCHITETTURA

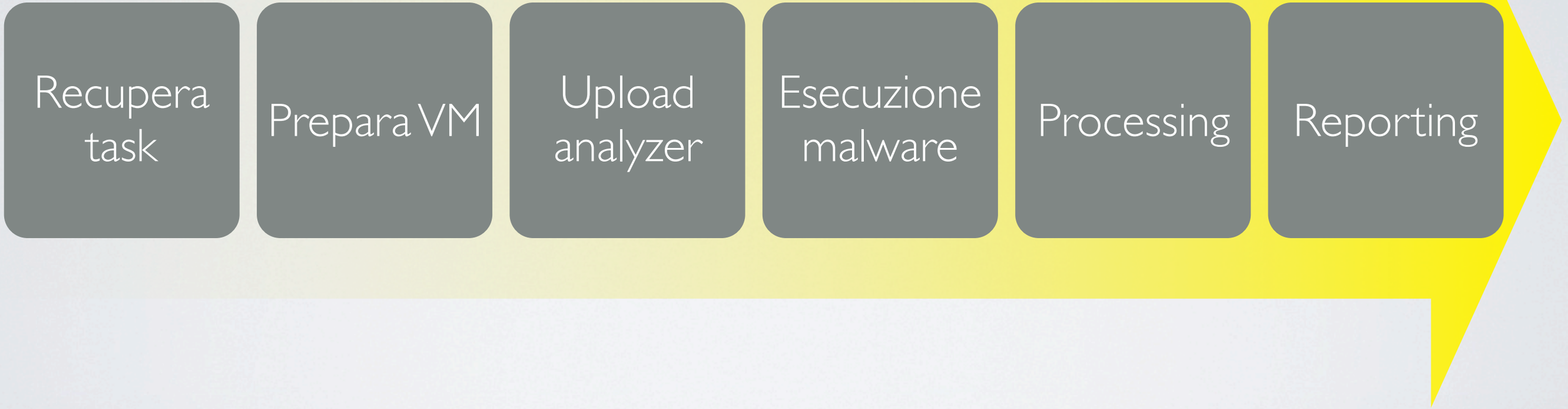
ARCHITETTURA

- Host GNU/**Linux**.
- Software di **virtualizzazione** (VirtualBox, KVM/libvirt, Vmware, XEN).
- Macchine virtuali (**VM**) o fisiche in cui eseguire il malware.



HACKINBO

CICLO DI ANALISI

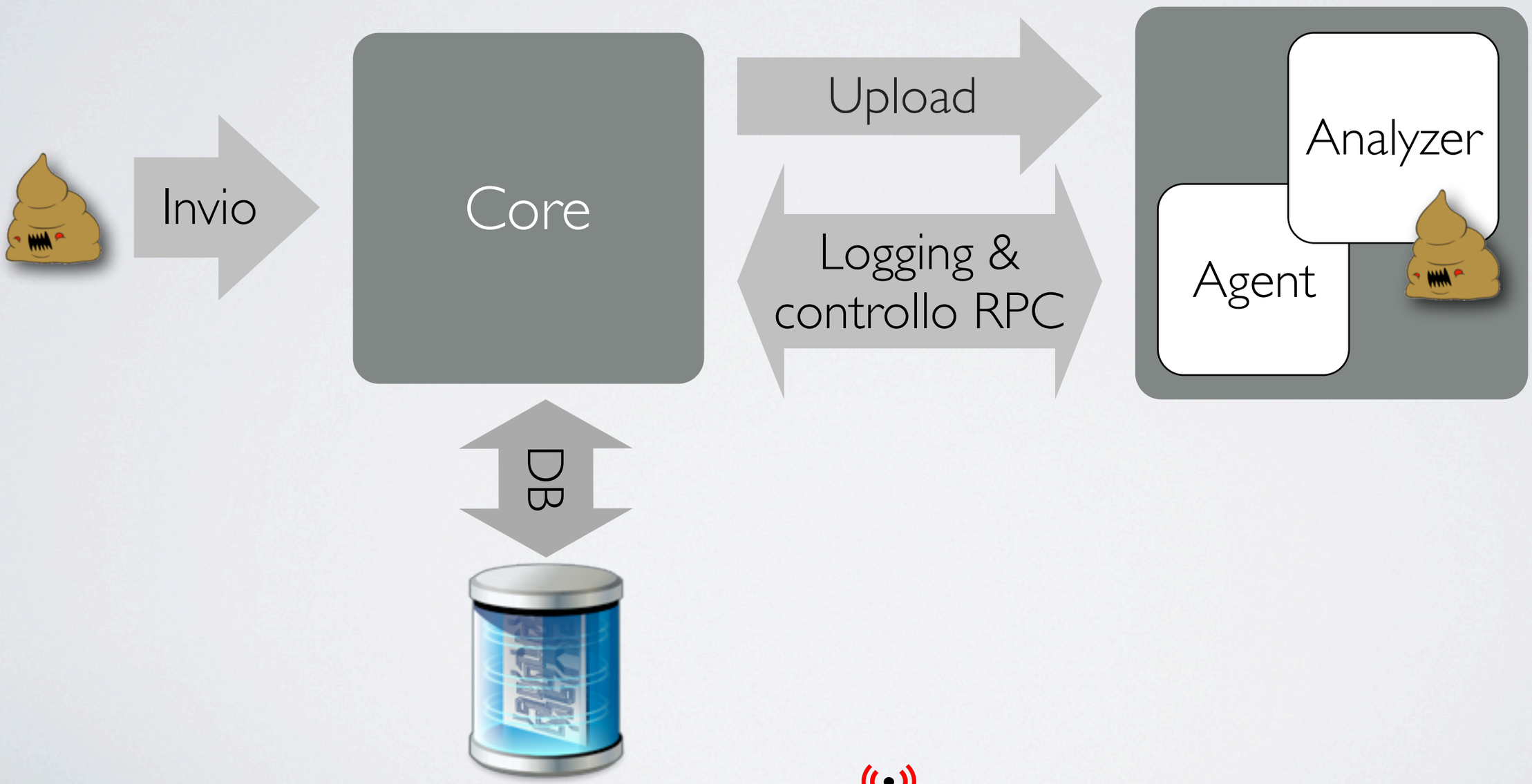


HACKINBO

COMPONENTI

- **Core deamon**
  - Gestisce il processo di analisi, i moduli e le VM.
- **Analyzer**
  - All'interno della VM **esegue** il sample e comunica al core le sue azione.
  - Modulare: per ogni sistema operativo.

CICLO DI ANALISI



HACKINBO

CUCKOO MONITOR

- Instrumentation via **DLL** injection.
- Hooking delle principali funzioni (circa 170 **APIs**).
- Logging in real time via network.
- Traccia i **processi** child o injected.
- Codice in C.

https://github.com/cuckoosandbox/monitor

THE BIG PICTURE

VM Win 7 | VM Linux | VM Mac OSX | Android | Physical

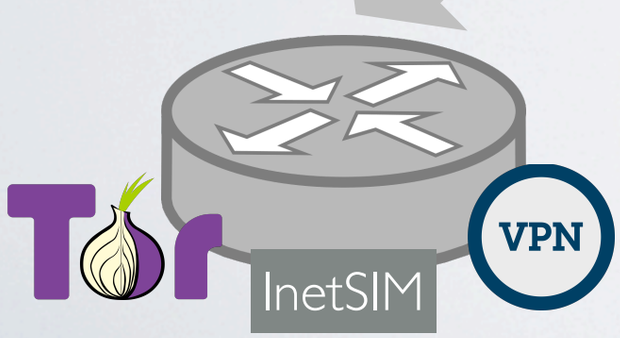
Cuckoo Framework

API

Networking

Data

Ext Tools



- MISP
- Moloch
- VirusTotal
- etc.

HACKINBO

MODULI

HACKINBO

MACHINERY

- Interagiscono con il software di **virtualizzazione**
- Codice Python in ***cuckoo/machinery/***
- Software supportati:
  - VirtualBox
  - VMWare Workstation
  - QEMU/KVM
  - XenServer
  - Base class LibVirt

```python
import logging

from lib.cuckoo.common.abstracts import LibVirtMachinery

class KVM(LibVirtMachinery):
    """Virtualization layer for KVM based on python-libvirt."""

    # Set KVM connection string.
    dsn = "qemu:///system"
```

AUXILIARY

- Eseguiti in **parallelo** all'analisi.
- Codice Python in **cuckoo/auxiliary/**
- Esempio:
  - Network sniffer
  - MitmProxy
  - Reboot detection

PROCESSING

- **Elaborano** i dati grezzi di analisi
- Codice Python in ***cuckoo/processing/***
  - Analysis Info
  - File Hashes, Analisi header PE32
  - Yara Signatures
  - Behavior Analysis
  - Dropped Files
- Analisi del memory dump con Volatility
- Analisi traffico di rete
  - TLS master key
  - Strings
  - Ricerca VirusTotal
  - Integrazione MISP, IRMA

```python
import os.path
import re

from cuckoo.common.abstracts import Processing
from cuckoo.common.exceptions import CuckooProcessingError

class Strings(Processing):
    """Extract strings from analyzed file."""
    MAX_FILESIZE = 16*1024*1024
    MAX_STRINGCNT = 2048
    MAX_STRINGLEN = 1024

    def run(self):
        """Run extract of printable strings.
        @return: list of printable strings.
        """
        self.key = "strings"
        strings = []

        if self.task["category"] == "file":
            if not os.path.exists(self.file_path):
                raise CuckooProcessingError(
                    "Sample file doesn't exist: \"%s\"" % self.file_path
                )

            try:
                data = open(self.file_path, "r").read(self.MAX_FILESIZE)
            except (IOError, OSError) as e:
                raise CuckooProcessingError("Error opening file %s" % e)

            strings = re.findall("[\x1f-\x7e]{6,}", data)
            for s in re.findall("(?:[\x1f-\x7e][\x00]){6,}", data):
                strings.append(s.decode("utf-16le"))

        # Now limit the amount & length of the strings.
        strings = strings[:self.MAX_STRINGCNT]
        for idx, s in enumerate(strings):
            strings[idx] = s[:self.MAX_STRINGLEN]

        return strings
```

SIGNATURES

- Scattano in corrispondenza di determinati **eventi** o **comportamenti**.
- Codice Python
- Esempi:
  - Riconoscere famiglie
  - Estrarre ulteriori dettagli (configurazioni)
- Community repository

  https://github.com/cuckoobox/community

```python
from lib.cuckoo.common.abstracts import Signature

class Prinimalka(Signature):
    name = "banker_prinimalka"
    description = "Detected Prinimalka banking trojan"
    severity = 3
    categories = ["banker"]
    families = ["prinimalka"]
    authors = ["nex"]
    minimum = "2.0"

    filter_apinames = "RegSetValueExA", "RegSetValueExW"

    def on_call(self, call, process):
        regkey = call["arguments"]["regkey"].lower()
        if regkey.endswith("_opt_server1"):
            self.mark_call()
            self.mark_ioc("cnc", call["arguments"]["value"])
            return True

```

REPORTS

- Presentano le informazioni in vari **formati**.
- Codice Python in ***cuckoo/reporting/***
- Default reports:
  - JSON
  - HTML
  - Database: MongoDB, Elasticsearch
  - External tools: MISP, Moloch, Mattermost

```python
import calendar
import datetime
import json
import requests

from cuckoo.common.abstracts import Report
from cuckoo.common.exceptions import CuckooReportError

def default(obj):
    if isinstance(obj, datetime.datetime):
        if obj.utcoffset() is not None:
            obj = obj - obj.utcoffset()
        return calendar.timegm(obj.timetuple()) + obj.microsecond / 1000000.0
    raise TypeError("%r is not JSON serializable" % obj)

class Notification(Report):
    """Notifies external service about finished analysis via URL."""
    order = 3

    def run(self, results):
        post = {
            "task_id": self.task["id"],
            "identifier": self.options.get("identifier"),
            "data": json.dumps(
                results.get("info"), default=default, sort_keys=False
            )
        }

        try:
            requests.post(self.options.get("url"), data=post)
        except Exception as e:
            raise CuckooReportError(
                "Failed posting message via Notification: %s" % e
            )
```

ANALYSIS PACKAGES

- **Lanciano** il sample in base al suo tipo (URL, Office, etc)
- Codice Python in **data/*analyzer/$OS/modules/packages/***
- Default packages:
  - Java applet, DLL, Word, executable, HTML, URL (Internet Explorer), Java JAR, Adobe PDF, VBS, Excel, ZIP

```python
import os

from lib.common.abstracts import Package

class HTA(Package):
    """HTA analysis package."""
    PATHS = [
        ("System32", "mshta.exe"),
    ]

    def start(self, path):
        mshta = self.get_path("mshta")

        # Enforce .hta extension.
        if not path.endswith(".hta"):
            os.rename(path, path + ".hta")
            path += ".hta"

        return self.execute(mshta, args=[path])
```

ANALYSIS AUXILIARY

- Eseguiti **parallelamente** al sample
- Codice Python in **data/*analyzer/$OS/modules/auxiliaries/***
- Esempi: muovere il mouse, screenshots

```
5   import logging
6
7   from lib.api.process import Process
8   from lib.common.abstracts import Auxiliary
9   from lib.common.exceptions import CuckooError
10
11  log = logging.getLogger(__name__)
12
13  class DumpTLSMasterSecrets(Auxiliary):
14      """Dump TLS master secrets as used by various Windows libraries."""
15      def start(self):
16          try:
17              p = Process(process_name="lsass.exe")
18              p.inject(track=False, mode="dumptls")
19          except CuckooError as e:
20              if "process access denied" in e.message:
21                  log.warning(
22                      "You're not running the Cuckoo Agent as Administrator. "
23                      "Doing so will improve your analysis results!"
24                  )
25              else:
26                  log.warning(
27                      "An unknown error occurred while trying to inject into "
28                      "the lsass.exe process to dump TLS master secrets: %s", e
29                  )
```

SETUP

HackInBo

DOWNLOAD

- Via **PIP**:

```
pip install cuckoo
```

- Dal **sito** ufficiale:

  http://www.cuckoosandbox.org

- Da **GitHub**:

  http://github.com/cuckoobox/cuckoo

INSTALLAZIONE

- Installare Cuckoo da pip
- Installare le **dipendenze** (da manuale)
- Creare una VM per l'analisi, eseguirci ***agent.py***, e fare uno snapshot
- Configurare il networking
- Modificare a piacimento la configurazione in ***.cuckoo***

CREAZIONE VM

- Diverse VM per **requisiti**
  - Sistema operativo e livello di patching
  - Architettura CPU
  - Applicativi installati (exploitable)
- Anti VM detection
- Fake stuff: credenziali, ecc.
- Eseguire ***agent.py***
- Fare **snapshot**
- **Vmcloack** to the rescue!

HACKINBO

CONFIGURAZIONE

- Configurazione generale
- Configurazione VM
- Sniffer
- Processing
- Reports

La configurazione deve essere **calibrata** sul risultato voluto

HACKINBO

UTILIZZO

SAMPLE SUBMISSION

- Via **console**: ***cuckoo submit $FILE***
- Via **API**: ***cuckoo api***
- Via interfaccia **web**
- Via codice **Python**

```
5   from cuckoo.core.database import Database
6   db = Database()
7   db.add_path("/tmp/malware.exe")
```

OPZIONI DI SUBMISSION

- Package di analisi e opzioni
- Timeout
- Priorità dell'analisi
- Virtual machine name
- Virtual machine platform
- Virtual machine tag
- Memory dump (VM)
- Memory dump (processo)
- Clock

RISULTATI

- Folder di analisi ***data/storage/analysis/{id}/***

- Il contenuto dipende dall'esito dell'analisi.

- Il contenuto dipende dai moduli abilitati.

HACKINBO

WEBAPP

- Django web application in **data/*web/***
- Submission con opzioni
- **Ricerca** di analisi
- Report **interattivo**
- **Comparazione** analisi.
- Monitoraggio sistema.
- Import / **export** analisi.

cuckoo Dashboard Recent Pending Search Submit Import

Insights

Cuckoo Installation

Version	2.0.4

Usage statistics

reported	395
completed	1
total	400
running	4
pending	0

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

Submit URLs/hashes

Submit

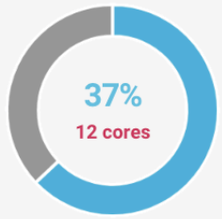
Drag your file into the left field or click the icon to select a file.

System info

free used total

FREE DISK SPACE

CPU LOAD



MEMORY USAGE

HACKINBO

Summary

cuckoo-40791a2bca437918bd35f212c96c6d0c2b4522cc49af13272a4560d05ec8d50a

File *cuckoo-40791a2bca437918bd35f212c96c6d0c2b4522cc49af13272a4560d05ec8d50a*

Summary

Download | Resubmit sample

Size	3.7MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
MD5	`b680a84bf8220dc7a0f802753e4ad553`
SHA1	`bfc6fa1f2793dda97f4f35485dcdbf566ec98f47`
SHA256	`40791a2bca437918bd35f212c96c6d0c2b4522cc49af13272a4560d05ec8d50a`
SHA512	Show SHA512
CRC32	`D857001D`
ssdeep	`49152:BYl8WhqlmZo0I0xZoDkzpMSUWZBVT74cwIlgUjcwMwx8UxSrrS9ouZmOAYnuj+u7:BYCW0luI0zos91BeC3JmU8mOsAO8+uhh`
Yara	None matched

Score

This file is **very suspicious**, with a score of **8.2 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

Information on Execution

Analysis

Category	Started	Completed	Duration	Logs
FILE	Oct. 13, 2017, 5:09 p.m.	Oct. 13, 2017, 5:09 p.m.	25 seconds	Show Analyzer Log Show Cuckoo Log

Summary
Static Analysis
Extracted Artifacts
Behavioral Analysis 2
Network Analysis
Dropped Files 0
Dropped Buffers 6
Process Memory 1
Compare Analysis
Export Analysis
Reboot Analysis
Options
Feedback
Lock sidebar

Signatures

- Queries for the computername (2 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable uses a known packer (1 event)
- One or more processes crashed (1 event)
- One or more potentially interesting buffers were extracted, these generally contain injected code, configuration data, etc.
- Performs some HTTP requests (1 event)
- Allocates read-write-execute memory (usually to unpack itself) (1 event)
- Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (3 events)
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- The executable is compressed using UPX (2 events)
- One or more of the buffers contains an embedded PE file (1 event)
- Detects virtualization software with SCSI Disk Identifier trick(s) (2 events)
- Creates known Bancos Banking Trojan files, registry keys and/or mutexes

Process contents

cuckoo-40791a2bca437918bd35f212c96c6d0c2b4522cc49af13272a4560d05ec8d50a.exe

PID 2240

Parent PID 2216

1 2 3 4 5

default registry file network process services synchronisation iexplore office pdf

Time & API	Arguments	Status	Return	Repeated
LdrLoadDll Oct. 13, 2017, 5:09 p.m.	module_name: KERNEL32.DLL basename: KERNEL32 stack_pivoted: 0 flags: 0 module_address: 0x770a0000	1	0	0
LdrGetProcedureAddress Oct. 13, 2017, 5:09 p.m.	ordinal: 0 function_address: 0x770b10ff function_name: Sleep module: kernel32 module_address: 0x770a0000	1	0	0
LdrLoadDll Oct. 13, 2017, 5:09 p.m.	module_name: KERNEL32.DLL basename: KERNEL32 stack_pivoted: 0 flags: 0 module_address: 0x770a0000	1	0	0

Network Analysis

Download pcap

Hosts 2 | DNS 1 | TCP 3 | UDP 12 | HTTP(S) 3 | ICMP 0 | IRC 0 | Suricata | Snort

TCP Requests

192.168.56.104:49165 → 5.149.254.182:80
teal.throcytes.ru

192.168.56.104:49166 → 5.149.254.182:80
teal.throcytes.ru

192.168.56.104:49158 → 81.198.165.210:80

192.168.56.104:49165 → 5.149.254.182:80

plaintext hex | 16 bytes 32 bytes 48 bytes 64 bytes

```
00000000: 504f 5354 202f 6170 6920 4854 5450 2f31  POST./api.HTTP/1
00000010: 2e30 0d0a 436f 6e6e 6563 7469 6f6e 3a20  .0..Connection:.
00000020: 6b65 6570 2d61 6c69 7665 0d0a 436f 6e74  keep-alive..Cont
00000030: 656e 742d 4c65 6e67 7468 3a20 3131 3233  ent-Length:.1123
00000040: 0d0a 486f 7374 3a20 7465 616c 2e74 6872  ..Host:.teal.thr
00000050: 6f63 7974 6573 2e72 750d 0a41 6363 6570  ocytes.ru..Accep
00000060: 743a 2074 6578 742f 6874 6d6c 2c61 7070  t:.text/html,app
00000070: 6c69 6361 7469 6f6e 2f78 6874 6d6c 2b78  lication/xhtml+x
00000080: 6d6c 2c61 7070 6c69 6361 7469 6f6e 2f78  ml,application/x
00000090: 6d6c 3b71 3d30 2e39 2c2a 2f2a 3b71 3d30  ml;q=0.9,*/*;q=0
000000a0: 2e38 0d0a 4163 6365 7074 2d45 6e63 6f64  .8..Accept-Encod
000000b0: 696e 673a 2069 6465 6e74 6974 790d 0a55  ing:.identity..U
000000c0: 7365 722d 4167 656e 743a 204d 6f7a 696c  ser-Agent:.Mozil
000000d0: 6c61 2f33 2e30 2028 636f 6d70 6174 6962  la/3.0.(compatib
000000e0: 6c65 3b20 496e 6479 204c 6962 7261 7279  le;.Indy.Library
000000f0: 290d 0a0d 0a                             ).....
```

192.168.56.104:49165 → 5.149.254.182:80

community

HackInBo

COMMUNITY REPO

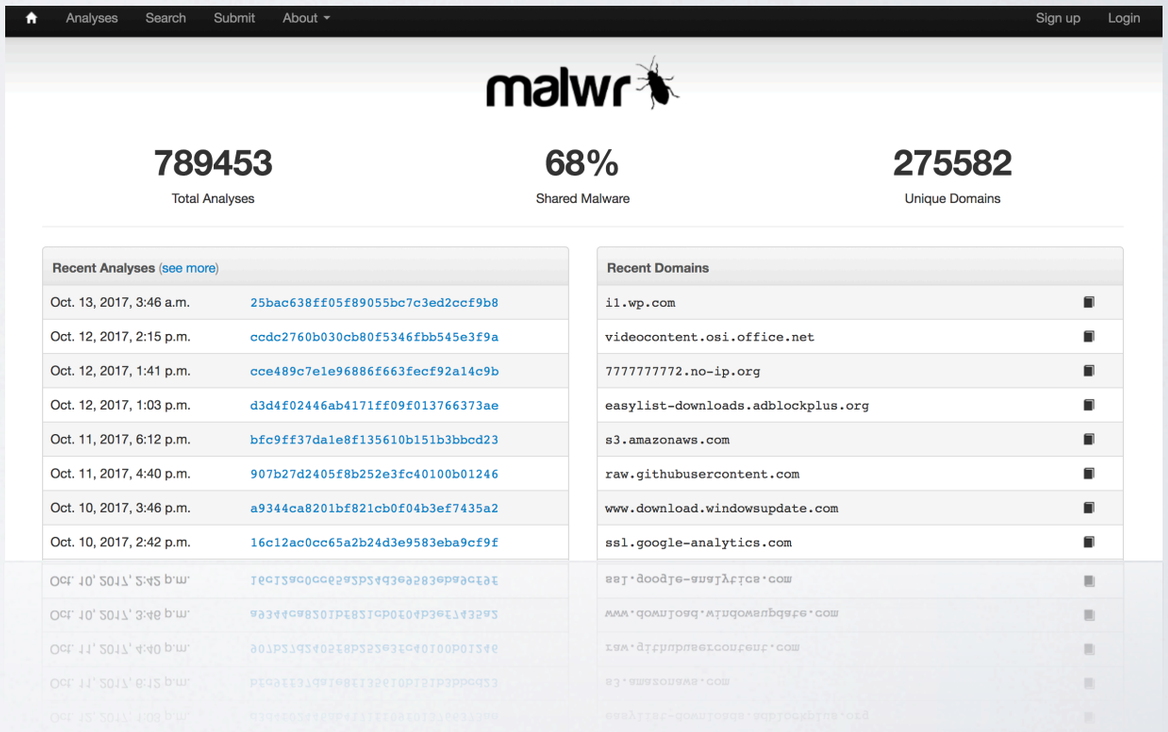
- GitHub repository di contributi dalla **community**.
- Analyzer, moduli e **signature**.
- Comando `cuckoo community`.
- https://github.com/cuckoosandbox/community

HackInBo

MALWR.COM

shadowserver

- Istanza pubblica.
- Sample **condivisi**.
- User accounts.
- Analisi **private**.
- Code of conduct.



HACKINBO

The End

AackInBo