IRMA

Incident Response & Malware Analysis plate-forme

Alexandre Quint Guillaume Dedrie
{aquint, gdedrie}@quarkslab.com

RMLL

July 07 2015

QUARKSLAB
INNOVATIVE SECURITY

Agenda

Plan

Background & Issues

De: admin@chat-k.cat
À: moi
Sujet: Try this one !!!

<3 cats

BestCatScreensaverEver.exe

Is BestCatScreenSaverEver.exe safe?

Is BestCatScreenSaverEver.exe safe?

Solution #1: Scan it with the local antivirus engine.

Is BestCatScreenSaverEver.exe safe?

Solution #1: Scan it with the local antivirus engine.

+ pretty easy

Is BestCatScreenSaverEver.exe safe?

Solution #1: Scan it with the local antivirus engine.

+ pretty easy
+ quick (most of the time. . .)

Is BestCatScreenSaverEver.exe safe?

Solution #1: Scan it with the local antivirus engine.

+ pretty easy
+ quick (most of the time. . .)
– relies exclusively on an unique antivirus editor

Is BestCatScreenSaverEver.exe safe?

Solution #1: Scan it with the local antivirus engine.

+ pretty easy
+ quick (most of the time. . .)
– relies exclusively on an unique antivirus editor

Not good enough

Is BestCatScreenSaverEver.exe safe?

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com
+ numerous antivirus engines available

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com
+ numerous antivirus engines available
− only one file at a time

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com
+ numerous antivirus engines available
– only one file at a time
– file is sent over Internet

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com
+ numerous antivirus engines available
– only one file at a time
– file is sent over Internet
– scanning options are unknown

Is BestCatScreenSaverEver.exe safe?

Solution #2: Scan it with an web-based multi-scanner

+ Several free online services:
  - virustotal.com
  - avcaesar.malware.lu
  - metascan.com
+ numerous antivirus engines available
– only one file at a time
– file is sent over Internet
– scanning options are unknown

Not good enough

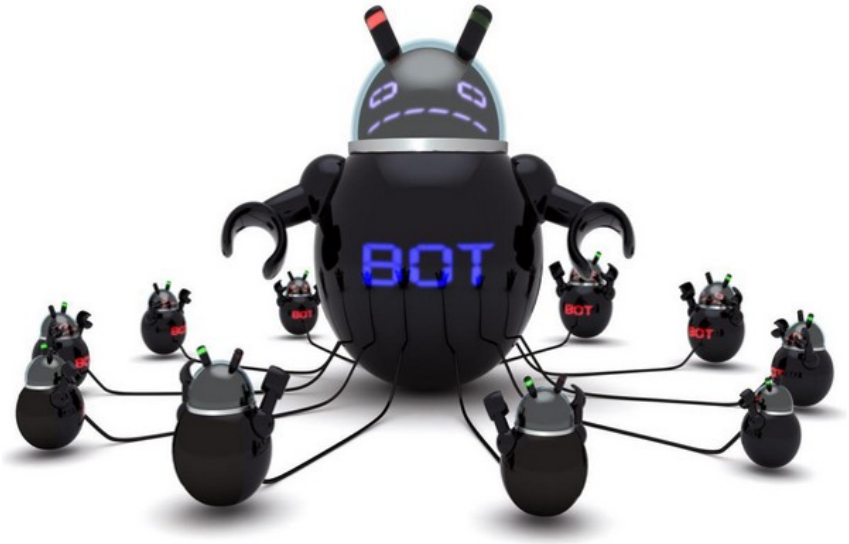
Is BestCatScreenSaverEver.exe safe?

Is BestCatScreenSaverEver.exe safe?

Solution #3: YOLO! Click on it and pray for god!

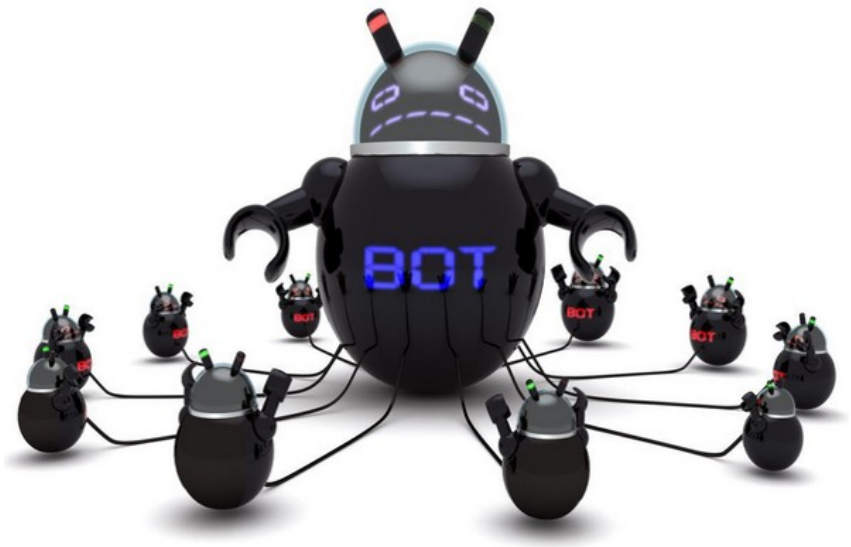
Is BestCatScreenSaverEver.exe safe?

Solution #3: YOLO! Click on it and pray for god!



Is BestCatScreenSaverEver.exe safe?

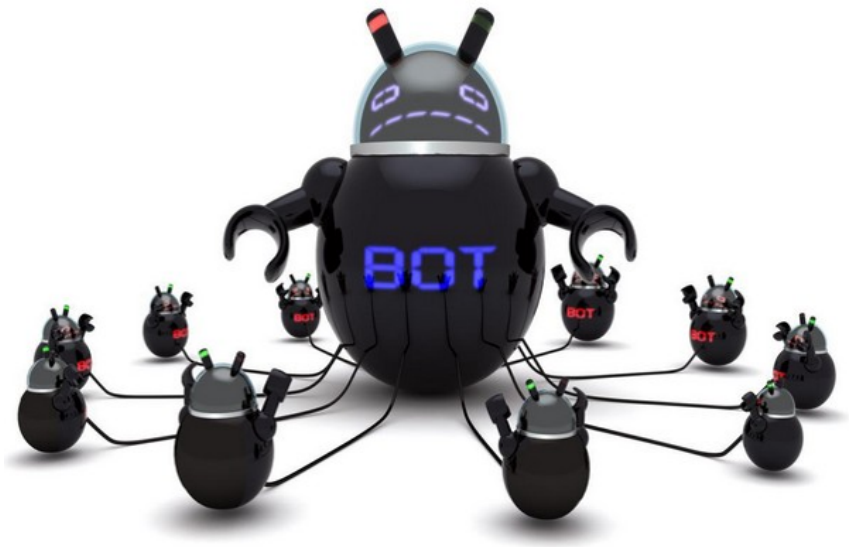
Solution #3: YOLO! Click on it and pray for god!



+ A good way to test your {backup,restore} procedures

Is BestCatScreenSaverEver.exe safe?

Solution #3: YOLO! Click on it and pray for god!



+ A good way to test your {backup,restore} procedures

No comment...

A need

A need


AIRBUS
GROUP


GRAND DUCHY OF LUXEMBOURG
GOVCERT.LU


DCNS


DE LA RECHERCHE À L'INDUSTRIE
cea


QUARKSLAB
INNOVATIVE SECURITY


orange™

Plan

IRMA

Incident Response & Malware Analysis

IRMA

Incident Response & Malware Analysis

- **private** platform dedicated to **file analysis**

IRMA

Incident Response & Malware Analysis

- **private** platform dedicated to **file analysis**
- **Open-source** (Apache V2 license, code hosted on Github)

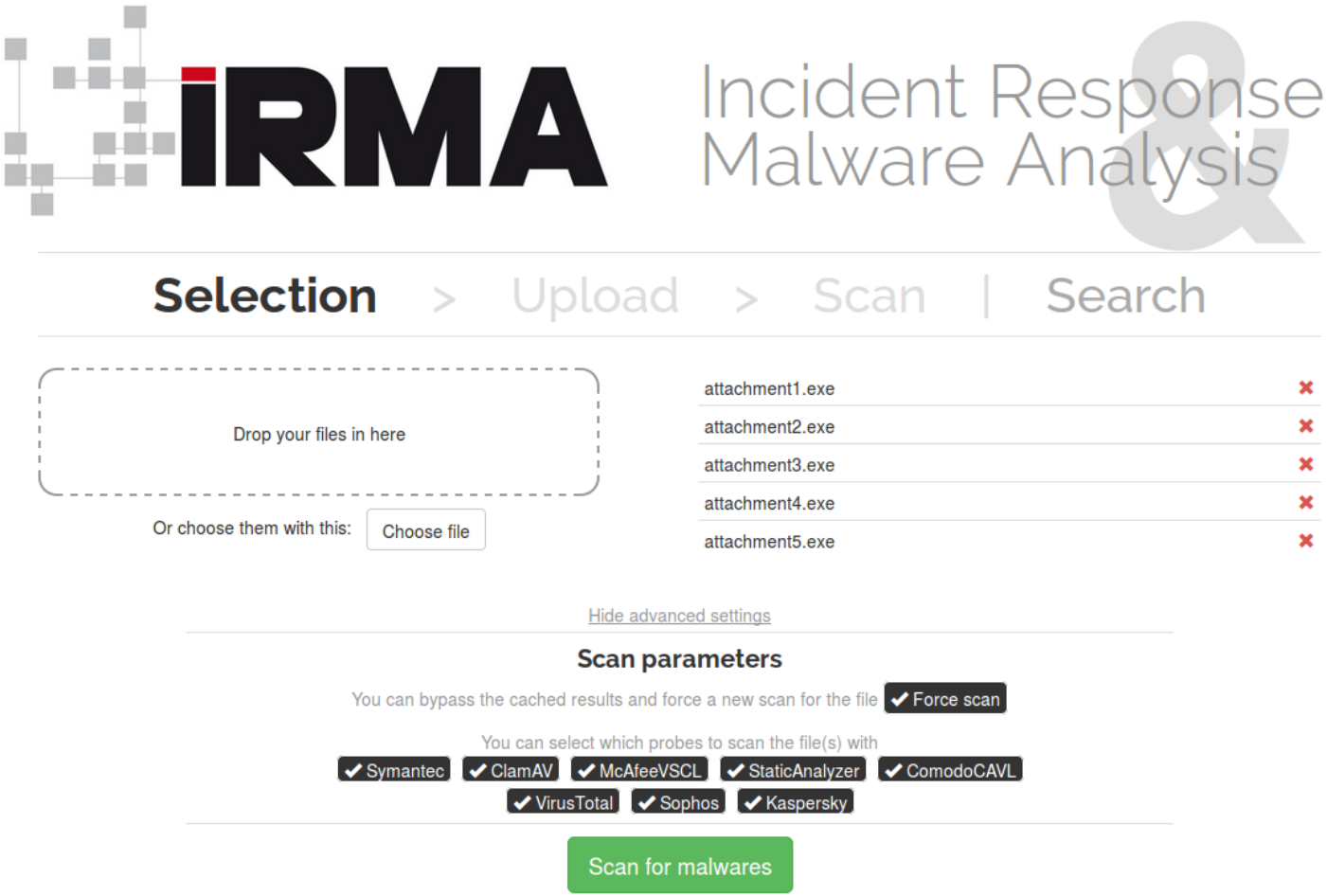
IRMA

Incident Response & Malware Analysis

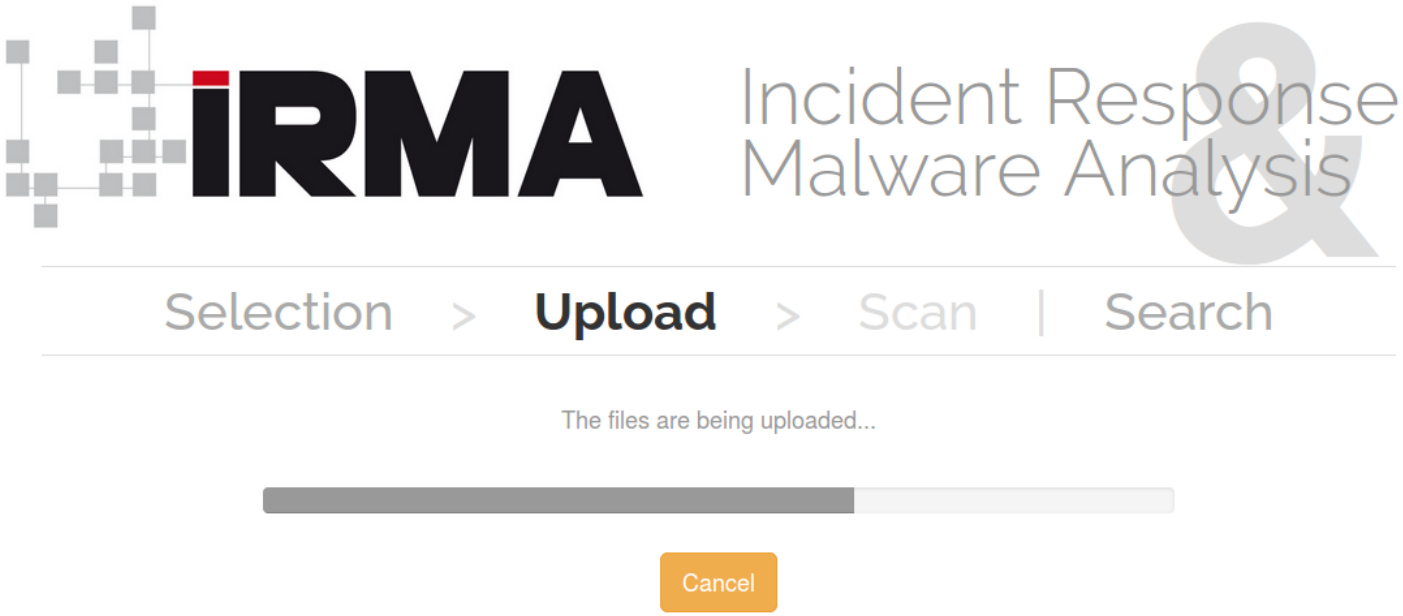
- **private** platform dedicated to **file analysis**
- **Open-source** (Apache V2 license, code hosted on Github)
- Can be **Customized at will**.

Demo

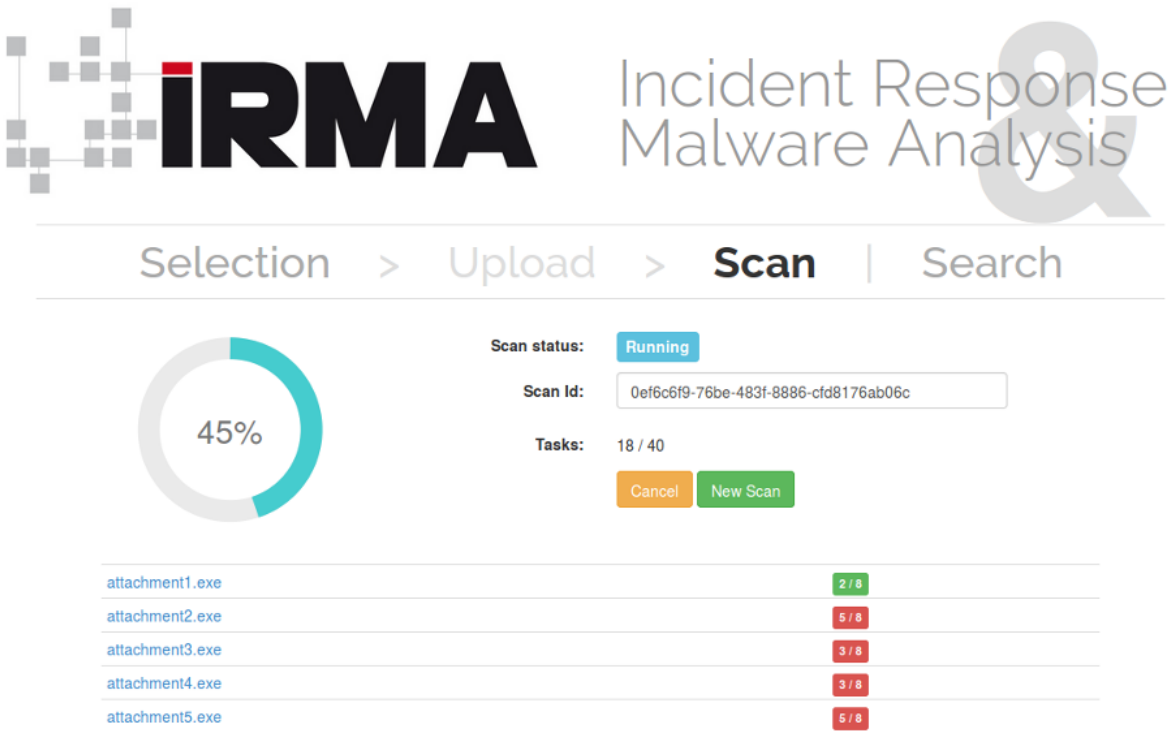
Demo


iRMA
Incident Response
Malware Analysis
Selection > Upload > Scan | Search
Drop your files in here
Or choose them with this:
Choose file
attachment1.exe
attachment2.exe
attachment3.exe
attachment4.exe
attachment5.exe
Hide advanced settings
Scan parameters
You can bypass the cached results and force a new scan for the file
Force scan
You can select which probes to scan the file(s) with
Symantec
ClamAV
McAfeeVSCL
StaticAnalyzer
ComodoCAVL
VirusTotal
Sophos
Kaspersky
Scan for malwares

Demo


IRMA
Incident Response
Malware Analysis
Selection > Upload > Scan | Search
The files are being uploaded...
Cancel

Demo


iRMA
Incident Response & Malware Analysis
Selection > Upload > Scan | Search
45%
Scan status: Running
Scan Id: 0ef6c6f9-76be-483f-8886-cfd8176ab06c
Tasks: 18 / 40
Cancel
New Scan
attachment1.exe 2 / 8
attachment2.exe 5 / 8
attachment3.exe 3 / 8
attachment4.exe 3 / 8
attachment5.exe 5 / 8

Demo

File informations

Filename	attachment2.exe
Size (bytes)	136192
MD5	37ee86deec0c2b7f7311742677d157d0
SHA256	2d80c5f0793c5520d2780157f296761972f7b02039585b14474ae7d9668f32f8
First Scan	Oct 21, 2014 11:20 AM
Last Scan	Oct 21, 2014 11:21 AM

Antivirus

Name	Version	Duration (in secs)	Result
Clam AntiVirus Scanner	0.98.4	0.03	Win.Trojan.Agent-604924
Comodo Antivirus for Linux	1.1.268025.1	0.27	
Kaspersky Anti-Virus	14.0.0.4837	0.59	HEUR:Trojan.Win32.Generic
McAfee VirusScan Command Line scanner	6.0.4.564	13.59	
Sophos Anti-Virus	1.01.1	8.05	Mal/Inject-CEE
Symantec Anti-Virus	12.1.4013.4013.105	11.05	Trojan.Gen.2

External

VirusTotal

Responded in 0.66 s

Full result is available here.

```
detected by 44/53
```

Demo

Metadata

StaticAnalyzer

Responded in 0.06 s


```
{
  - pe_imports: [
      - {
          - imports: [
              - {
                  name: "shutdown",
                  address: "0x4070dc"
                },
              - {
                  name: "connect",
                  address: "0x4070e0"
                },
              - {
                  name: "send",
                  address: "0x4070e4"
                }
            ],
            dll: "WS2_32.dll"
        },
      - {
          - imports: [
              - {
                  name: "HeapFree",
                  address: "0x407000"
                },
              - {
                  name: "VirtualProtect",
                  address: "0x407004"
                },
              - {
                  name: "GetLocaleInfoA",
                  address: "0x407008"
                },
```

Plan

Technologies

python™

NGINX

uWSGI

Bottle

SQLAlchemy

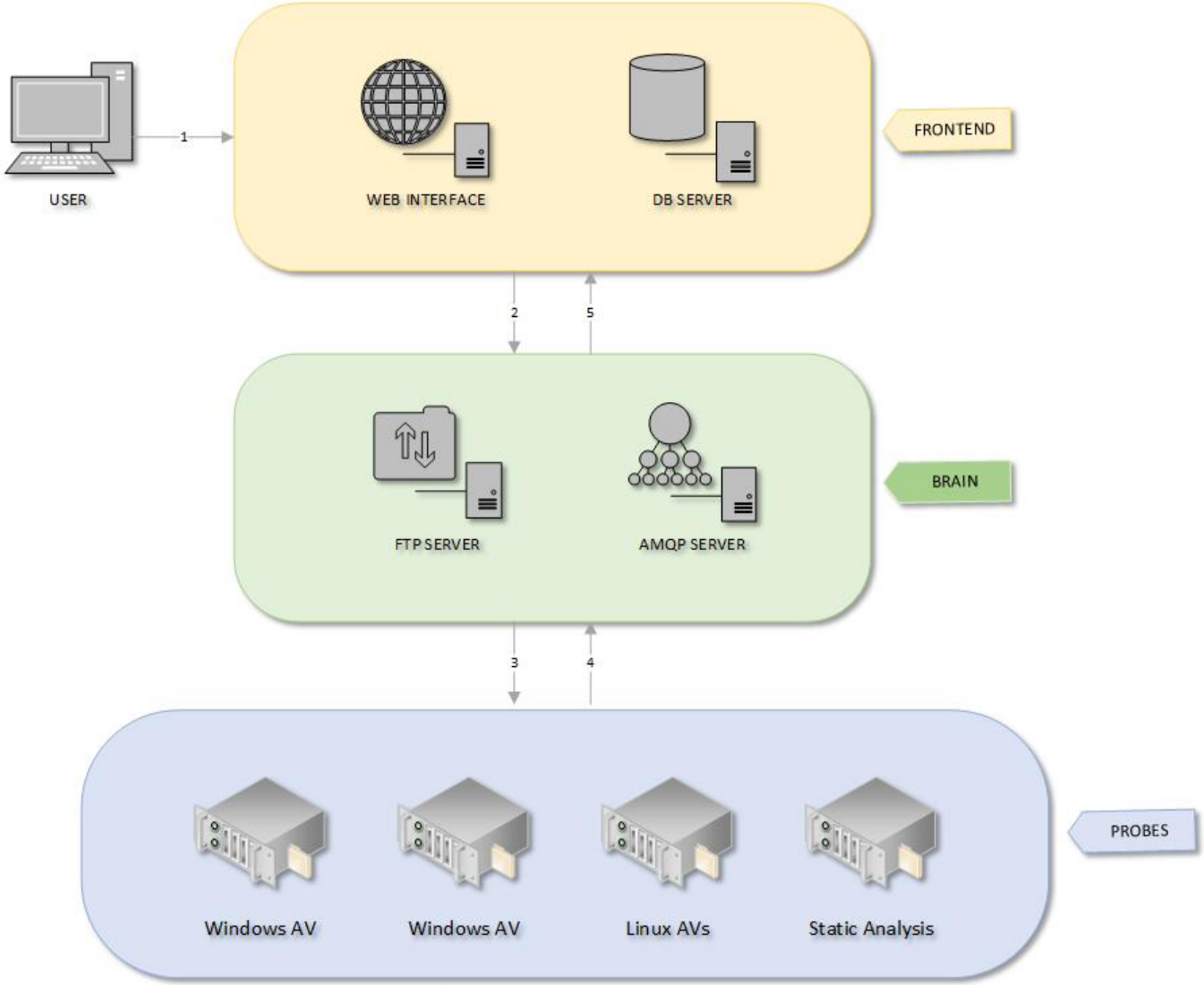
mongoDB

PureFTPd
A secure FTP daemon

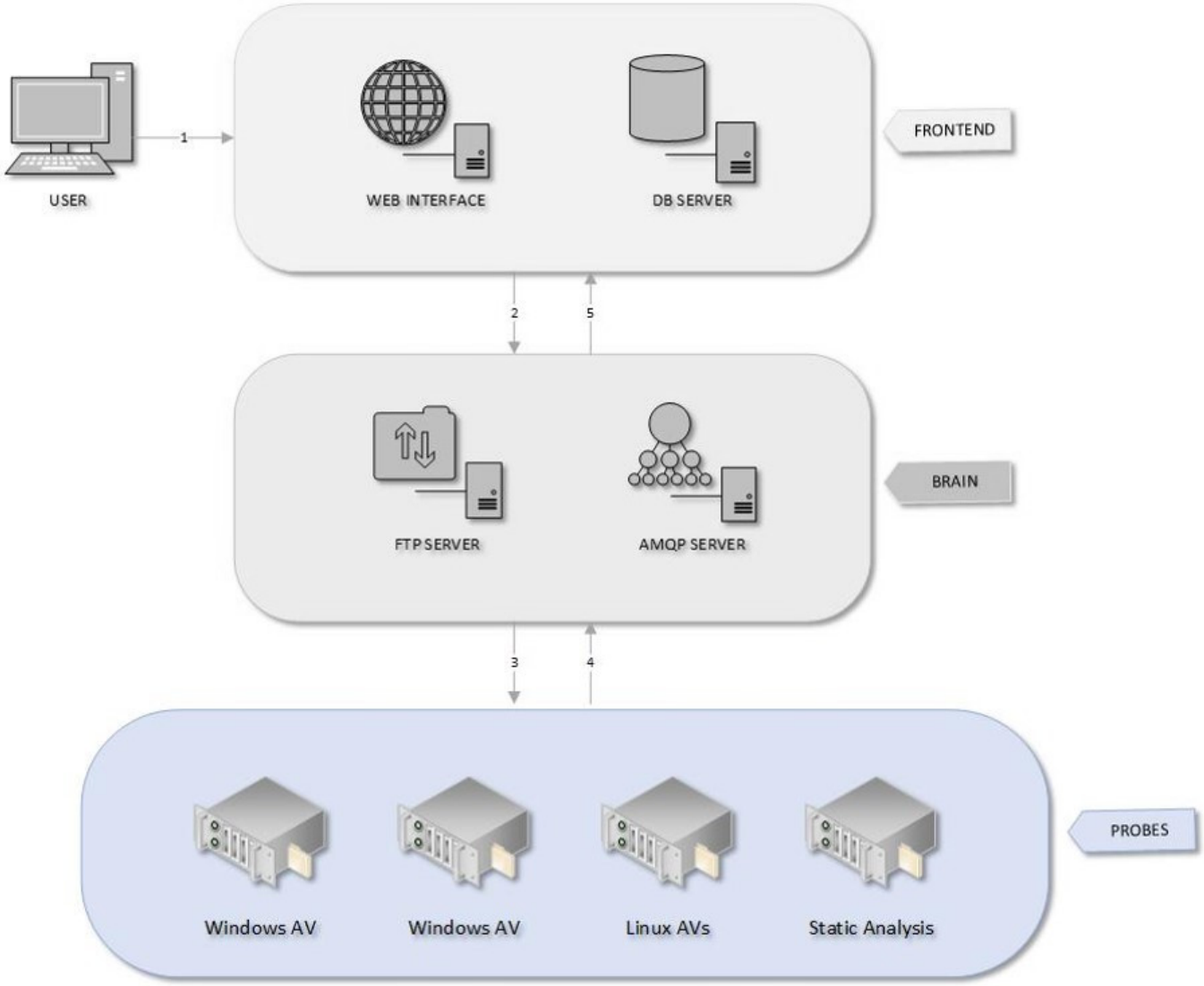
RabbitMQ™
Messaging that just works

C

The infrastructure



The infrastructure - Probe



The infrastructure - Probe Supported

AVIRA
GDATA
MCAFEE
SYMANTEC
EMSISOFT
KASPERSKY
SOPHOS

ANTIVIRUS

AVAST
BITDEFENDER
COMODO
ESETNOD32
FPROT
MCAFEE
AVG
CLAMAV
DrWEB
ESCAN
FSECURE
SOPHOS
VIRUSBLOKADA
ZONER

ANTIVIRUS

PEiD
YARA
PE STATIC ANALYSIS

METADATA

NSRL

DATABASE

VIRUSTOTAL

EXTERNAL

The infrastructure - Probe Example - Balbuzard

The infrastructure - Probe Example - Balbuzard

Balbuzard - malware analysis tools to extract patterns of interest and crack obfuscation such as XOR

Author: Philippe Lagadec
Homepage: http://www.decalage.info/python/balbuzard

The infrastructure - Probe Example - Balbuzard

```
>> from balbuzard.balbuzard import patterns, Balbuzard
>> Bal = Balbuzard(patterns=patterns)
>> data = open("./attachment1.exe").read()
>> list(Bal.scan(data))
[(<balbuzard.balbuzard.Pattern at 0x7fd37cda23d0>, [(0, 'MZ'), (15320, 'MZ')]),
 (<balbuzard.balbuzard.Pattern at 0x7fd37cda2410>,
  [(232, 'PE'), (9541, 'PE'), (50172, 'PE'), (78332, 'PE')]),
[...],
 (<balbuzard.balbuzard.Pattern at 0x7fd37cda2710>, [(27129, 'Pop')])]
```

The infrastructure - Probe Example - Balbuzard

```
# =============
#  constructor
# =============

def __init__(self):
    module = sys.modules['balbuzard.balbuzard']
    patterns = module.patterns
    self.Analyzer = module.Balbuzard(patterns=patterns)
    return

def analyze(self, filename):
    res = {}
    with open(filename, "rb") as f:
        data = f.read()
    for (match_pattern, matches) in self.Analyzer.scan(data):
        res[match_pattern.name] = matches
    return res

# ==================
#  probe interfaces
# ==================
def run(self, paths):
    response = PluginResult(name=type(self).plugin_name,
                            type=type(self).plugin_category,
                            version=None)
    try:
        started = timestamp(datetime.utcnow())
        response.results = self.analyze(paths)
        stopped = timestamp(datetime.utcnow())
        response.duration = stopped - started
        response.status = self.BalbuzardResult.SUCCESS
    except Exception as e:
        response.status = self.BalbuzardResult.ERROR
        response.results = str(e)
    return response
```

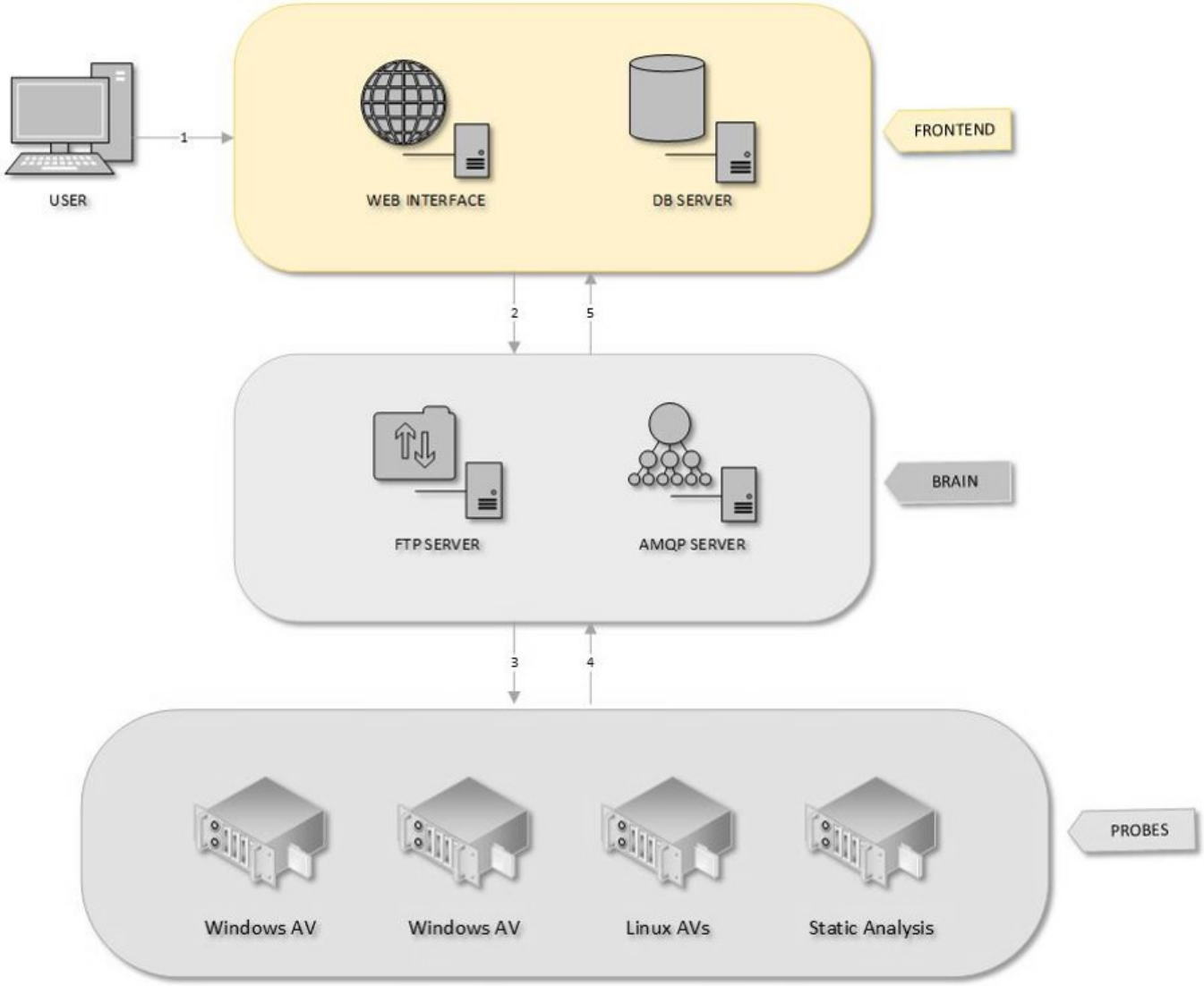
The infrastructure - Probe Example - Balbuzard

Balbuzard

Responded in 0.26 s

```
EXE: section name:
    .rdata (704)
    .rsrc (784)
    .reloc (744)
Executable filename:
    Explorer.exe (17184)
    winzip32.exe (18188)
    WinRAR.exe (18264)
    rar.bat (18287)
    zip.bat (18307)
    sIRC4.exe (52512)
    kernel32.dll (56400)
    user32.dll (56914)
    advapi32.dll (56970)
    oleaut32.dll (57034)
```

The infrastructure - Frontend



The infrastructure - Frontend API

The infrastructure - Frontend API

Kiosque d'analyse de clé USB

The infrastructure - Frontend API

Kiosque d'analyse de clé USB

Filtrage des pièces jointes

Plan

Detection - Efficiency

Results based on the analysis of 2445 Malwares appeared in Spring 2014.

Antivirus	Détection	Taux
Symantec	2331	95%
ComodoCAVL	2430	99%
Sophos	1781	73%
ClamAV	1582	65%
Kaspersky	2396	98%
McAfeeVSCL	1748	71%

Detection - Time

Probe	Min	Max	Moyenne
FSecure	0.03s	46.9s	0.397s
EScan	1.12s	25.45s	1.453s
AvastCoreSecurity	0.01s	0.56s	0.039s
ClamAV	0.01s	13.24s	0.082s
AVGAntiVirusFree	1.3s	3.32s	1.67s
ComodoCAVL	1.13s	6.82s	1.32s
McAfeeVSCL	**12.57s**	**28.48s**	**14.922s**
Zoner	0.0s	31.01s	0.077s
BitdefenderForUnices	3.02s	26.94s	5.651s
VirusBlokAda	2.12s	29.44s	2.704s

Best result

Best result

- An Open-Source project, that's nice...

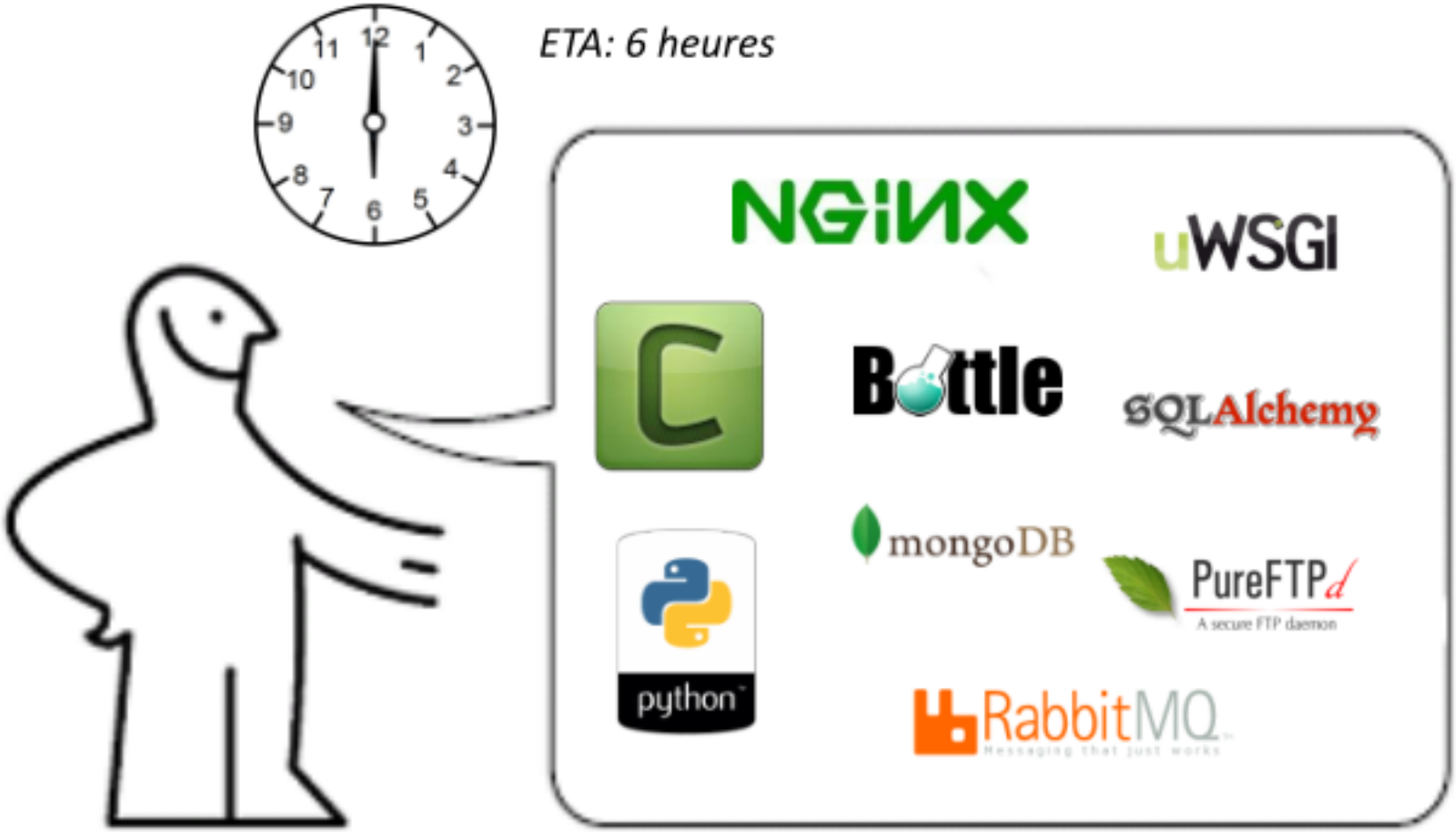
Best result

- An Open-Source project, that's nice...
- Get Users, that's better...

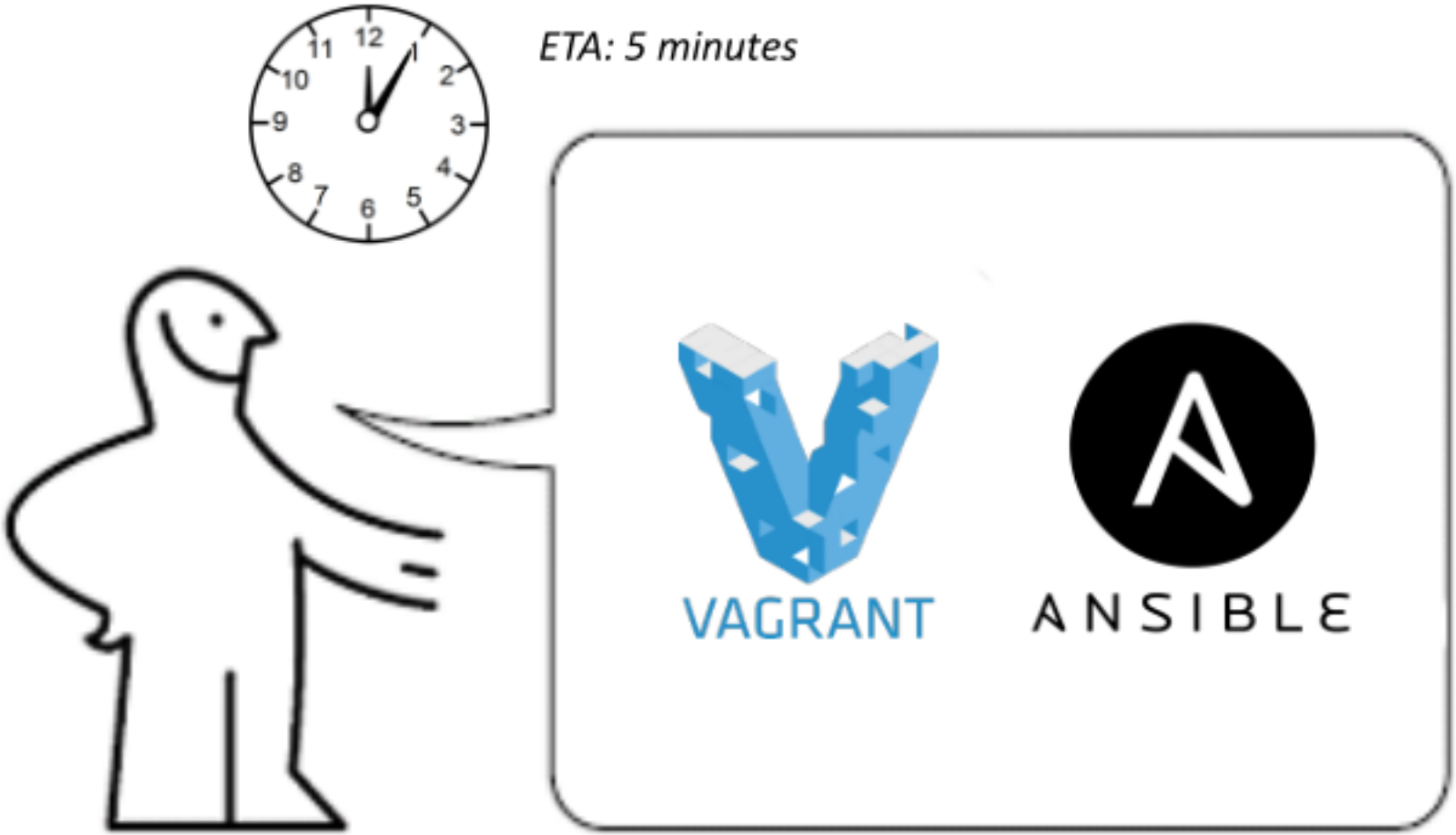
Best result

- An Open-Source project, that's nice...
- Get Users, that's better...
- Get contributors, that's the best!

Installation



Installation



Installation

Installation Vagrant :

```
https://www.vagrantup.com/downloads.html
```

Installation Ansible :

```
$ sudo pip install ansible
```

Installation IRMA:

```
$ git clone https://github.com/quarkslab/irma-ansible
$ cd irma-ansible
$ ansible-galaxy install -r ansible-requirements.yml
$ vagrant up
```

Plan

Como-dort?

Como-dort?

Before	After
42	499
8%	99%

McAfee?

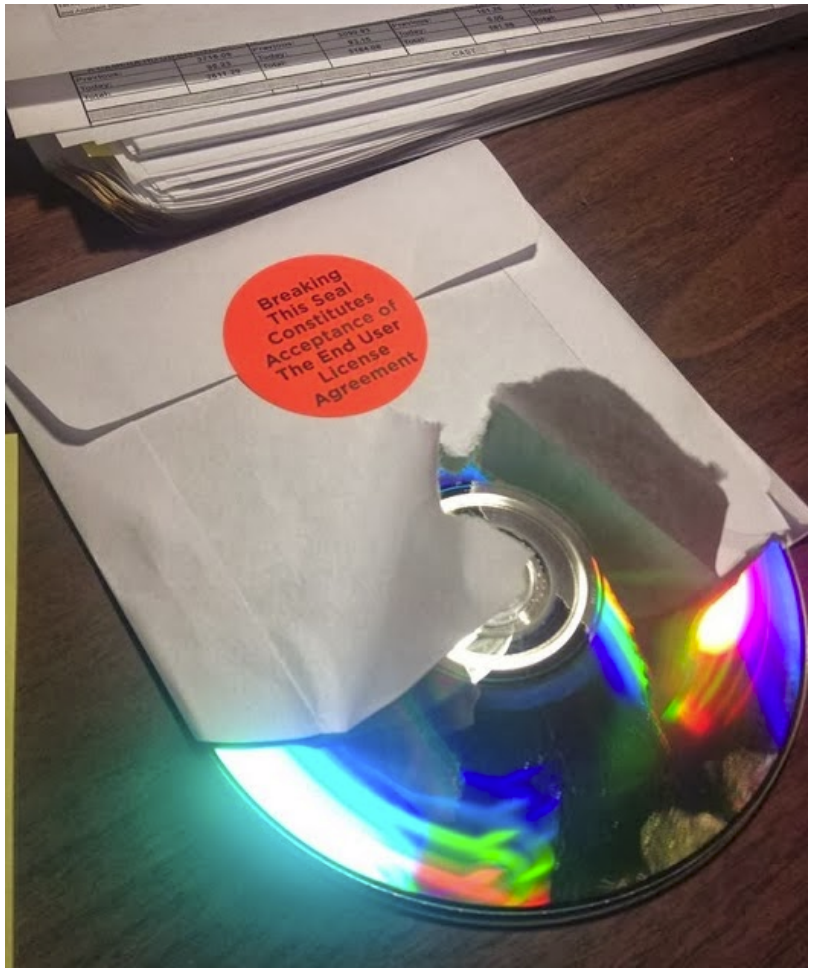
McAfee?

McAfee VirusScan Command Line scanner	PWS-Zbot-FBDH	6.0.4.564	19.29
McAfee VirusScan Daemon	PWS-Zbot-FBDH	6.0.4.564	0.04

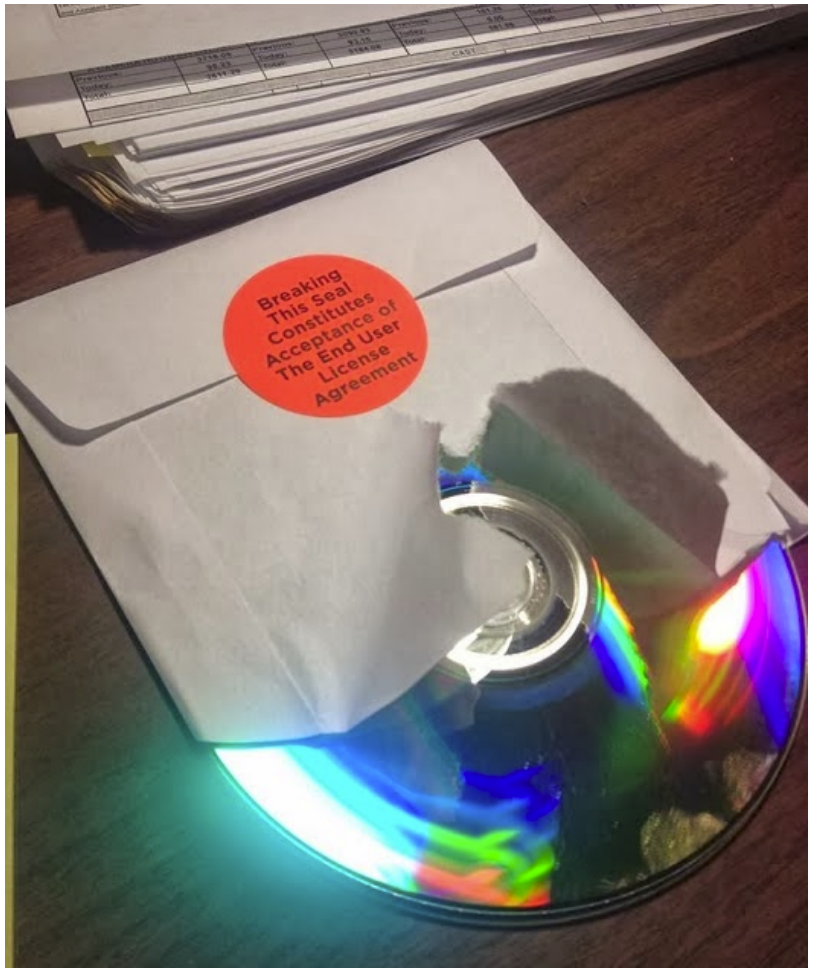
x500

End-User License Agreement (EULA)

End-User License Agreement (EULA)



End-User License Agreement (EULA)



"Is it possible to get your samples feed if you decide to make your instance online?"

Plan

For a malware analyst

For a malware analyst

- Search similar malwares using results:
  - Strings (IP addr, function's name, . . .)
  - Imported sections
  - Compilation informations
  - Unpacker's informations

For a system administrator

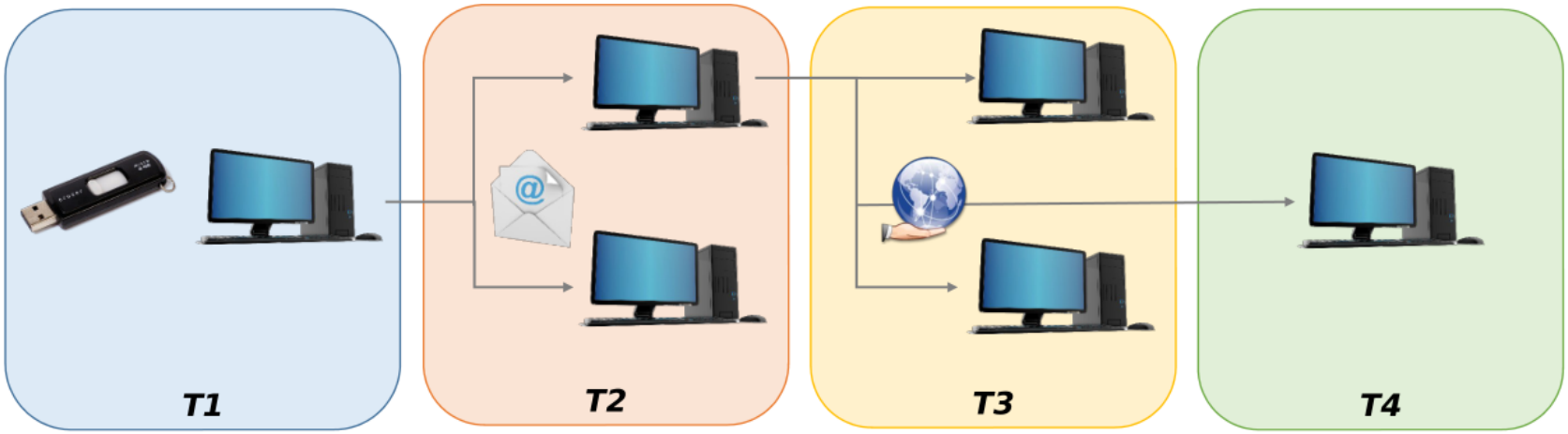
For a system administrator

- Use a desktop agent (PoC) to send file

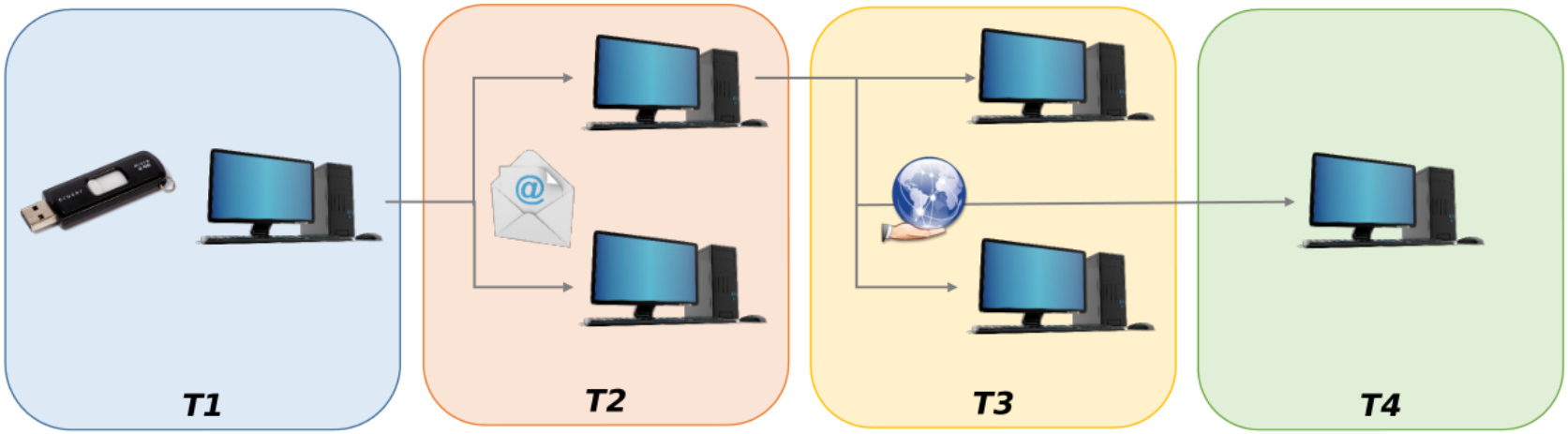
For a system administrator

- Use a desktop agent (PoC) to send file
- Get a Malware propagation timeline

For a system administrator

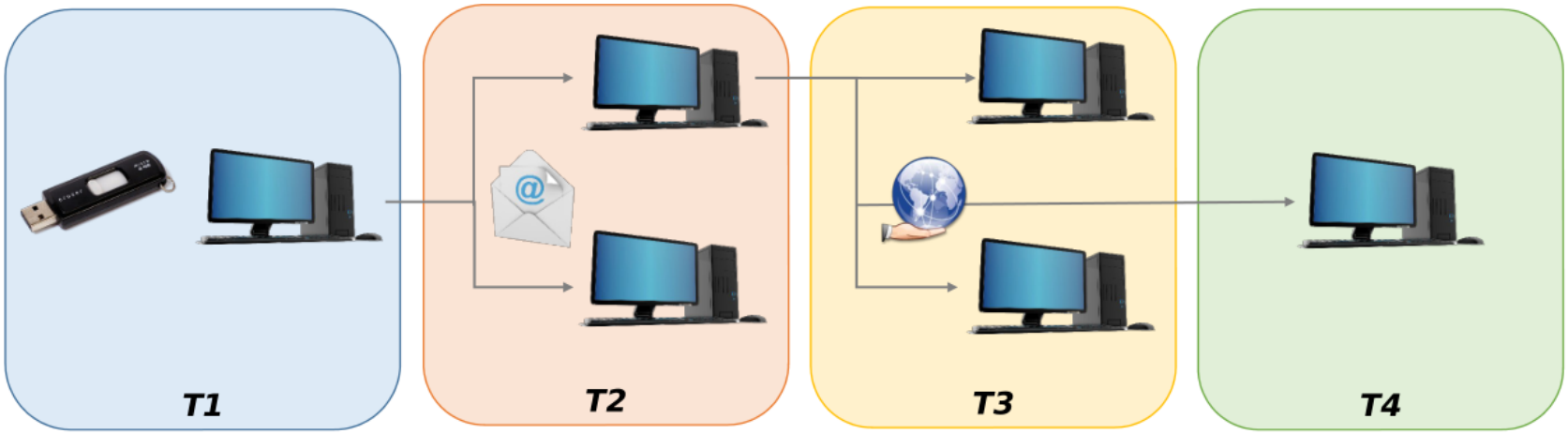


For a system administrator



T1: file found on an usb drive

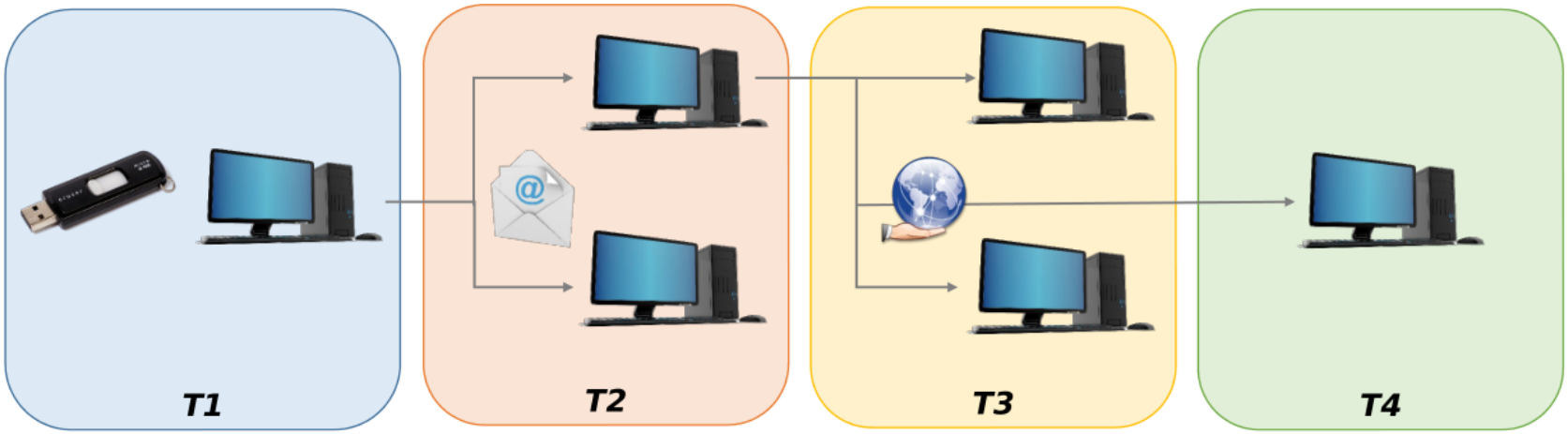
For a system administrator



T1: file found on an usb drive

T2: file sent by email

For a system administrator

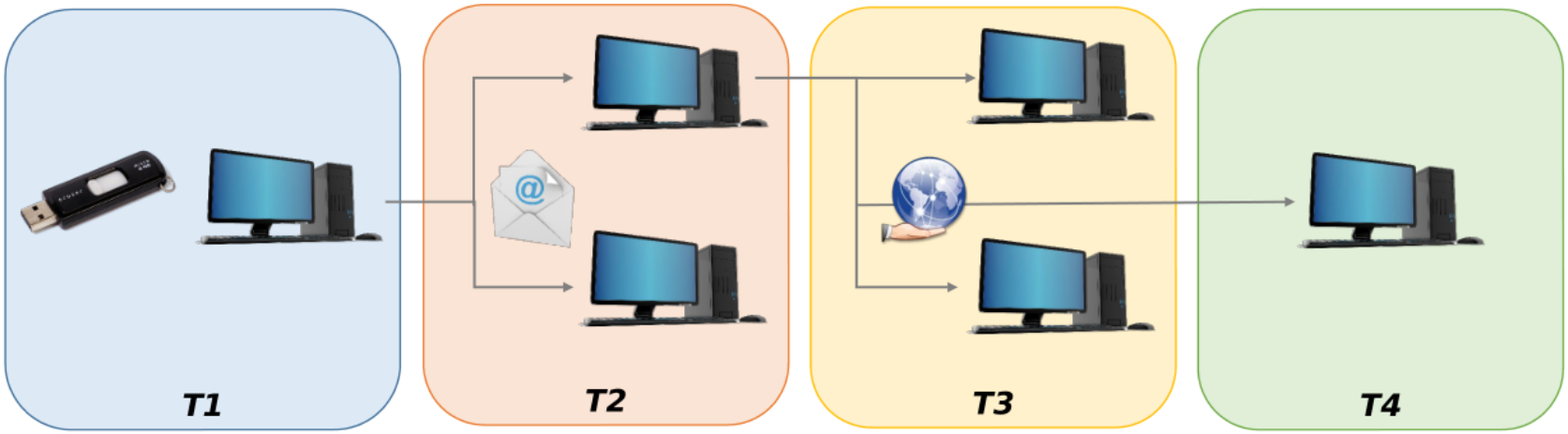


T1: file found on an usb drive

T2: file sent by email

T3: file copied to a network storage

For a system administrator



T1: file found on an usb drive

T2: file sent by email

T3: file copied to a network storage

T4: file downloaded later from the network storage

Contact

Homepage: `http://irma.quarkslab.com`

Github: `https://github.com/quarkslab/irma`

Twitter: `@qb_irma`

IRC: `#qb_irma@freenode`

Do you have any questions?

QUARKSLAB
INNOVATIVE SECURITY

www.quarkslab.com

contact@quarkslab.com | @quarkslab.com