

IRMA

Incident Response & Malware Analysis



Fernand Lone-Sang - Alexandre Quint – Guillaume Dedrie
SSTIC 2015 - Rennes

Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Problématique

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

<3 cats



BestCatScreensaverEver.exe

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 1 : le scanner avec l'antivirus local.

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 1 : le scanner avec l'antivirus local.

+ facile à faire

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 1 : le scanner avec l'antivirus local.

- + facile à faire
- + rapide (enfin souvent)

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 1 : le scanner avec l'antivirus local.

- + facile à faire
- + rapide (enfin souvent)
- on se repose entièrement sur un éditeur

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 1 : le scanner avec l'antivirus local.

- + facile à faire
- + rapide (enfin souvent)
- on se repose entièrement sur un éditeur

C'est bien mais pas suffisant

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
 - virustotal.com
 - avcaesar.malware.lu
 - metascan.com

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
virustotal.com
avcaesar.malware.lu
metascan.com
- + nombreux AV supportés

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
virustotal.com
avcaesar.malware.lu
metascan.com
- + nombreux AV supportés
- un fichier à la fois

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
 - virustotal.com
 - avcaesar.malware.lu
 - metascan.com
- + nombreux AV supportés
- un fichier à la fois
- on envoie le fichier sur Internet

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
 - virustotal.com
 - avcaesar.malware.lu
 - metascan.com
- + nombreux AV supportés
- un fichier à la fois
- on envoie le fichier sur Internet
- on ne connaît aucunes des options utilisées

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 2 : le faire scanner par un site web

- + nombreux sites disponibles gratuitement :
 - virustotal.com
 - avcaesar.malware.lu
 - metascan.com
- + nombreux AV supportés
- un fichier à la fois
- on envoie le fichier sur Internet
- on ne connaît aucune des options utilisées

C'est bien mais pas suffisant

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 3 : Cliquer dessus #YOLO

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 3 : Cliquer dessus #YOLO



Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 3 : Cliquer dessus #YOLO

+ c'est l'occasion de tester ses procédures de backup/restore

Problématique

BestCatScreensaverEver.exe est-il sain ?

Solution 3 : Cliquer dessus #YOLO

+ c'est l'occasion de tester ses procédures de backup/restore

No comment

Initiative commune



IRMA



Incident Response & Malware Analysis

IRMA



Incident Response & Malware Analysis

- Plate-forme **privée** d'**analyse** de fichiers

IRMA



Incident Response & Malware Analysis

- Plate-forme **privée** d'**analyse** de fichiers
- **Open-source** (licence Apache V2)

IRMA



Incident Response & Malware Analysis

- Plate-forme **privée** d'**analyse** de fichiers
- **Open-source** (licence Apache V2)
- **Personnalisable**

IRMA



Incident Response & Malware Analysis

- Plate-forme **privée** d'**analyse** de fichiers
- **Open-source** (licence Apache V2)
- **Personnalisable**

Première version publique annoncée en RUMP SSTIC 2014

Disclaimer

IRMA

Incident Response & Malware Analysis est un outil en ligne qui permet de combiner plusieurs moteurs d'analyse de fichiers pour obtenir plus d'informations, et des informations plus précises. On peut combiner des analyses anti-virus, Hashdb, des analyses statiques, des sandbox, etc

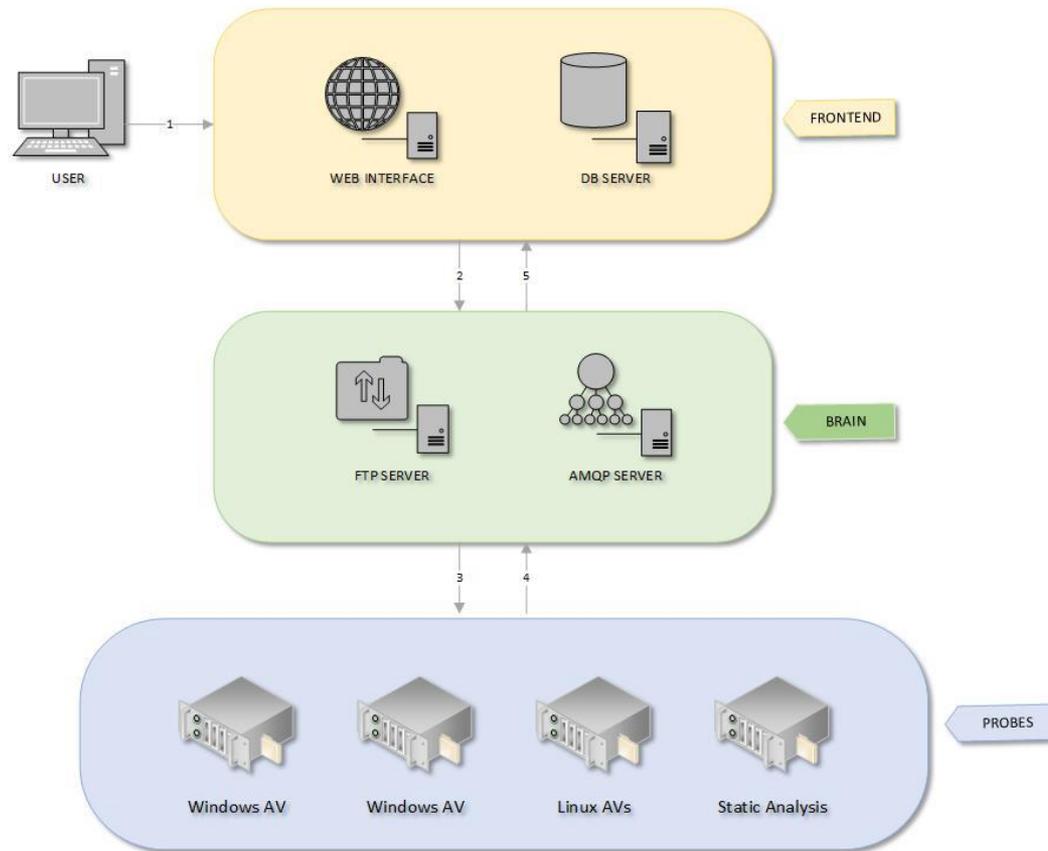
C'est disponible sous licence Apache 2.0, en ligne sur les dépôts GitHub de Quarkslab (quarkslab@github/irma-*) et ~~une version de test est en ligne : <http://frontend.irma.qb>~~ il n'y a pas encore de version de test en ligne.

https://quack1.me/sstic_2014_2_rumps.html

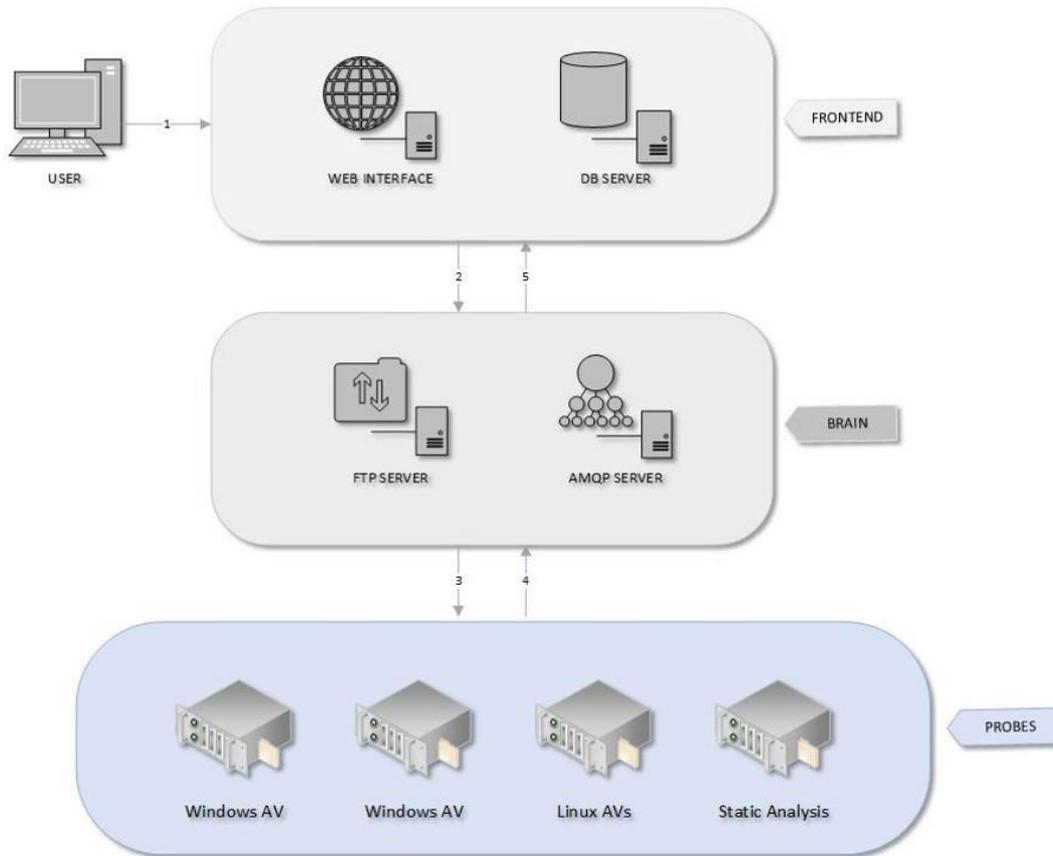
Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Architecture globale



Probes



Modules d'analyses supportés

AVIRA
GDATA
MCAFEE
SYMANTEC

EMSIOSOFT
KASPERSKY
SOPHOS



ANTIVIRUS

AVAST
BITDEFENDER
COMODO
ESETNOD32
FPROT
MCAFEE

AVG
CLAMAV
DrWEB
ESCAN
FSECURE
SOPHOS

VIRUSBLOKADA
ZONER



ANTIVIRUS

PEiD
YARA
PE STATIC ANALYSIS

METADATA

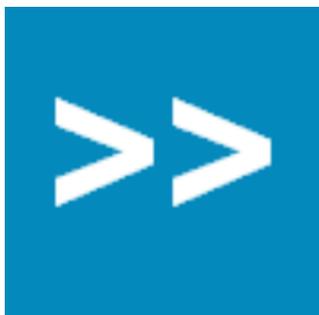
NSRL

DATABASE

VIRUSTOTAL

EXTERNAL

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>

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')])]
```

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
```

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)

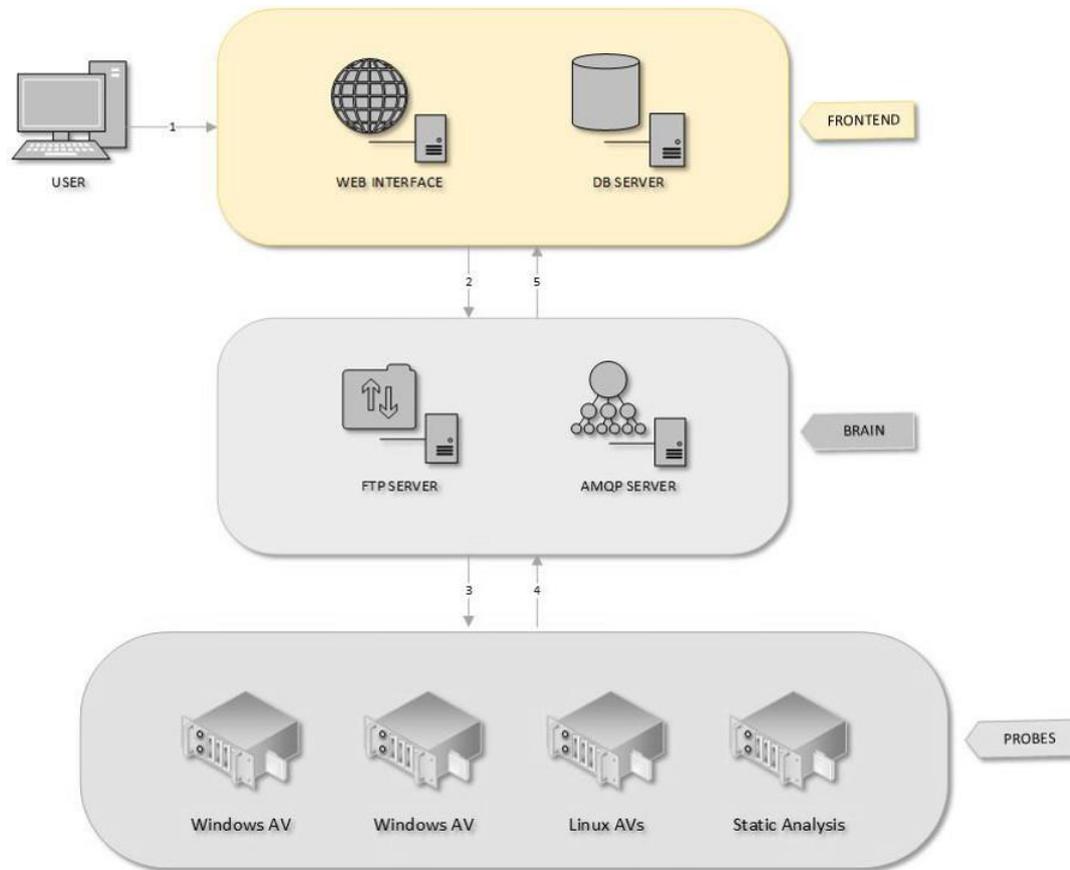
kernel32.dll (56400)

user32.dll (56914)

advapi32.dll (56970)

oleaut32.dll (57034)

Frontend



Web API

IRMA API

[Apache 2.0](#)

Scans

Show/Hide | List Operations | Expand Operations

GET	/scans	List all scans
POST	/scans	Create a scan
GET	/scans/{scanId}	Retrieve a scan
POST	/scans/{scanId}/launch	Launch a scan
POST	/scans/{scanId}/cancel	Cancel a scan
POST	/scans/{scanId}/files	Create a file upload
GET	/scans/{scanId}/results	List all results from a scan
GET	/scans/{scanId}/results/{resultId}	Retrieve a result for a specific scan

Exemples de clients

Kiosque d'analyse de clé USB



Exemples de clients

Kiosque d'analyse de clé USB



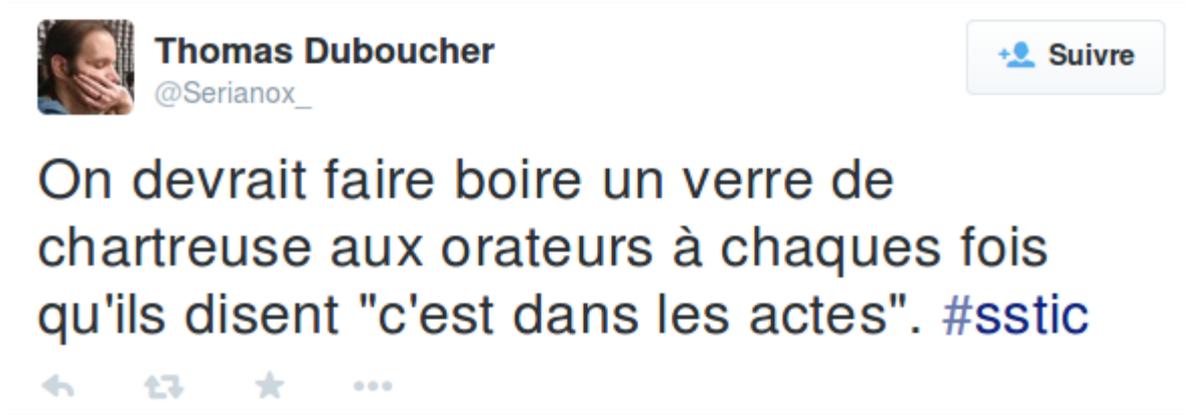
Filtrage des pièces jointes



Démo



Au fait...



Rappel : L'abus d'alcool est dangereux pour la santé

Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Plus de sources, plus d'infos

Référentiel de 2445 malwares publics datés de l'été 2014.

Plus de sources, plus d'infos

Référentiel de 2445 malwares publics datés de l'été 2014.

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

Plus de sources, plus d'infos

Référentiel de 2445 malwares publics datés de l'été 2014.

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

Comodo avant ... après

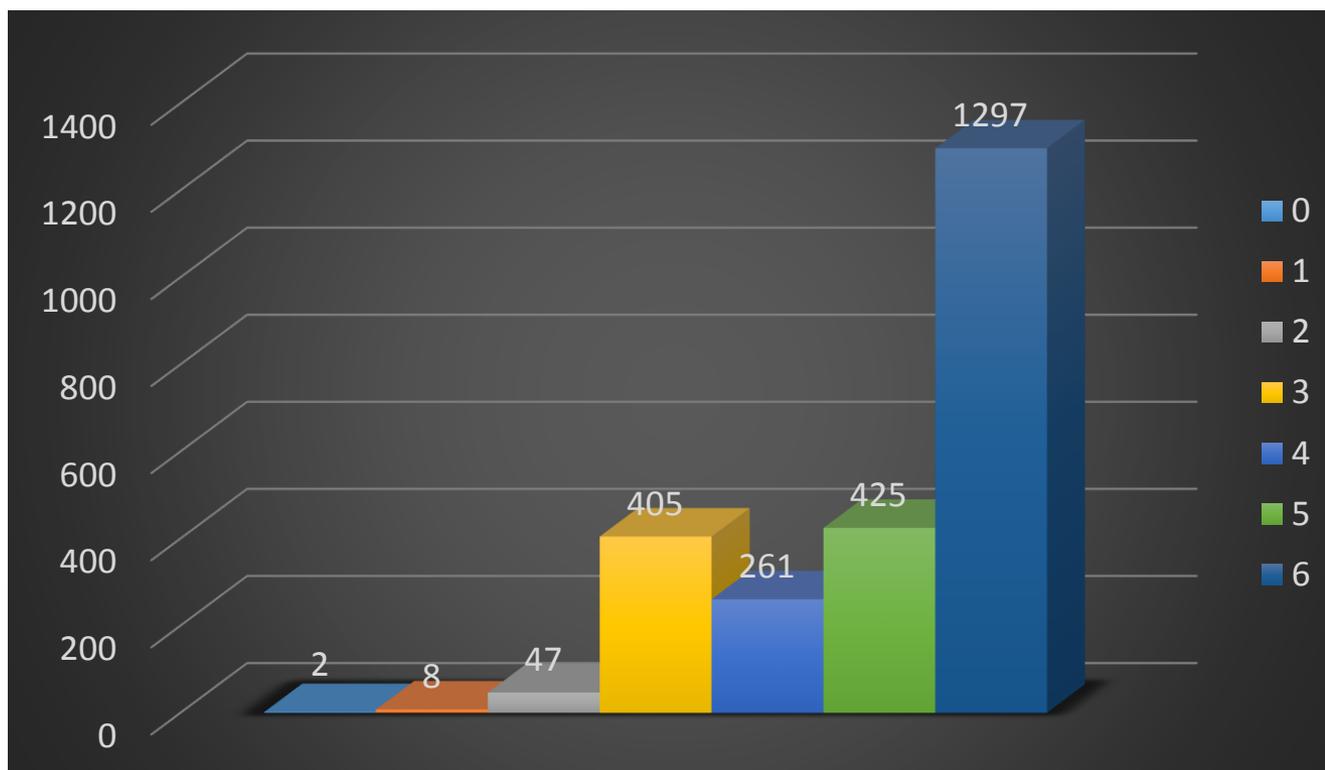
Test sur 500 malwares publics, avant et après l'installation des signatures à jour :

Comodo avant ... après

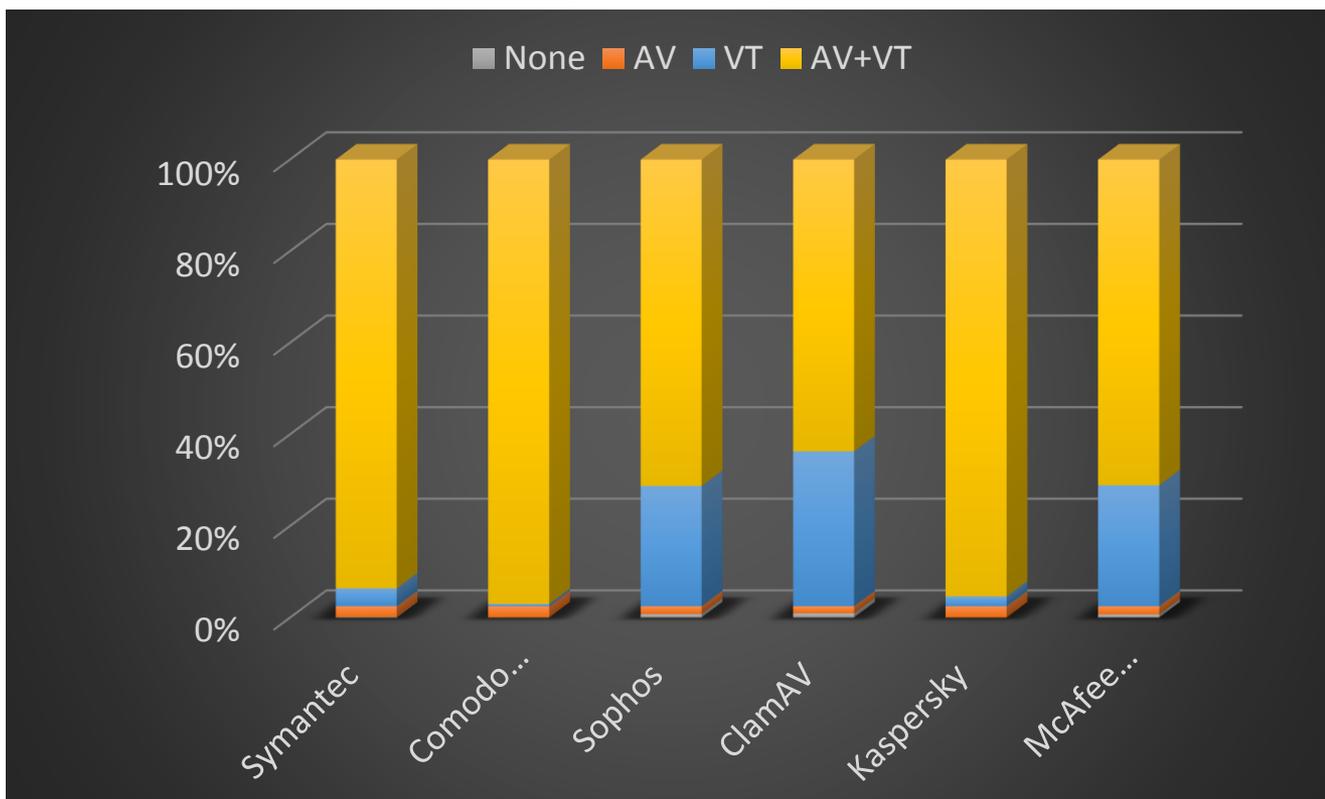
Test sur 500 malwares publics, avant et après l'installation des signatures à jour :

Avant	Après
42	499
8%	99%

Distribution des détections



Comparaison Antivirus / Virustotal



Temps d'exécution

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

Mcafee

Chargement
Signatures

Scan

Mcafee-daemon

Chargement
Signatures

Démon

Mcafee-daemon

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

Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Construire une communauté

Avoir un projet open-source c'est bien.

Avoir des **utilisateurs** c'est mieux.

Avoir des **contributeurs** c'est encore mieux.

Construire une communauté

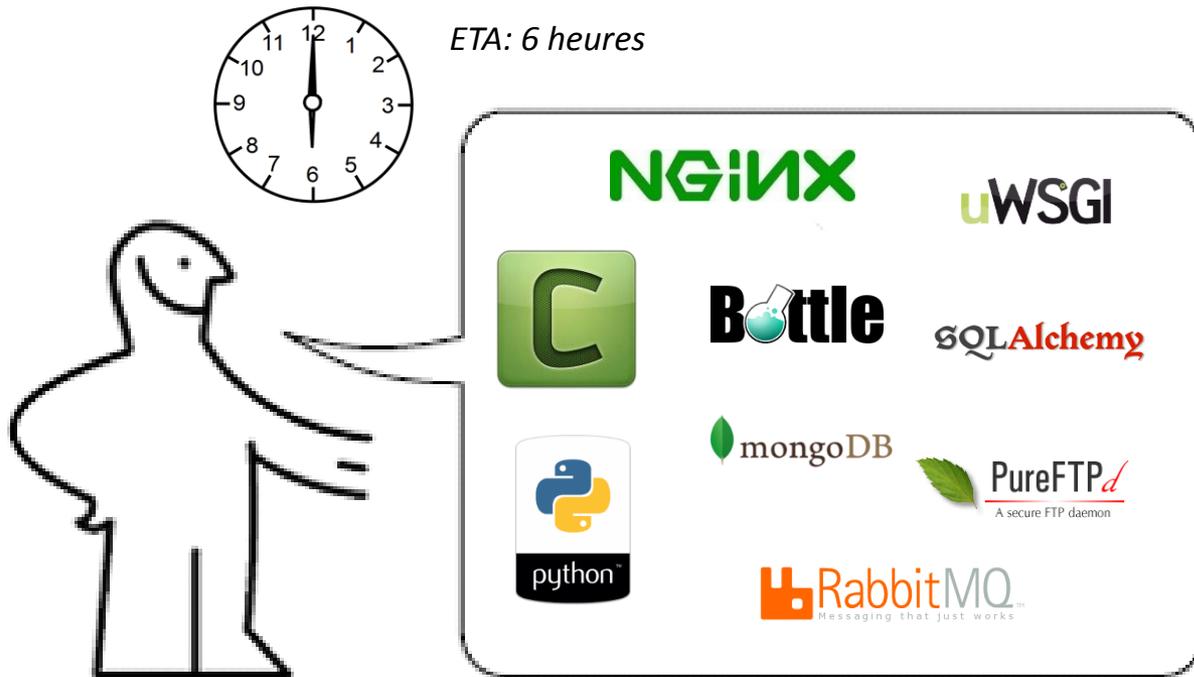
Avoir un projet open-source c'est bien.

Avoir des **utilisateurs** c'est mieux.

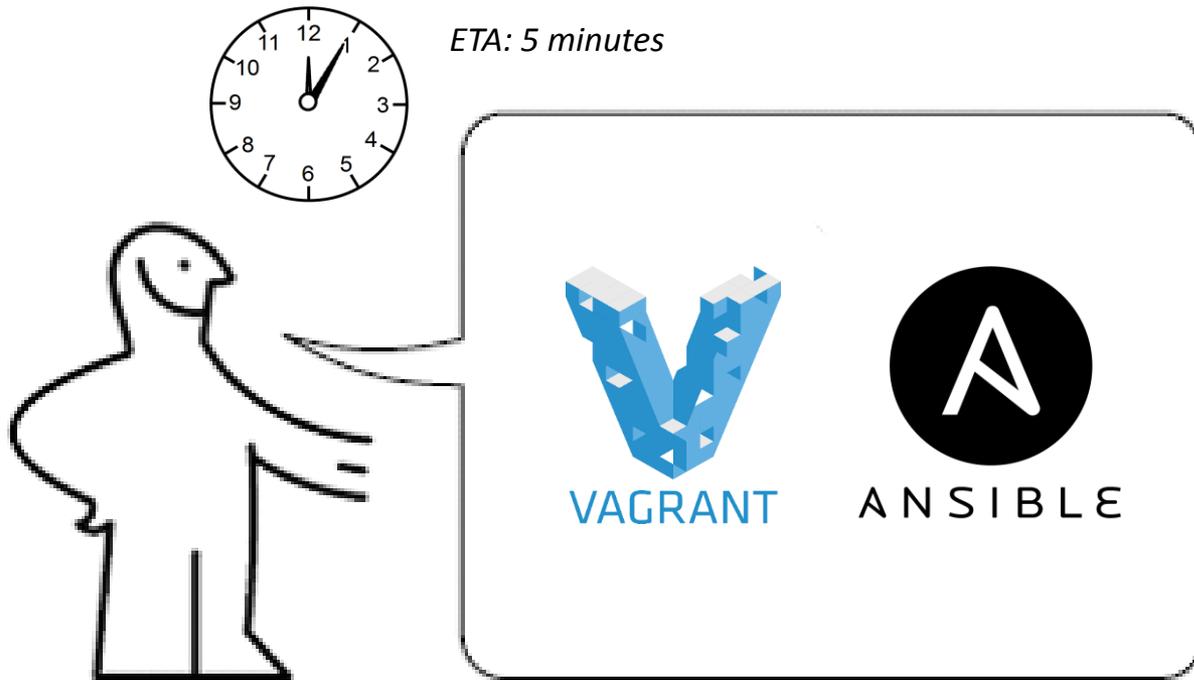
Avoir des **contributeurs** c'est encore mieux.

Nécessite un système d'installation simple et déterministe

Installation v1.0



Installation v1.1.0



Installation v1.1.0

Installation Vagrant :

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

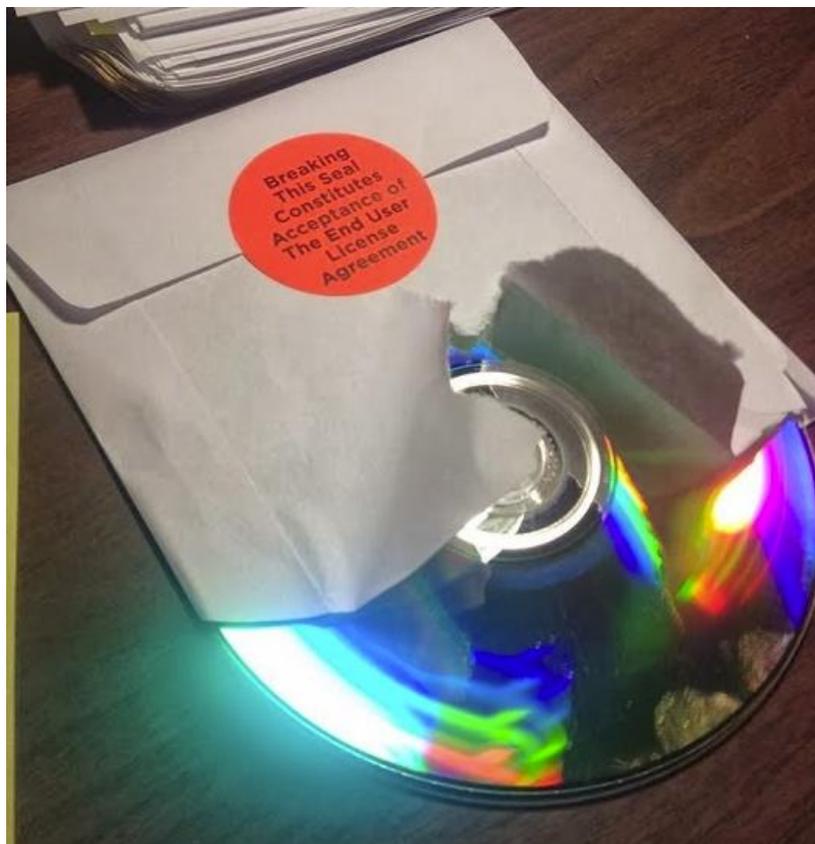
Installation Ansible :

```
$ sudo pip install ansible
```

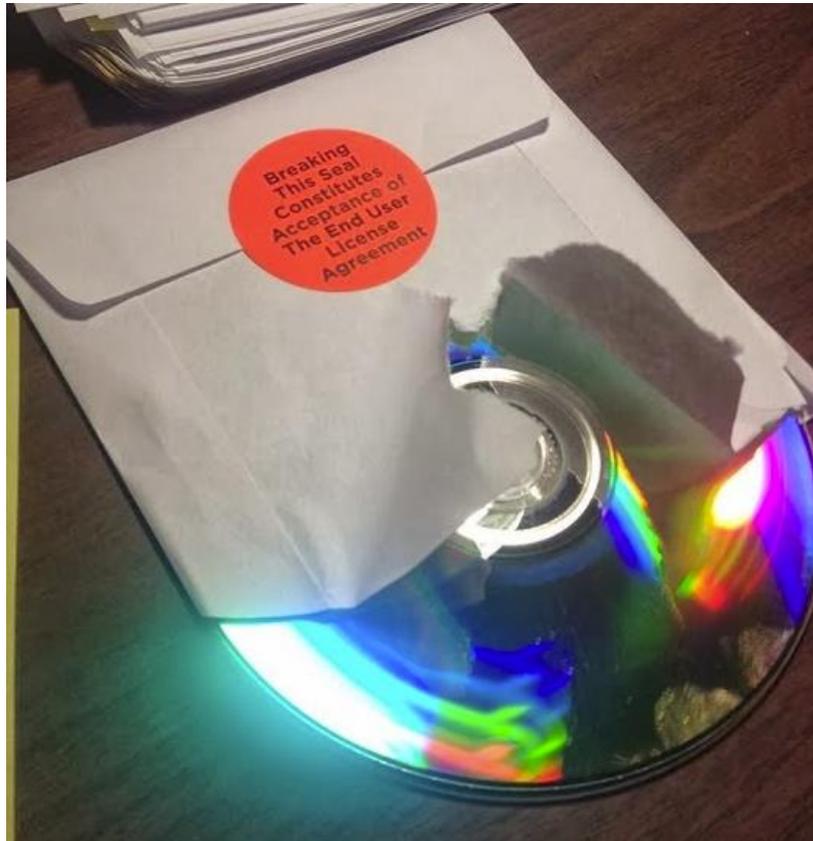
Installation IRMA:

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

EULA



EULA



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

Plan

1. Contexte et problématique
2. Fonctionnement
3. Quelques résultats
4. Retour d'expérience
5. Conclusion

Conclusion

- Framework privé d'analyse de fichiers.
- Facilité d'intégration de nouveaux modules.
- Multitude d'utilisations possibles.

Travaux futurs

- Recherche avancée sur les résultats d'analyses
- Ajout de probes:
 - analyse dynamique (Cuckoo Sandbox)
 - analyse d'applications mobiles
- Ajout de dispatcher

Contact

<http://irma.quarkslab.com> - irma-info@quarkslab.com



<https://github.com/quarkslab/irma>



@qb_irma

#irc

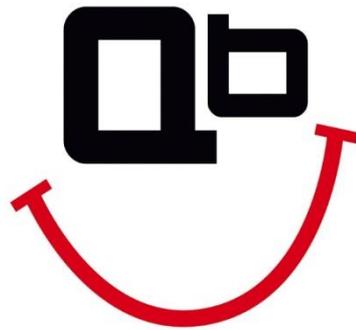
#qb_irma@freenode



Workshop



4 au 10 juillet 2015



www.quarkslab.com

contact@quarkslab.com | [@quarkslab](https://twitter.com/quarkslab)