

Malwares! Everywhere!

- par tAd pour le /tmp/lab -

Malwhat?

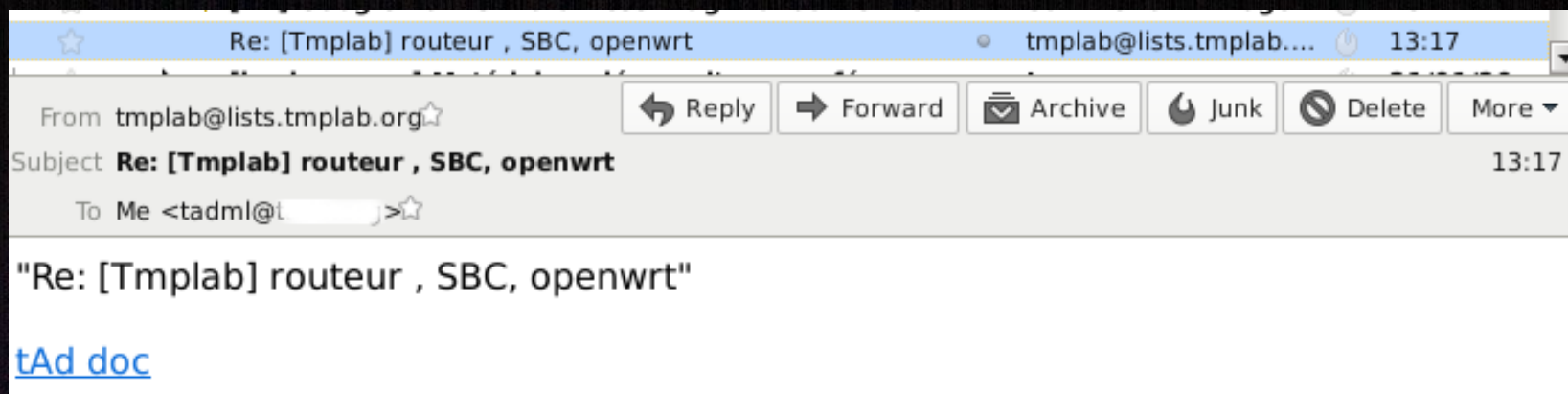
« Un logiciel malveillant ou maliciel (logiciel nuisible) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. » Wikipédia

Vecteurs d'infection

- . Mail (*phishing, spear phishing, whaling*)
- . Visite site (frame cachée, 0px, ...)
- . Ouverture fichier (.exe, .pdf, .swf, .doc, ...)
- . [...]

Once upon a time

C'est l'histoire d'un mail se faisant passer pour un mail provenant de la mailing-list du /tmp/lab:





Mail contenant un lien vers une URL tout à fait suspecte :

<http://phreshbanana.com/11103863SkBHf76f8HyKtE2NEdsfdN8KfNainbD6r5EA3zFfH52ZAFbFtrNe5KG5bAQYQkFi47G8Nrdhf47Gz9aRnQZfksarSQa/dEFk/3FFdEFk/>

!!!

Des outils en ligne

Analyse de l'URL par un navigateur en ligne: URLQuery



The screenshot shows the URLQuery website interface. At the top, there is a navigation bar with links for 'urlQuery', 'Search', 'Statistics', and 'About', and a 'Login' button on the right. Below the navigation bar, the 'Overview' section displays a table with the following information:

URL	phreshbanana.com/11103863SkBHf76f8HyKtE2NEdsfdN8KfNainbD6r5EA3zFfH52ZAFbFtrNe5KG5bAQYQkFi47G8Nrdhf47Gz9aRnQZfksarSQa/dEFk/3FFdEFk/
IP	97.74.180.128
ASN	AS26496 GoDaddy.com, LLC
Location	 United States
Report completed	2017-01-25 22:48:25 CET
Status	Report complete.
urlQuery Alerts	No alerts detected

To the right of the table, there is a small thumbnail image labeled 'Screenshot @' showing a webpage with a search bar and a 'Search' button.

<http://urlquery.net/report.php?id=1485380068601>

→ Récupération de l'URL exacte
du fichier

Des outils en ligne

→ Récupération de l'URL exacte
du fichier

```
GET /s/view/tAd.doc.zip HTTP/1.1
Host: lekovicmilos.com

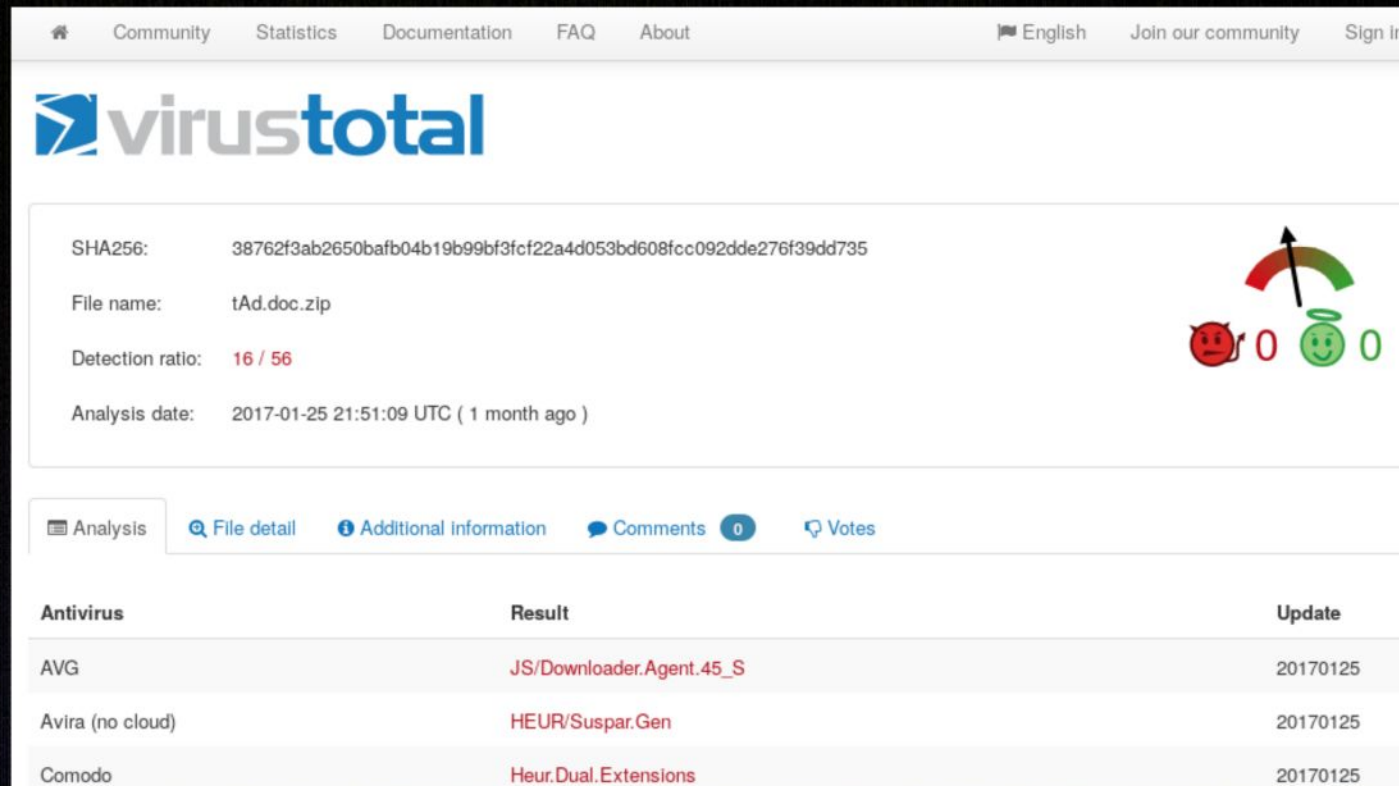
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://lekovicmilos.com/s/index.php?q=/11103863S
kBHf76f8HyKtE2NEdsfdN8KfNainbD6r5EA3zFfH52ZAFbFtrNe5KG5bA
QYQkFi47G8Nrdhf47Gz9aRnQZfksarSqa/dEFk/3FFdEFk/
```

```
185.96.210.16
HTTP/1.1 200 OK
Content-Type: application/zip
Date: Wed, 25 Jan 2017 21:47:40 GMT
Server: Apache
Last-Modified: Wed, 25 Jan 2017 21:47:39 GMT
Accept-Ranges: bytes
Content-Length: 10175
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

Récupération du fichier, pour analyse
(statique/dynamique)

Des outils en ligne

Analyse du fichier (ou de son hash) sur VirusTotal par exemple...



The screenshot shows the VirusTotal website interface. At the top, there is a navigation bar with links for Community, Statistics, Documentation, FAQ, and About. On the right, there are links for English, Join our community, and Sign in. The main header features the VirusTotal logo. Below the header, the analysis details for a file are displayed:

- SHA256: 38762f3ab2650bafb04b19b99bf3fcf22a4d053bd608fcc092dde276f39dd735
- File name: tAd.doc.zip
- Detection ratio: 16 / 56
- Analysis date: 2017-01-25 21:51:09 UTC (1 month ago)

To the right of these details is a gauge showing the detection ratio and two smiley face icons representing the ratio.

Below the analysis details, there is a tabbed interface with the following tabs: Analysis (selected), File detail, Additional information, Comments (0), and Votes.

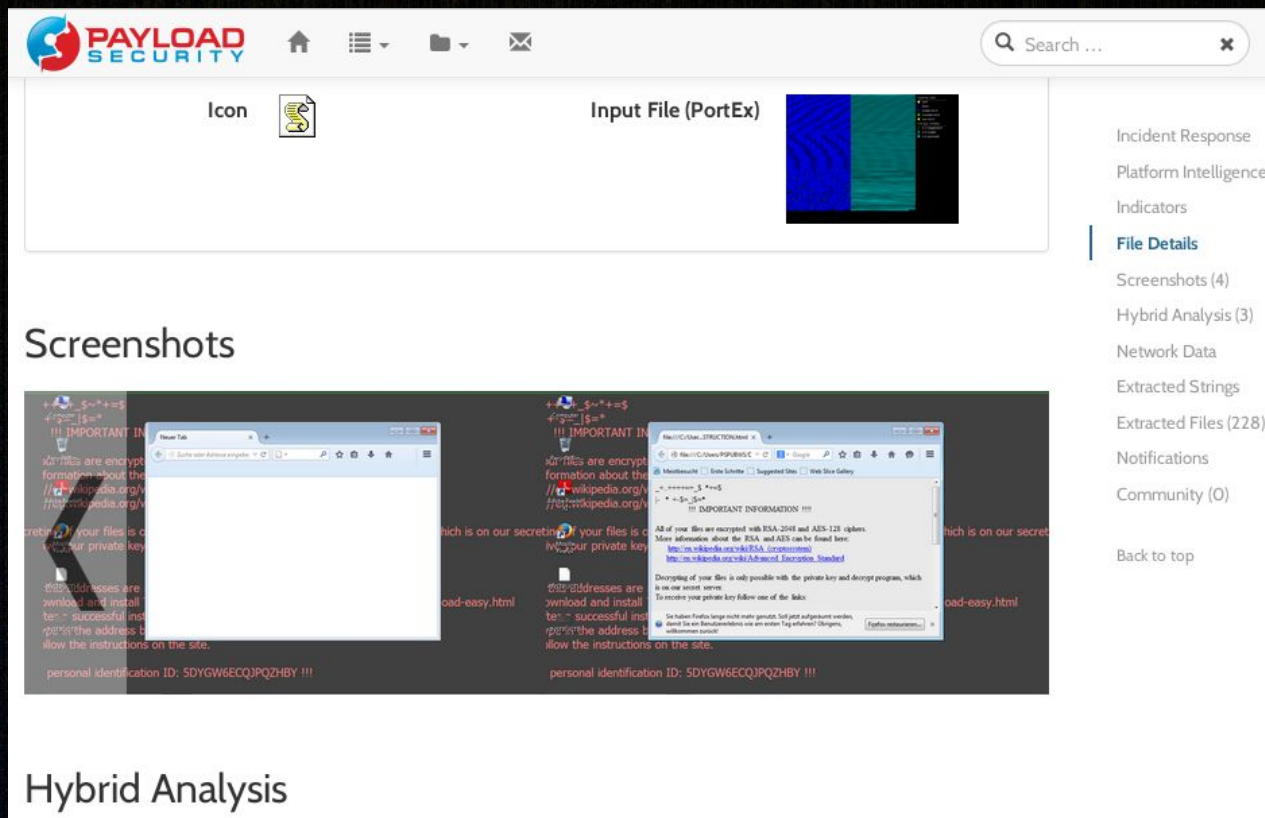
The Analysis tab displays a table of antivirus results:

Antivirus	Result	Update
AVG	JS/Downloader.Agent.45_S	20170125
Avira (no cloud)	HEUR/Suspar.Gen	20170125
Comodo	Heur.Dual.Extensions	20170125

→ permet de déterminer la nature de la menace, trouver des analyses existantes et déjà documentées

Des outils en ligne

Analyse du fichier sur une sandbox en ligne comme hybrid-analysis par exemple...

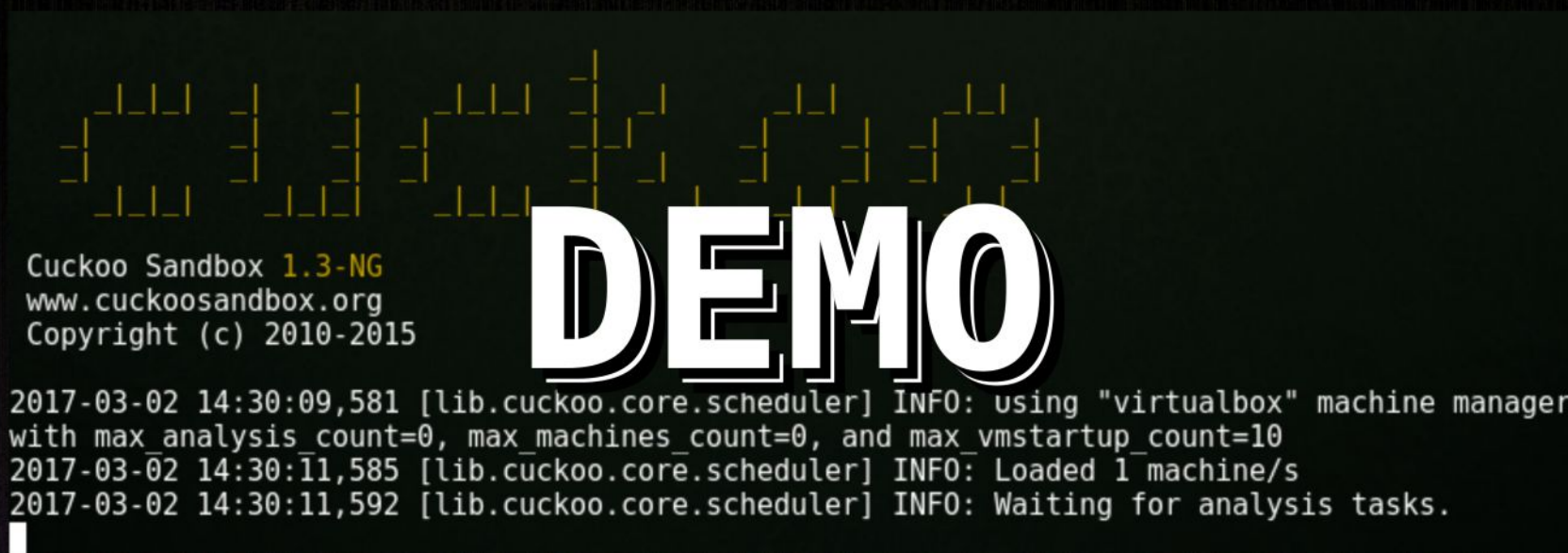


→ permet la récupération des IOC, l'analyse fine de la menace (génération rapport analyse), si cela s'exécute...

Des outils locaux

Analyse dynamique du fichier par exécution en sandbox: Cuckoo-modified

(<https://github.com/spender-sandbox/cuckoo-modified>)



→ permet de ne pas exfiltrer de données, la récupération des IOC (génération rapport analyse), ...

Des outils locaux

Analyse statique du fichier : rien n'est exécuté.

```
$ sha256sum tAd.doc.zip  
970e8600cfb3ee15baa0d55e8decf6d6194fb740ea48af8fd05d98285450cc37 tAd.doc.zip
```

```
$ zipinfo tAd.doc.zip  
Archive: tAd.doc.zip  
Zip file size: 5074 bytes, number of entries: 1  
-rw-rw-rw- 2.0 unx 8729 b- defN 16-Dec-31 07:17 tAd.doc.js  
1 file, 8729 bytes uncompressed, 4956 bytes compressed: 43.2%
```

```
$ sha256sum tAd.doc.js  
d13154232632001012d9ab342fccfe28eccff004f485970a8a95dcc526c09cb1 tAd.doc.js
```

```
$ file tAd.doc.js  
tAd.doc.js: ASCII text, with very long lines, with CRLF line terminators
```

**→ permet d'éviter les attaques sur la sandbox,
d'exposer l'architecture réseau, le SI, ...**

**Déjà beaucoup plus long et compliqué...
À suivre donc !**